Anno VII, n.ro 4 (19) - Periodicità bimestrale - **LUGLIO/AGOSTO 2015**

Poste Italiane Spedizione in A.P. - 45% Art. 2 Comma 20/B Legge 662/96 - Aut. N. DCDC/035/01/CS/CAL

SPECIALI

Win Magazine

SUL DVD
TUTTO IL SOFTWARE

INTERNET HACKING

LA GRANDE GUIDA

I trucchi degli esperti e i tool unofficial per **usare la grande Rete come non hai mai fatto prima**

- Naviga anche senza ADSL
- Scarica oltre i limiti di banda
- Chatta anonimo al 100%
- Proteggi la tua ADSL dai pirati
- Trucca il router e potenzia il Wi-Fi
- Scopri i segreti del Deepweb

Ed altri 40 progetti da veri smanettoni

ASUS®
IN SEARCH OF INCREDIBLE

ASUS consiglia Windows.

ASUS All In One PC
Tocca con mano la perfezione

Prestazioni formidabili
Sistema operativo Windows 8.1 e processore Intel® Core™ garantiscono potenza, velocità e massima efficenza

Immagini impeccabili
Display IPS 16:9 con risoluzione Full HD e ampio angolo di visualizzazione per un'esperienza visiva perfetta

Audio cristallino
Tecnologia ASUS SonicMaster per una eccezionale nitidezza sonora e bassi ricchi e corposi

Intrattenimento
Tutta la funzionalità dello schermo multi-touch 10 punti, connessione Wi-Fi 802.11n, 4 porte USB 3.0, Webcam e sintonizzatore TV integrato

Segui ASUS Italia

Lavora meglio. Divertiti di più. Windows

Poste Italiane Spedizione in A.P. - 45% Art 2 Comma 20/B Legge 662/96 - Aut. N. DCB/CI/0201/15/CS/CAL

SPECIALI

Win Magazine

INTERNET HACKING
LA GRANDE GUIDA

I trucchi degli esperti e i tool unofficial per **usare la grande Rete come non hai mai fatto prima**

- Naviga anche senza ADSL
- Scarica oltre i limiti di banda
- Chatta anonimo al 100%
- Proteggi la tua ADSL dai pirati
- Trucca il router e potenzia il Wi-Fi
- Scopri i segreti del Deepweb

Ed altri 40 progetti da veri smanettoni

Sommario

Win Magazine Speciali
Anno VII - n.ro 4 (19) - Luglio/Agosto 2015
Periodicità bimestrale
Reg. Trib. di Cs: 741 del 6 Ottobre 2009
Cod. ISSN: 2037-1608
e-mail: winmag@edmaster.it
www.winmagazine.it

DIRETTORE EDITORIALE: Massimo Mattone
DIRETTORE RESPONSABILE: Massimo Mattone

RESPONSABILE EDITORIALE: Gianmarco Bruni

EDITOR: Carmelo Ramundo
REDAZIONE: Paolo Tarsitano, Giancarlo Giovinazzo

SEGRETERIA DI REDAZIONE: Rossana Scarcelli

REALIZZAZIONE GRAFICA: CROMATIKA s.r.l.
RESPONSABILE GRAFICO DI PROGETTO: Salvatore Vuono
RESPONSABILE PRODUZIONE: Giancarlo Sicilia
AREA TECNICA: Dario Mazzei
ILLUSTRAZIONI: Tony Intieri
IMPAGINAZIONE: E. Monaco, L. Ferraro, F. Maddalone, T. Diacono

PUBBLICITÀ: MASTER ADVERTISING s.r.l.
Viale Andrea Doria, 17 - 20124 Milano - Tel. 02 83121211
Fax 02 83121207
advertising@edmaster.it

EDITORE: Edizioni Master S.p.A.
Via B. Diaz, 13 – 87036 RENDE (CS)
PRESIDENTE E AMMINISTRATORE DELEGATO: Massimo Sesti

ARRETRATI
ITALIA
Costo arretrati (a copia): il prezzo di copertina + € 6,10 (spedizione con corriere).
Prima di inviare i pagamenti, verificare la disponibilità delle copie arretrate inviando una e-mail ad arretrati@edmaster.it e la copia del pagamento potrà essere inviata via email o via fax al n. 199.50.00.05. La richiesta contenente i Vs. dati anagrafici e il nome della rivista, dovrà essere inviata via fax al num. 199.50.00.05* oppure via posta a EDIZIONI MASTER S.p.A. Viale Andrea Doria, 17 - 20124 Milano, dopo avere effettuato il pagamento, secondo le modalità di seguito elencate:

- assegno bancario non trasferibile (da inviare in busta chiusa con la richiesta);
- carta di credito, circuito Visa, Cartasi, o Eurocard/Mastercard (inviando la Vs. autorizzazione, il numero di carta, la data di scadenza, l'intestatario della carta e il codice CVV2, cioè le ultime 3 cifre del codice numerico riportato sul retro della carta).
- Bonifico bancario intestato a EDIZIONI MASTER S.p.A. c/o BANCA DI CREDITO COOPERATIVO DI CARUGATE E INZAGO S.C. - IBAN IT47R0845333200000000066000 (inviare copia della distinta insieme alla richiesta).

SOSTITUZIONE: Qualora nei prodotti fossero rinvenuti difetti o imperfezioni che ne limitassero la fruizione da parte dell'utente, è prevista la sostituzione gratuita, previo invio del materiale difettato. La sostituzione sarà effettuata se il problema sarà riscontrato e segnalato entro e non oltre 10 giorni dalla data effettiva di acquisto in edicola e nei punti vendita autorizzati, facendo fede il timbro postale di restituzione del materiale.
Inviare il supporto difettoso in busta chiusa a:
Edizioni Master - Servizio clienti Viale Andrea Doria, 17 - 20124 Milano

SERVIZIO CLIENTI
@ servizioclienti@edmaster.it
199.50.00.05* sempre in funzione
199.50.50.51* dal lunedì al venerdì 10.00 -13.00
*Costo massimo della telefonata 0,118 € + iva a minuto di conversazione, da rete fissa, indipendentemente dalla distanza. Da rete mobile costo dipendente dall'operatore utilizzato.

ASSISTENZA TECNICA (e-mail): winmag@edmaster.it
STAMPA: ROTOPRESS INTERNATIONAL S.r.l.
Via Mattei, 106 - 40138 - Bologna
DUPLICAZIONE SUPPORTI: Ecodisk S.r.l. - Via Enrico Fermi, 13
Burago di Molgora (MB)

DISTRIBUTORE ESCLUSIVO PER L'ITALIA:
m-dis distribuzione media S.p.A. - via Cazzaniga, 19 - 20132 Milano
tel: 02/25.82.1

Finito di stampare nel mese di Giugno 2015

Sommario

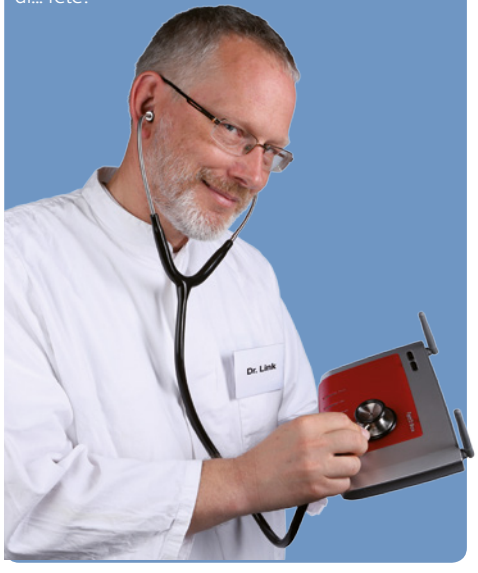
Internet dall'antenna. 08
Esiste una Rete fai da te, indipendente e aperta, accessibile a tutti... senza pagare alcun abbonamento. Solo noi ti diciamo come si fa!

Trucca il tuo router e naviga gratis!. 16
Lo accendi e senza inutili configurazioni accede a tutte le reti Wi-Fi... anche fino a 10km di distanza

Attenti a quel router Wi-Fi!. 18
Si chiama Beini CP-150JP ed è il preferito dai pirati: perché? In pochi clic permette a chiunque di bucare qualsiasi rete senza fili

Reti Wi-Fi crackate fino a 10 km 20
Alla scoperta delle nuove distribuzioni create per scardinare qualsiasi rete wireless: bastano davvero un paio di clic per farlo!

Cure miracolose per il Wi-Fi lento. 26
Non sentiamoci imbarazzati: quasi tutti soffriamo per una WLAN poco prestante. Ora finalmente è arrivato il rimedio per tutti i mal di... rete!



Windows diventa hotspot! 31
- ✓ Posso condividere la connessione Internet del PC con altri dispositivi hi-tech?
- ✓ Come sfruttare il router virtuale di Windows 8?

Naviga gratis con Facebook 32
Parti in vacanza e resta connesso a Internet. Gli hotspot Wi-Fi e le chiavi di accesso le trovi sulla tua bacheca!

Estendi il segnale della rete Wi-Fi. 35
Grazie ad un ripetitore wireless ti bastano pochi minuti per portare Internet in tutte le stanze di casa. Ecco come fare

Router: guida all'uso. 36
Scopri tutti i segreti del dispositivo che consente al tuo PC di accedere a Internet

Router no problem! 38
La connessione Internet non va o il PC non si collega alla LAN? Ecco i trucchi degli esperti per essere sempre connessi!

Internet doppia velocità 40
Tutti i trucchi per sfruttare contemporaneamente le connessioni 3G e ADSL e scaricare a 2X

L'antifurto per il Wi-Fi 44
Ecco come creare una finta rete wireless "aperta" per attirare in trappola gli intrusi e scoprire quali sono le loro intenzioni

"Così sblocco il router Alice" 48
Ecco come i pirati attivano un pannello di controllo avanzato per navigare più veloci senza smontare nulla

Tutti hacker, ma per gioco! 50
In regalo il simulatore di hacking per divertirsi a mettere sotto scacco il Web. Ecco come funziona

Abbiamo scoperto il Web segreto. 54
C'è una porta nascosta del Web dalla quale si accede ad un archivio di comunicazioni private

ADSL gratis su tablet e cellulari. 58
C'è chi ha trovato un modo per scroccare la connessione Wi-Fi altrui e navigare senza spendere un euro...

Il super browser di Win Magazine 62
Supera i limiti del Web e trasforma il tuo software di navigazione in un sistema perfetto per fare di tutto e di più in Rete

La cronologia del Web anonimo. 69
- ✓ È possibile risalire ai siti visitati durante una sessione di navigazione in incognito?
- ✓ Posso consultare Internet senza lasciare tracce?

Maledette toolbar!. 70
Rallentano la navigazione, consumano memoria e rubano dati personali. Rimuovile per sempre

Scarica tutto dalle reti segrete. . . . 74
Software e abbonamento Premium per avere libero accesso ai canali underground del file sharing

Il telefono invisibile! 78
Configura un dispositivo VOIP "inesistente" per dire e scrivere di tutto senza essere intercettati!

La mia casa è cablata! 84
Tutte le soluzioni per condividere ADSL, file, cartelle e stampanti tra i dispositivi della tua rete LAN domestica

Condividiamo i dati in LAN 90
Ecco come creare una cartella condivisa sul PC accessibile via rete dal nostro smartphone o dal tablet Android

il nostro NAS finisce in Rete 95
La guida per condividere i nostri contenuti multimediali tra i PC della LAN e avviarne lo streaming

I prezzi di tutti i prodotti riportati all'interno della rivista potrebbero subire variazioni e sono da intendersi IVA inclusa

TP-LINK®
The Reliable Choice

Sorveglianza 24 ore su 24

Telecamera Cloud Notte/Giorno 300Mbps Wi-Fi NC220

TP-LINK cloud

- Notte e giorno con **LED IR**
- **Range Extender** amplia la copertura Wi-Fi
- Semplice configurazione col pulsante **WPS**
- Posizionamento flessibile

Monitoraggio bambini

Monitoraggio domestico

Monitoraggio animali

Non perdere di vista ciò che ami.

Con il portale web **tplinkcloud.com** e l'App gratuita **tpCamera**, è possibile registrare video, scattare foto o verificare quello che sta succedendo.
Avvisi Motion Detection inviati tramite e-mail o FTP.

TP-LINK ITALIA s.r.l. www.tp-link.it support.it@tp-link.com

TP-LINK è fornitore a livello mondiale di prodotti di networking SOHO e uno dei maggiori player sul mercato globale, con prodotti disponibili in oltre 120 paesi e decine di milioni di clienti.

Il software sul DVD-Rom

SPECIALI Win Magazine

INCLUDE

DVD da 4,3 GB

INTERNET

Ufo Wardriving 4 Invasion

Recupera le chiavi di Rete di tantissimi router Wi-fi

Tipo: Freeware File: setup_ufo4.zip

ADSL no problem

La guida PDF per dire addio ai problemi di Rete

Tipo: Freeware File: ebook_adsl_no_problem.zip

Mother

Il simulatore di hacking per mettere sotto scacco il Web

Tipo: Freeware File: mother.zip

TOR Browser 4.5

Naviga e scarica da Internet senza lasciare tracce

Tipo: Freeware File: torbrowser-install_it.zip

WPA Tester 4

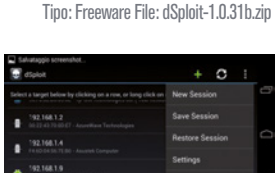
Scova i bug nel tuo router Wifi

Tipo: Freeware File: online

dSploit 1.0.31b

L'app android per scardinare qualsiasi rete

Tipo: Freeware File: dSploit-1.0.31b.zip



jDownloader 2

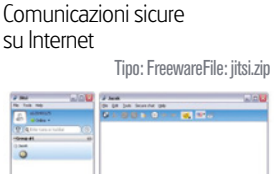
Scarica senza attese dai principali siti di filehosting

Tipo: Freeware File: JDownloader2Setup.zip

Jitsi 2.4

Comunicazioni sicure su Internet

Tipo: FreewareFile: jitsi.zip



TorChat

Chattare in perfetto anonimato

Tipo: FreewareFile: torchat.zip

Comodo IceDragon Browser

Il browser per viaggiare spediti in Rete

Tipo: FreewareFile: icedragon.zip

Mymail-Crypt

La mia posta è cifrata

Tipo: FreewareFile: online

Mozilla Firefox 37.02

Il browser veloce e sicuro con le videochiamate integrate

Tipo: FreewareFile: Firefox Setup.zip

Google Chrome 42.0.2311

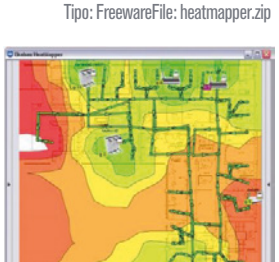
Il browser multifunzione che mette il turbo

Tipo: FreewareFile: ChromeSetup.zip

Ekahau HeatMapper

Mappa la qualità del segnale WiFi di casa tua

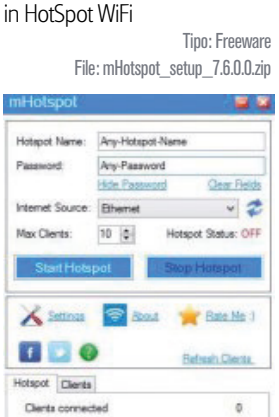
Tipo: FreewareFile: heatmapper.zip



mHotspot 7.6.0

Trasforma il computer in HotSpot WiFi

Tipo: Freeware File: mHotspot_setup_7.6.0.0.zip



pfSense 2.1.4

Il Firewall sviluppato su piattaforma FreeBSD

Tipo: FreewareFile: pfSense-LiveCD-2.1.4.ZIP

OpenWRT-Raspi

L'immagine del sistema operativo OpenWRT

Tipo: FreewareFile: openwrt-raspi.zip

Putty 0.64

Client SSH e telnet per Windows

Tipo: FreewareFile: putty.zip

WinMagazine Explorer 1.0

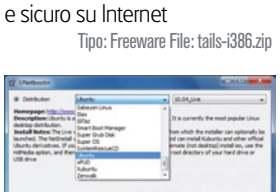
Il browser di Win Magazine per navigare "senza volto"

Tipo: FreewareFile: WinMagExplorer.zip

Tails OS 1.4

Il sistema operativo anonimo e sicuro su Internet

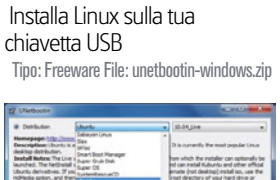
Tipo: Freeware File: tails-i386.zip



Titolo: UNetbootin 608

Installa Linux sulla tua chiavetta USB

Tipo: Freeware File: unetbootin-windows.zip



BF Words

Il tool che crea dizionari per attacchi brute force

Tipo: Freeware File: bf-words-windows.zip

XiaoPan OS PRO 1.0

Tutti gli strumenti per il crack delle reti Wi-Fi

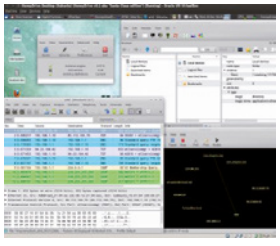
Tipo: Freeware File: online

Aircrack 1.2.1

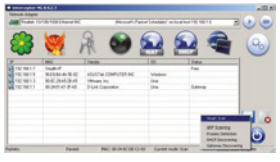
Il passepartout per le connessioni Wi-Fi!

Tipo: FreewareFile: aircrack.zip

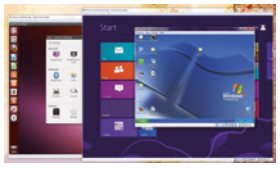
HoneyDrive 3
Tutti i tool per controllare il traffico Web
Tipo: Freeware File: online



Intercepter-NG 0.9.9
Lo sniffer di rete che intercetta il traffico
Tipo: Freeware File: Intercepter-NG.zip

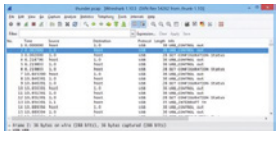


VirtualBox 4.3.24
Virtualizzazione completa dei sistemi operativi
Tipo: Freeware File: VirtualBox-Win.zip

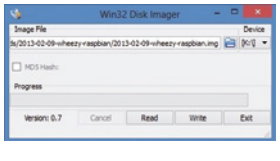


Greasemonkey 2.3
Il plug-in di Firefox per modificare le pagine Web
Tipo: Freeware File: greasemonkey-fx.zip

Wireshark 1.10.1
Analizza e filtra il contenuto di tutti i pacchetti di rete
Tipo: Freeware File: Wireshark-win.zip

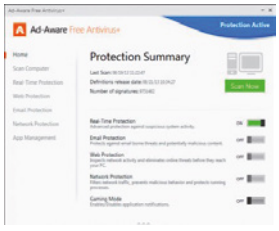


Win32 Disk Imager 0.9.5
Il tool per avviare i sistemi operativi da Pendrive USB
Tipo: Freeware File: Win32DiskImager-install.zip

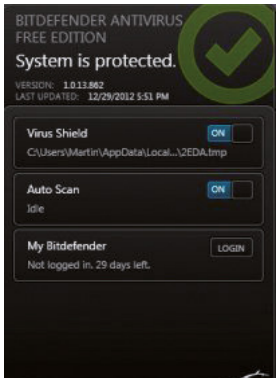


Look@LAN Network Monitor 2.50 build 35
Tieni sotto controllo la tua rete LAN
File: Look@man.exe

Ad-Aware Free Antivirus 11+
La soluzione contro virus e spyware
Tipo: Freeware File: Adaware_Installer.zip

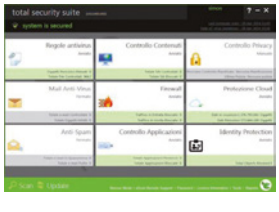


Bitdefender Antivirus Free Edition
Lo scanner che ripulisce il PC da qualsiasi minaccia
Tipo: Freeware File: Antivirus_Free_Edition.zip



Emsisoft Emergency Kit 4.0
La cassetta di sicurezza per curare il PC infetto
Tipo: Freeware File: EmsisoftEmergencyKit.zip

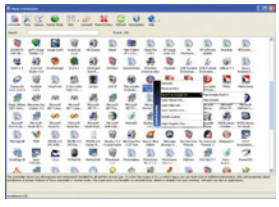
eScan Total Security 14
La nuova suite per la sicurezza del PC
Tipo: Trial File: twn2k3ek.zip



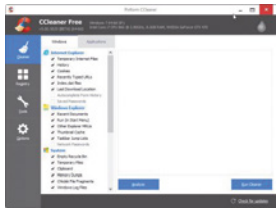
Malwarebytes Anti-Malware 2.1.4
Scansione e rimozione di spyware e malware
Tipo: Freeware File: mbam-setup.zip

Junkware Removal Tool 6.6.5
Piazza pulita delle toolbar indesiderate
Tipo: Freeware File: JRT.zip

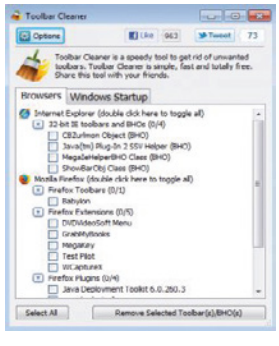
Revo Uninstaller 1.95
Uninstaller radicale che non lascia traccia dei software
Tipo: Freeware File: revosetup.zip



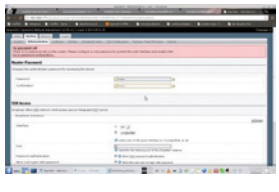
CCleaner 5.05.5176
Ripulisci a fondo il PC da file inutili e obsoleti
Tipo: Freeware File: ccsetup.zip



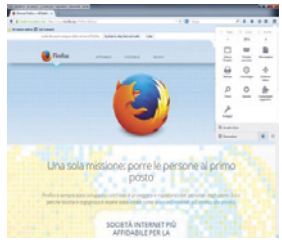
Toolbar Cleaner
Via le toolbar in pochi secondi
Tipo: Freeware File: toolbarcleaner_setup.zip



OpenWRT-Raspi
L'immagine del sistema operativo OpenWRT
Tipo: Freeware File: openwrt-raspi.zip

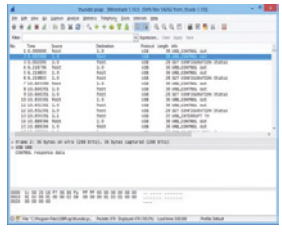


Firefox Hello
Chiamate vocali direttamente dal browser
Tipo: Freeware File: Firefox Setup.zip

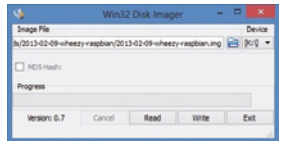


Greasemonkey
Sottotitolo: Il plug-in di Firefox per modificare le pagine Web
Tipo: Freeware File: greasemonkey-fx.zip

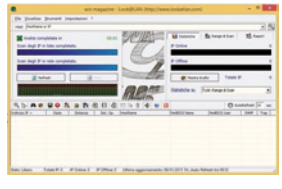
Wireshark
Analizza e filtra il contenuto di tutti i pacchetti di rete
Tipo: Freeware File: Wireshark-win.zip



Win32 Disk Imager
Il tool per avviare i sistemi operativi da Pendrive USB
Tipo: Freeware File: Win32DiskImager-install.zip

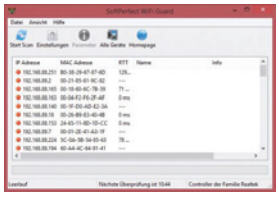


Look@LAN Network Monitor
Tieni sotto controllo la tua rete LAN
Tipo: Freeware File: look-lan-network-monitor.zip

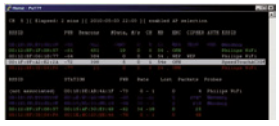


Wifi Protector 3.3.34
Connessione WiFi sotto controllo
Tipo: Freeware File: wifiprotector.zip

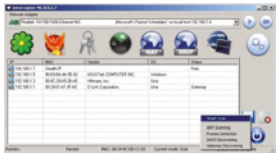
SoftPerfect WiFi Guard 1.05
Controlla e gestisce gli accessi alla rete WiFi
Tipo: Freeware File: wifiguard_windows_setup.zip



Aircrack 1.2.2
Il passepartout per controllare le connessioni WiFi!
Tipo: Freeware File: aircrack-ng-1.2-rc2-win.zip

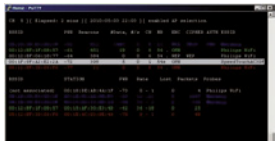


Intercepter-NG 0.9.9
Lo sniffer di rete che intercetta il traffico
Tipo: Freeware File: Intercepter-NG.zip



WPA Tester Defectum
Scova i bug nel tuo router Wifi
Tipo: Freeware File: wpatester.zip

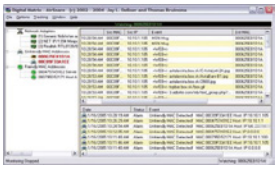
Aircrack GUI
Il passepartout per le connessioni Wifi
Tipo: Freeware File: aircrack.zip



zANTI
Il tool avanzato per testare la sicurezza della Rete
Tipo: Freeware File: zanti.zip

inSSIDer for Home 4
Controllare le reti wireless e cambiare i canali
Tipo: Freeware File: inSSIDer4-installer.zip

AirSnare 1.5
Connessione wireless al riparo da intrusioni
Tipo: Freeware File: AirSnare-Setup.zip



Internet dall'antenna

Esiste una Rete fai da te, indipendente e aperta, accessibile a tutti... senza pagare alcun abbonamento. Solo noi ti diciamo come si fa!

Che la situazione dell'infrastruttura di rete in Italia sia disastrata, è ormai cosa nota. Nonostante i progressi degli ultimi anni, esistono ancora molte zone sprovviste di un collegamento ad Internet a velocità accettabili, complice anche la morfologia del nostro territorio. I tempi, però, sono cambiati. Una volta erano necessari grandi investimenti per collegare in rete dei computer, perché l'unico strumento disponibile erano dei cavi di rame. Oggi, invece, le tecnologie Wi-Fi ci consentono di connettere tra loro tanti computer con una spesa minima (del resto, le onde radio non si pagano).

Il guadagno è garantito

Facciamo una semplice stima: un router (o ripetitore) Wi-Fi deve essere posizionato ogni 100 metri, che è anche la lunghezza massima consigliabile per un cavo ethernet. Supponiamo di voler collegare al massimo 30 dispositivi, in modo da dare a ciascuno almeno 3 Mb/s di banda. Per ciascun dispositivo spendiamo 20 euro per il cavo ethernet, mentre dividendo il costo di un router Wi-Fi per un centinaio di dispositivi, abbiamo una spesa di circa 0,5 euro a computer. In pratica, il Wi-Fi costa ben 40 volte in meno, e siamo stati piuttosto generosi nei confronti della tecnologia via cavo. È infatti necessario considerare anche le reti a 5 GHz, che possono portare la distanza massima di collegamento a 10 chilometri con un unico punto di accesso.

Così nascono le reti mesh

Leggendo questi numeri verrebbe da chiedersi come mai non si utilizzi proprio la tecnologia Wi-Fi per collegare più computer possibili. In

effetti, a molti è venuta in mente questa stessa idea, la cui messa in pratica ha portato alla realizzazione delle cosiddette "reti mesh" (dette anche reti a maglia). Rispetto alla tradizionale Internet che usiamo ogni giorno, una rete mesh si basa su una infrastruttura decentralizzata in cui non ci sono server centrali, ma un gran numero di nodi che fungono essi stessi da trasmettitori, ricevitori e ripetitori del segnale Wi-Fi. Le reti mesh, quindi, sono state sviluppate anche con l'intenzione di creare una "internet" indipendente dai provider, funzionante senza pagare alcun abbonamento e, per la sua particolare tipologia di collegamento (Wireless punto a punto), fino a 30 volte più veloce della tradizione connessione ADSL. Ed inoltre, vantaggio non da poco, rimarrà accessibile anche quando i server dei provider e il Web in generale saranno down.

Ninux: la rete mesh in pratica

Uno dei progetti più interessanti e promettenti in questo senso è Ninux (http://ninux.org), la principale rete mesh italiana in cui non esiste un provider che fornisce la connessione agli utenti, ma ogni utente è esso stesso un piccolo provider. I computer collegati a Ninux, infatti, si chiamano nodi (proprio come quelli di una rete da pesca) e sono tra loro interconnessi in modo automatico. Il risultato è che ogni nodo può comunicare con un altro qualsiasi, semplicemente passando attraverso diversi altri nodi (anche se la connessione Wi-Fi è in chiaro, se la comunicazione è cifrata dall'applicazione i nodi intermedi non possono leggerla). L'aspetto più importante di questa struttura è che non esiste un "capo". Non c'è alcun organismo che possa controllare la rete e censurarla: Ninux è quindi una rete libera. Ed anche gratuita perché, come abbiamo detto, le onde radio (a 2,4 o 5 GHz, in uso da Ninux) non si pagano e non vi è alcun canone.

Nel progetto Ninux la parola "hacker" assume il suo più vero significato. Troppo spesso, infatti, siamo abituati ad utilizzare il termine hacker con una accezione negativa, come sinonimo di pirata informatico. Chi utilizza strumenti informatici per commettere crimini o comunque azioni moralmente controverse è definito "cracker". Questo equivoco è dovuto anche alla somiglianza tra i suoni dei due termini. In realtà, la parola hacker indica una persona che inventa nuovi metodi e strumenti per migliorare la vita delle persone utilizzando l'informatica. In particolare, è hacker chi crede nella libertà di informazione e nel diritto per chiunque di accedere a computer e reti internet.

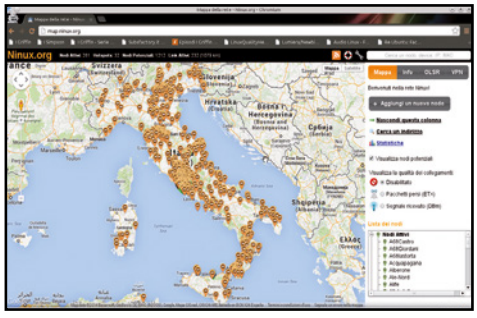
Bastano antenna e router

Gli strumenti necessari a mettere in piedi un nodo Ninux sono facilmente acquistabili tramite Internet oppure in un supermercato, e chiunque può farlo a casa propria. Noi abbiamo contattato l'HackLab di Cosenza (http://hlcs.it) per approfondire la questione e, in queste pagine, vogliamo guidarvi nella realizzazione di un nodo "foglia" (il tipo più semplice di

punto di accesso Ninux). Noi stessi ne abbiamo realizzato uno nella nostra redazione. Per installare anche a casa gli apparati per collegarsi alla rete Ninux, oltre a seguire la nostra guida pratica, possiamo prendere contatti con gli esperti di Ninux, iscrivendosi alla mailing list ufficiale (inviando un'e-mail vuota all'indirizzo wireless-subscribe@ml.ninux.org) e chiedendo un supporto pratico per l'installazione. Soprattutto se non siamo molto pratici di configurazione delle reti e non abbiamo mai messo mano al nostro router casalingo, è

A Posizioniamo l'antenna Wi-Fi

Sfruttando la mappa disponibile sul sito del progetto Ninux possiamo individuare altri nodi della rete nelle nostre vicinanze. Se non ci sono ostacoli visivi tra noi e l'Access Point, procediamo con l'installazione dell'antenna.



1 La mappa dei nodi

Per entrare in Ninux dobbiamo collegarci ad un nodo vicino. Verifichiamo se ne esistono vicini a noi visitando la pagina http://map.ninux.org. Funziona come una mappa di Google ed ogni punto verde indica un nodo attivo, mentre gli arancioni sono utenti che, come noi, vogliono collegarsi.

2 Si vede o non si vede?

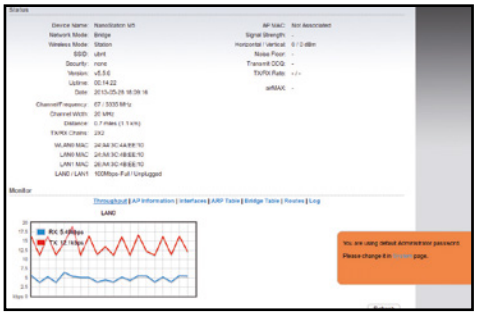
Verificata l'esistenza di un nodo a meno di 10 km di distanza, verifichiamo l'effettiva visibilità della sua antenna. Basta salire sul tetto o scendere in giardino con un binocolo e, con l'aiuto di una bussola (oppure usando la mappa di Ninux che consente di collegare i nodi), individuare il punto di accesso.

3 Cacciavite in mano

A questo punto fissiamo l'antenna Wi-Fi al supporto, sul tetto o in giardino, realizzando l'operazione nel modo più sicuro possibile (http://photogallery.ninux.org): se necessario, chiediamo aiuto ad esperti. Considerando il costo dell'antenna, sarebbe un peccato vederla volare alla prima folata di vento.

B Configuriamo l'antenna Wi-Fi

Colleghiamo la nostra Ubiquiti Nanostation M5 direttamente al computer utilizzando un normale cavo Ethernet. Tramite un intuitivo pannello di controllo basteranno pochi clic per configurarla al meglio.



1 Ecco l'interfaccia Web

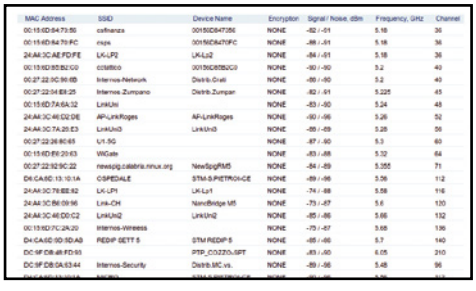
Per la configurazione iniziale, l'antenna va collegata al PC tramite cavo Ethernet. Questa operazione si può fare mentre siamo sul tetto o in giardino, in modo da posizionare al meglio l'antenna, quindi usiamo un notebook. Col browser colleghiamoci all'indirizzo *192.168.1.20*.

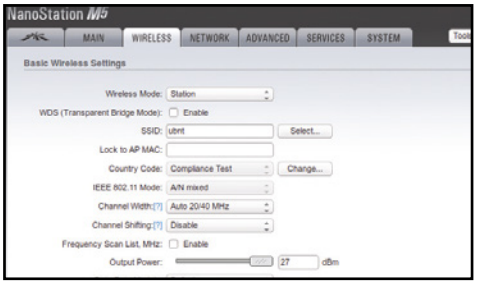
2 Nome utente e password

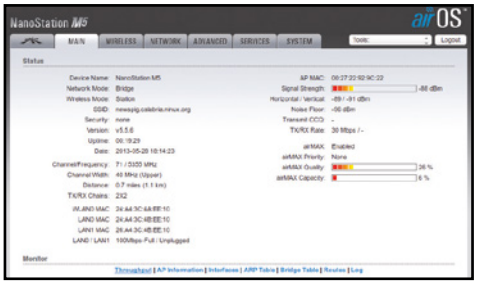
La pagina che si apre è il pannello di configurazione dell'antenna. Dobbiamo effettuare il login inserendo i dati di accesso predefiniti: *ubnt* sia come nome utente sia come password. È anche necessario specificare che risiediamo nel paese *Italia*, mentre possiamo mantenere la lingua inglese.

3 Il pannello di controllo

Dal menu *Tools* (in alto a destra nella schermata) scegliamo la funzione *Site Survey*: apparirà una finestra popup con l'elenco delle reti visibili dalla nostra postazione. Questo ci serve per verificare che l'antenna del nodo a cui vogliamo collegarci sia effettivamente visibile.







4 Tutte le antenne Wi-Fi

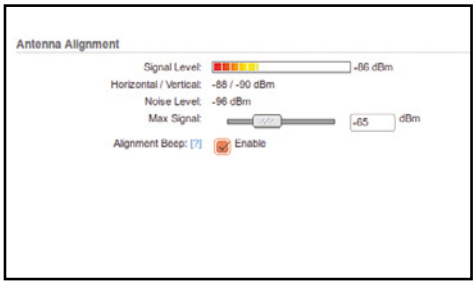
Trovare l'antenna che ci interessa dovrebbe essere facile: di solito, infatti, ha lo stesso nome del nodo Ninux che abbiamo letto sulla mappa della rete. Sarebbe opportuno anche avvisare il proprietario del nodo in questione, piuttosto che collegarci alla sua antenna senza farglielo sapere.

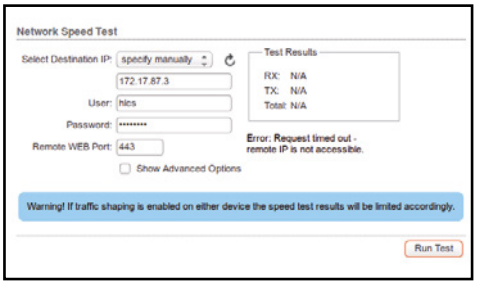
5 A chi mi collego?

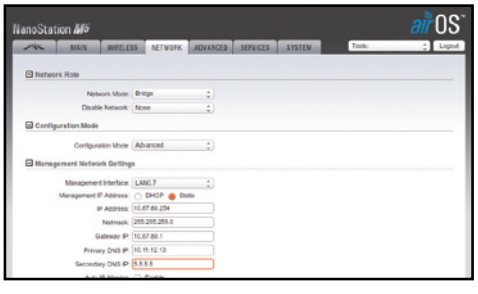
Nel pannello di controllo, dalla scheda Wireless clicchiamo sul pulsante *Select* a fianco del campo *SSID* e scegliamo dall'apposito menu popup il nome dell'antenna a cui vogliamo collegarci. Quindi selezioniamo il campo *Look to AP MAC* e clicchiamo sul pulsante *Change/Apply*.

6 È buona la ricezione?

Una volta effettuata l'associazione con il nostro nodo Ninux di riferimento, nella scheda *Main* possiamo visualizzare la potenza del segnale: si tratta della barra *Signal strength*. Nella stessa scheda dovrebbe comparire anche una stima della velocità di connessione (*TX/RX Rate*).







7 Più a destra, più a sinistra!

Se ci troviamo sul tetto, assieme al nostro notebook, possiamo sfruttare il tool di allineamento (*Antenna Alignment*) per verificare quale sia la posizione migliore per l'antenna, in modo da avere un segnale tra i *-70* e *-65 decibel*. Questo strumento si trova sempre nel menu a tendina *Tools*.

8 Il test della velocità

Mentre spostiamo l'antenna, potremmo sentire dei segnali sonori: il "beep" si farà più acuto man mano che il segnale diventerà più forte. Contemporaneamente, possiamo eseguire un test della velocità di connessione, usando lo strumento *Speed Test* dal solito menu a tendina *Tools*.

9 Impostazioni di rete

Per impostare la connessione, da *Network* selezioniamo *Configuration Mode/Advanced*. Impostiamo gli indirizzi prenotati su *http://wiki.ninux.org/GestioneIndirizzi*, eventualmente facendo riferimento alla *Guida Completa al Routing a Terra Ninux* (www.winmagazine.it/link/2653).

meglio avere vicino (anche virtualmente) qualcuno che se ne intenda più di noi. È importante ricordare che la rete Ninux è una rete parallela alla Internet che conosciamo e alla quale ci colleghiamo tutti i giorni, quindi il traffico su di essa è ben distinto da quello tipico del Web. Tuttavia, esistono dei nodi che potrebbero fornire un punto di uscita proprio verso Internet, condividendo la propria ADSL, di modo che gli utenti di Ninux possano accedere ai loro siti Web preferiti della rete mondiale pur rimanendo all'interno della mesh network.

Non esiste solo Ninux

Ninux è dunque un progetto adatto alle utenze domestiche, considerando che le apparecchiature non sono propriamente tascabili. Non è comunque l'unica rete mesh esistente.Abbiamo infatti scoperto altri due progetti molto interessanti: il primo si chiama AirChat, è stato progettato da alcuni membri del collettivo Anonymous, ed è una sorta di Ninux portatile. È stato molto utile durante le proteste in Egitto e Siria per consentire alle persone un libero accesso alla rete bypassando la censura governativa e senza rischio di intercettazione. L'altro progetto è chiamato Serval e vuole creare una rete di telefonia mobile libera e gratuita per comunicare senza bisogno di SIM e abbonamenti. Per saperne di più leggiamo i due approfondimenti di pagina 15, dedicati proprio a queste tecnologie.

La parola all'avvocato

CONDIVIDERE L'ADSL È LEGALE?

Guido Scorza è uno dei massimi esperti in Diritto delle Nuove Tecnologie

Un nodo della rete Ninux può fornire l'accesso a Internet ad altri nodi della rete stessa. Ma è legale condividere la propria ADSL con altri utenti? Lo abbiamo chiesto all'avvocato Guido Scorza.

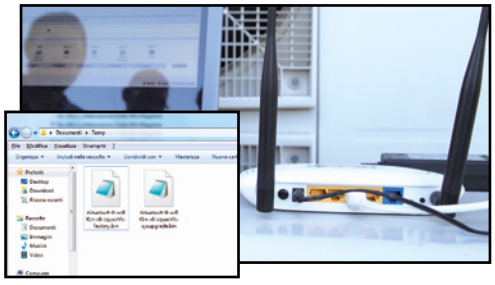
A casa abbiamo un contratto di abbonamento a Internet intestato a noi. Se facciamo parte della community Ninux, possiamo condividerlo con altri utenti della rete?
Dobbiamo abituarci a pensare a Internet come al telefono, alla luce, all'acqua o al gas. È vietato ridistribuire tali risorse all'esterno della nostra abitazione e, comunque, dietro pagamento di un corrispettivo. Ma nessuno può impedirci di condividerne l'utilizzo con i nostri amici, parenti ed ospiti.

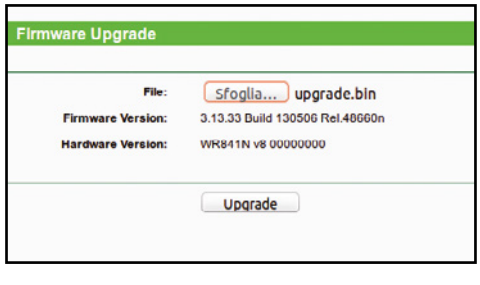
Adesso che il Wi-Fi in Italia è stato liberalizzato, possiamo condividere le nostre risorse di connettività?
L'abrogazione del famigerato Decreto Pisanu che ha "liberalizzato" il Wi-Fi anche nel nostro Paese non ha niente a che vedere con questo tipo di situazione e la risposta è, sfortunatamente, negativa. La possibilità di porre a disposizione la connettività Internet al nostro vicino di casa (in questo caso un utente Ninux) e, quindi, al di fuori delle mura domestiche, è probabilmente preclusa già dal contratto di fornitura che ci lega al provider. E poi tale condotta rischia di trasformarci in un piccolo Internet Service Provider, con conseguente esigenza di una speciale autorizzazione ad esercitare tale funzione e, soprattutto, con un'insostenibile mole di piccole e grandi obbligazioni a nostro carico.

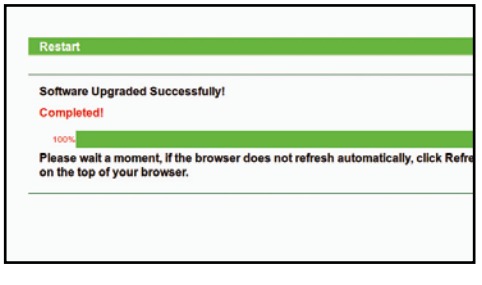
A proposito di Wi-Fi libero, cosa significa esattamente? Da oggi possiamo andare in un bar e scaricare tutta la musica che piace a noi?
"Wi-Fi libero" è solo una formula giornalistica di successo per evidenziare la riconquistata libertà dell'uso del Wi-Fi dopo anni di regime fortemente burocratizzato a causa del cosiddetto Decreto Pisanu. L'espressione non ha, tuttavia, niente a che fare con lo specifico utilizzo del quale ciascuno di noi può o meno fare delle risorse di connettività. Il Peer to Peer non è, certamente, vietato e, pertanto, se il gestore del bar o un nodo Ninux non ha niente in contrario, lo lascerà usare ai propri clienti/utenti. Che, tuttavia, non potranno utilizzarlo per scaricare illecitamente materiale protetto da diritto d'autore, a pena di commettere, in prima persona, un reato.

C Prepariamo il router per Ninux

Il firmware originale installato sul TP-Link usato nelle prove è troppo "rigido" e non permette la connessione alla rete mesh Wi-Fi. Grazie a OpenWRT possiamo aggirare il problema. Ecco come aggiornare il firmware.







1 Immagine già pronta

Sul Win DVD-Rom troviamo il file *ninucswrt-tl-wr841n-v8-squashfs-factory.bin*, che contiene l'immagine di OpenWRT: scarichiamolo dal supporto allegato alla rivista e copiamolo sul PC. Colleghiamo il router al computer, avviamo il browser e colleghiamoci all'indirizzo *192.168.0.1*.

2 L'interfaccia Web

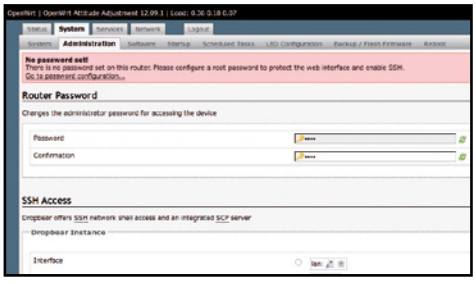
Cerchiamo, nell'interfaccia Web del router, la pagina dedicata all'aggiornamento del firmware (cioè del sistema operativo). In tale pagina ci verrà richiesto di fornire un file che contenga l'immagine: ovviamente, noi scegliamo il file che abbiamo trovato sul Win DVD-Rom.

3 Benvenuto, OpenWRT

Cliccando sul pulsante *Upgrade*, il router comincerà a caricare il firmware nella propria memoria interna. Dopo pochi minuti dovrebbe apparire a video il messaggio *Completed!*. Da questo momento in poi il router sarà accessibile all'indirizzo *192.168.1.1* e girerà con OpenWRT.

La configurazione del router

Installato il firmware OpenWRT, possiamo completare la procedura necessaria per stabilire una connessione con la rete Ninux (la guida dettagliata è su www.winmagazine.it/link/2653). Terminata questa fase, saremo on-line!

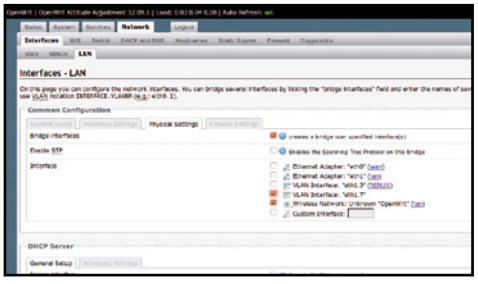


1 Una password nuova

Al primo accesso all'interfaccia Web di OpenWRT, tramite l'indirizzo *192.168.1.1*, inseriamo una nuova password. Questo è fondamentale per rendere attivi i vari servizi del sistema, ed è una misura di sicurezza per evitare che qualcuno usi un router non protetto da una password robusta.

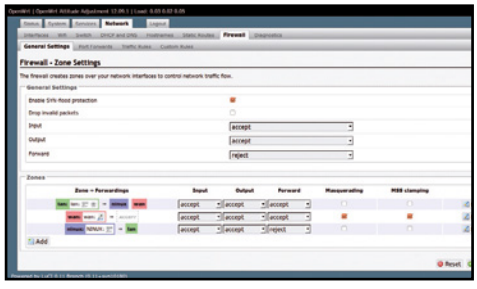
2 Apriamo le porte giuste

È necessario che una delle porte Ethernet del router sia riservata al cavo collegato all'antenna. Impostiamo la correlazione tra porte fisiche (del router) e virtuali (di OpenWRT) nel tab *Network/Switch*. Come si vede in figura, le VLAN dovranno essere la *3* e la *7*. Clicchiamo *Save*.



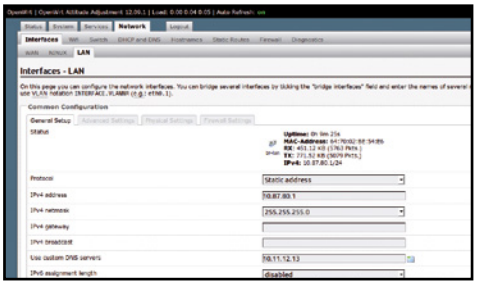
3 Un'altra interfaccia

Nella scheda *Network/Interfaces* creiamo una nuova interfaccia cliccando *Add new interface* e impostandola come in figura. Premendo *Submit* passeremo all'impostazione degli indirizzi IPv4 assegnatoci da Ninux. In *Physical settings* dovremo spuntare la voce *VLAN7*.



4 Anche nel firewall

In *Firewall settings* andiamo a creare una nuova firewall zone con lo stesso nome dell'interfaccia di rete (ninux nel nostro caso). Clicchiamo *Save* e procediamo. In *Network/Firewall/General Settings* impostiamo i forwarding come in figura (da LAN verso ninux e viceversa).

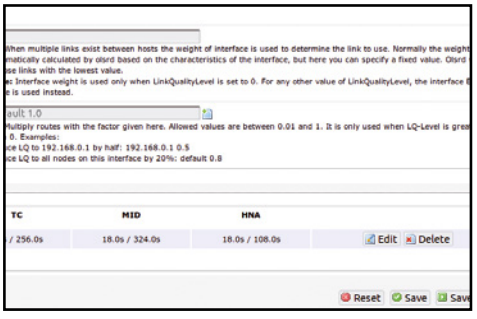


5 Il router e l'antenna

Clicchiamo *Save&Apply*, abbiamo quasi terminato. Ora possiamo collegare il cavo Ethernet dell'antenna alla porta che gli abbiamo riservato sul router. Se tutto va bene, l'antenna dovrebbe essere raggiungibile all'indirizzo *192.168.1.20*. Se così non fosse, ripetiamo la procedura.

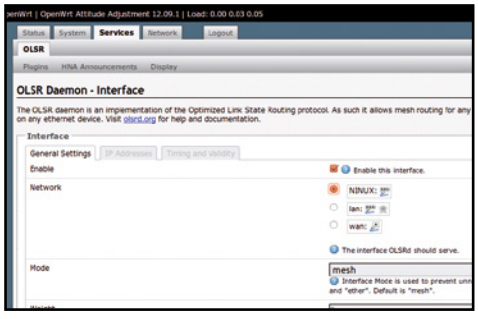
6 Un nuovo protocollo

Andiamo ora ad aprire la scheda *Services/OLSR*, che contiene le impostazioni del protocollo di routing di Ninux. È necessario, infatti, far sapere al nostro router come collegarsi alla rete Ninux, di modo che i pacchetti di rete possano trovare la strada giusta tra i vari nodi della rete.



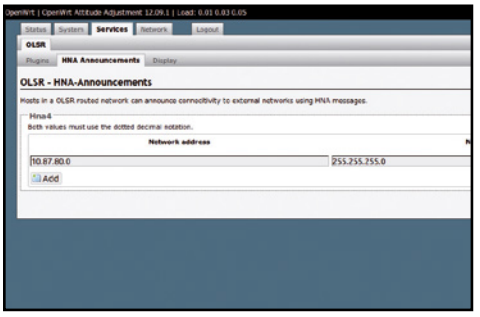
7 Le nostre interfacce

La scheda *General Settings* contiene diverse sezioni: a noi interessa quella chiamata *Interfaces*, che si trova in fondo alla pagina. Non vogliamo aggiungere altre interfacce, ma piuttosto modificare quella attualmente selezionata. Quindi clicchiamo sul pulsante *Edit*.



8 La rete in stile mesh

Apparirà una pagina per la modifica dell'interfaccia di connessione. Qui dobbiamo scegliere la voce *Ninux*. La modalità della rete deve essere mesh e, ovviamente, è necessaria la spunta all'opzione *Enable this interface*. A questo punto possiamo procedere cliccando *Save*.



9 La rete in stile mesh

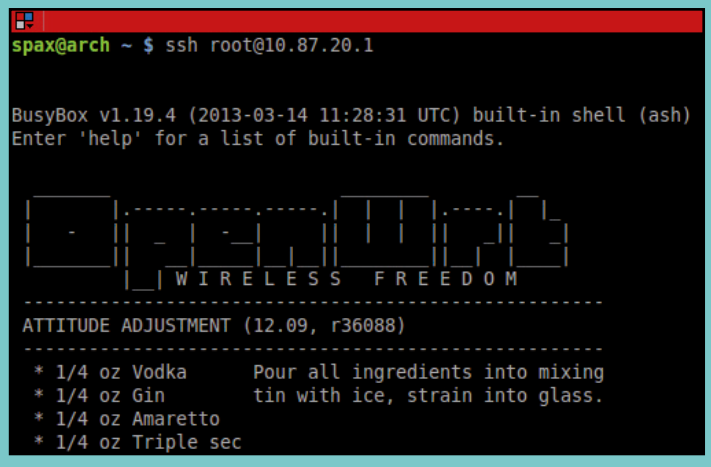
In *HNA Announcements*, sempre da *Services/OLSR*, clicchiamo *Add* e inseriamo uno degli IP forniti da Ninux (**Passo B9**). In particolare ci serve quello che termina con uno zero. Questo ci consentirà di far sapere all'intera rete che esistiamo e siamo on-line. Clicchiamo *Save & Apply* per confermare.

ABILITIAMO TUTTI I SERVIZI GRATUITI DELLA RETE NINUX

Attivando il plug-in Multicast DNS del protocollo di routing OLSR saremo in grado di far funzionare i servizi di rete in modo automatico grazie alla tecnologia ZeroConf. Per cominciare, colleghiamoci col browser all'interfaccia Web del router digitando ***192.168.1.1*** nella barra indirizzi e scegliamo la scheda ***Services/OLSR/Plugins***. Cerchiamo la voce ***olsrd_mdns.so.1.0.1***, spuntandola come ***Enabled***. Clicchiamo quindi sul pulsante ***Save&Apply***. Per maggiore sicurezza, avviamo il programma Putty (si può scaricare gratuitamente da www.winmagazine.it/link/2651) ed eseguiamo una connessione SSH al router dal prompt dei comandi. Ovviamente, indirizzo, nome utente, e password saranno gli stessi che utilizziamo per l'accesso tramite interfaccia Web. Appena otteniamo un prompt, possiamo digitare: ***vi /etc/config/olsrd***. In questo modo apparirà sullo schermo il contenuto del file di configurazione di OLSR. Scorriamo con la freccia verso il basso fino a trovare le righe:

config LoadPlugin
option library 'olsrd_mdns.so.1.0.1'
option NonOlsrIf 'lan'

Se esistono e sono identiche a queste, vuol dire che va tutto bene. Nel caso l'ultima parola non sia '***lan***', sarà sufficiente cancellare l'intera riga con il tasto ***Canc*** e poi riscriverla. Per farlo, si deve digitare il comando



:i seguito da ***Invio***. A quel punto è possibile digitare il testo corretto, terminandolo con la pressione del tasto ***Invio*** e poi ***Esc***. Per chiudere il file si deve digitare ***:wq***. Riavviamo il router per sicurezza: da ora, sarà possibile sfruttare i vari servizi offerti da Ninux.

IN PRATICA

RETI MESH WI-FI

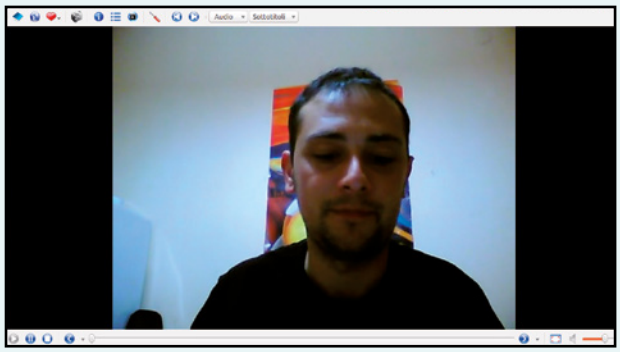
DIVERTIAMOCI A GIOCARE CON IL MULTIPLAYER ON-LINE

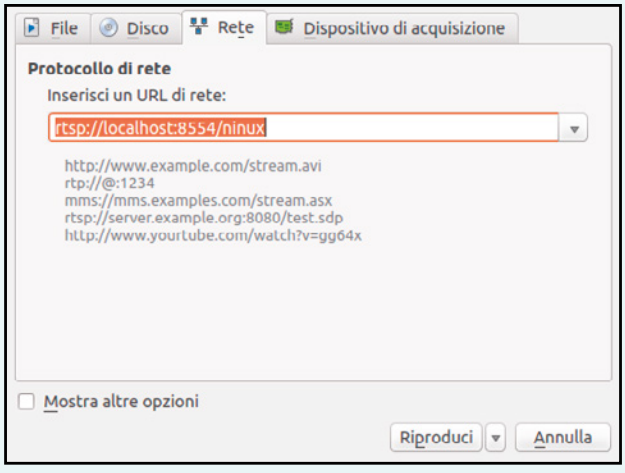
Terminata la fase di configurazione della rete Ninux, abbiamo iniziato a giocare al multiplayer di OpenArena. Dopo aver scaricato il gioco (www.winmagazine.it/link/2657) e installato sul PC abbiamo creato il server di gioco on-line dal menu ***Multiplayer*** cliccando sul pulsante ***Create***, per accedere alla schermata di creazione della partita. Abbiamo scelto il tipo di incontro da disputare. Alcune voci dell'elenco sono: ***Free for All*** (Tutti contro tutti), ***Team deathmatch*** (Incontro a squadre) e il classico ***Capture the Flag*** (Cattura la bandiera). Fatta la nostra scelta, abbiamo settato su ***On*** la voce ***Auto change map***, così da giocare tutte le mappe una dopo l'altra, oppure sceglierle personalmente selezionando una mappa dalla lista. Procediamo nella creazione del server cliccando su ***Next*** e accediamo all'ultima schermata. Ora lo schermo sostanzialmente è diviso in due parti. Nella metà di sinistra troviamo la voce per impostare l'abilità dei bot (giocatori virtuali comandati dal computer), il nostro nome preceduto dalla scritta Human e, nel caso di un incontro a squadre, il colore del team per cui combatteremo. Adesso ci viene chiesto di scegliere quanti slot (numero di giocatori) il nostro server può avere impostando su ***Open*** gli slot nella sezione ***human*** o nella sezione ***bot*** (indicando anche se questo giocatore deve appartenere alla squadra blue o red). Nella seconda metà dello schermo ci viene mostrata la mappa, la modalità scelta in precedenza e un menu composto da diverse voci tra le quali: ***Frag Limit*** (Limite di uccisioni per completare la partita), ***Time Limit*** (Limite di tempo), ***Friendly Fire*** (Fuoco Amico), ***All rockets*** (Solo lanciamissili) e infine ***Hostname*** (nome del server) che di default è settato su noname, ma al quale noi daremo un nome a piacere. Quando ci sentiamo pronti per iniziare possiamo cliccare su ***Fight*** e, una volta caricata la partita, invitare gli amici. Non ci resta che farli entrare nel nostro server. Dobbiamo innanzitutto comunicare loro l'indirizzo IP del PC (per esempio***: 10.87.200.228***). Poi, una volta entrati nel menu ***Multiplayer***, le nostre future vittime dovranno cliccare sul pulsante ***Specify***, che le inoltrerà alla schermata per l'inserimento dell'indirizzo da noi fornito. Indicato l'IP potranno cliccare su ***Fight*** e cominciare a giocare con noi!

IN PRATICA

VIDEO IN STREAMING CON NINUX

Grazie ai protocolli di comunicazione usati nella nostra nuova rete mesh possiamo anche costruire una Web TV o allestire un sistema di videochiamate ad alta velocità tra i singoli nodi. Come? Usando il player VLC potremo mandare in streaming il flusso audio/video proveniente dalla nostra Webcam verso gli altri nodi della rete. Avviamo VLC e apriamo il menu ***Media/Trasmetti***. Andiamo nella scheda ***Dispositivo di Acquisizione*** e selezioniamo i nostri input video e audio.Clicchiamo su ***Flusso*** e poi su ***Successivo*** per procedere oltre. Ora possiamo scegliere la destinazione dello streaming. Nella maggior parte dei casi andrà bene HTTP o RSTP. Clicchiamo su ***Aggiungi*** e si aprirà una nuova scheda dedicata alla nostra destinazione. Selezioniamo una porta e un percorso, che andranno poi a far parte del link del nostro streaming. Infine attiviamo la transcodifica del video. Non tutte funzioneranno con la nostra Webcam, quindi dovremo effettuare qualche prova. Una scelta "sicura " è quella ***MPEG2***. Avviamo lo streaming con ***Flusso***. Forniamo agli amici il link allo streaming, nella forma ***http://10.87.20.208:8080/ninux***, se abbiamo scelto HTTP come destinazione, porta di default e percorso /ninux. Aprendo il link con VLC, gli amici vedranno la nostra Webcam!





IN PRATICA

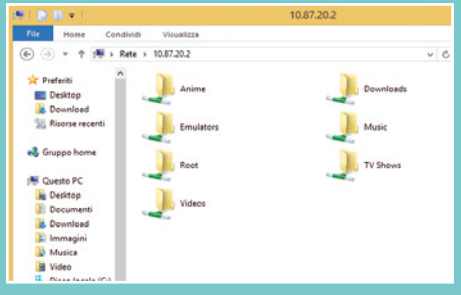
CHATTARE IN PRIVATO

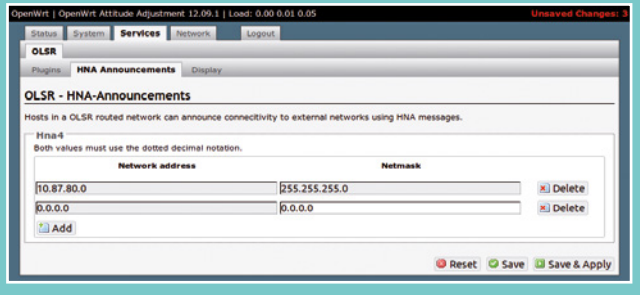
Installiamo sul PC il tool Pidgin (lo trovi sul Win DVD) per chattare in totale sicurezza e parlare con tutti gli altri nodi Ninux. Avviamo il programma: se è la prima volta, ci apparirà una schermata di benvenuto che consente la creazione di un nuovo account. Cliccando sul pulsante ***Aggiungi*** possiamo creare il nostro profilo. Gli unici dati richiesti sono il protocollo ed il nome utente. Il primo deve essere scelto dal menu a tendina e deve essere ***Bonjour.*** Il secondo può essere qualsiasi cosa vogliamo. Dopo avere eseguito l'accesso, vedremo automaticamente comparire gli altri nodi Ninux che stanno utilizzando un client compatibile all'interno della nostra lista. Ora possiamo chattare con chi vogliamo in modo sicuro e libero.

IN PRATICA

CONDIVIDIAMO FILE, CARTELLE E CONNESSIONE A INTERNET

Nella rete Ninux possiamo anche vedere e accedere automaticamente alle risorse condivise dagli altri utenti (le cartelle presenti in un NAS, ad esempio) e scaricare tutti i contenuti in esse archiviati. Se cerchiamo un nodo Ninux specifico e non lo troviamo nell'elenco delle risorse di rete, sarà sufficiente scrivere il suo indirizzo preceduto da "\\" nella barra degli indirizzi di ***Esplora Risorse***. Le nostre cartelle ***Documenti condivisi***, ***Musica condivisa*** ecc. sono automaticamente disponibili per gli altri utenti della rete Ninux. Per sicurezza, comunque, verifichiamo che i permessi di queste cartelle siano impostati, almeno in lettura, su ***Everyone***. Ci si può connettere a queste cartelle condivise anche da Mac OS o GNU/Linux grazie al protocollo ***Samba***, applicazione che simula la condivisione file di Windows. Se invece vogliamo condividere la connessione a Internet, possiamo tornare col browser sull'interfaccia Web del router, nella scheda ***Services/OLSR/HNA Announcements***. In questa pagina avevamo già inserito una riga durante l'installazione del plug-in ZeroConf: ora dobbiamo aggiungerne un'altra, impostando entrambi i campi all'indirizzo ***0.0.0.0***. Condividere la propria connessione ADSL è fondamentale per fornire agli altri nodi di Ninux che, magari, non hanno a disposizione una connessione al Web, la possibilità di uscire sulla rete mondiale. Volendo, grazie ad OpenWRT, sarà poi possibile, con strumenti avanzati come ***tc*** (traffic control) e front-end più amichevoli come ***qosscripts*** (disponibili nei repository di Ninux), limitare la banda condivisa mantenendo la connessione responsiva.





Le altre reti mesh disponibili

Oltre a Ninux esistono altri progetti di reti senza fili che permettono di scambiare dati tra PC e telefonini anche quando ci si trova in zone disagiate dove le normali infrastrutture di comunicazione non funzionano.

AIRCHAT: LA RETE MESH LIBERA USATA DA ANONYMOUS

Anonymous, il più noto gruppo di hacker del momento, non poteva certamente accontentarsi della normale rete Internet, troppo centralizzata e facile da controllare da parte di chi detiene il potere in un certo paese. Anche perché, essendo attivisti spesso politicamente impegnati, e responsabili di buona parte delle rivolte scoppiate nel medio oriente negli ultimi anni, non potevano fidarsi delle reti controllate dai governi dittatoriali che volevano rovesciare. Per questi motivi hanno sviluppato AirChat, una sorta di Ninux mobile, che consente lo scambio di messaggi e file tramite computer portatili anche in mezzo al deserto o sotto i bombardamenti. Il progetto richiede ancora una buona dose di lavoro per essere davvero alla portata di tutti: al momento è necessario avere una discreta dimestichezza con gli strumenti informatici per potersi assemblare una stazione mobile AirChat. Noi ci stiamo documentando per saperne di più su questo progetto. Nei prossimi numeri ci ritorneremo per analizzare in maggior dettaglio il suo funzionamento. Ad ogni modo, per chi volesse sperimentare, sul sito ufficiale (https://github.com/lulzlabs/AirChat) si trovano spiegazioni abbastanza dettagliate sia a proposito del lato software (cioè cosa si deve installare sul proprio computer), sia per quanto riguarda il lato hardware (cioè come assemblare l'apparato di ricetrasmissione wireless). In particolare, per quanto riguarda l'hardware, AirChat utilizza dei ricetrasmettitori UHF/VHF in modulazione di frequenza (praticamente la stessa tecnologia alla base delle trasmissioni televisive).

Cos'è: Rete mesh che sfrutta le onde radio per la comunicazione.

Come funziona: Basata sulla stessa tecnologia delle trasmissioni televisive, usa ricetrasmettitori UHF/VHF per le comunicazioni.

A cosa serve: Allo scambio di messaggi e file tramite PC portatili anche in mezzo al deserto o sotto i bombardamenti.

SERVAL: LA RETE MESH PER TELEFONARE SENZA SIM

Il progetto è stato sviluppato in Australia (www.servalproject.org), con la collaborazione della Croce Rossa Neozelandese, e mira a rendere possibili le chiamate vocali in qualsiasi parte del mondo, senza doversi basare sui satelliti e le antenne che oggi sono usate per i telefonini. L'impiego che la Croce Rossa ha in mente è destinato alle situazioni di emergenza come terremoti e uragani, casi in cui le prime cose a saltare sono proprio le telecomunicazioni, che invece sono fondamentali per coordinare i soccorsi e salvare più vite possibili. L'idea di base è praticamente la stessa della rete Ninux: si tratta, infatti, sempre di una rete mesh basata sul Wi-Fi, nella quale ogni utente costituisce un nodo e consente la comunicazione ad altri utenti. La connessione senza fili utilizzata ha il pregio di sfruttare l'hardware dei moderni smartphone (al momento l'app è disponibile solo per Android), che hanno sempre una scheda di rete wireless, e non richiede quindi l'acquisto di ulteriore strumentazione da parte degli utenti. Tuttavia, questo comporta alcuni problemi di campo: il Wi-Fi, infatti, ha un raggio piuttosto limitato. In realtà, già all'interno di una grande città sarebbe possibile telefonarsi usando questo sistema. Per le zone poco popolate, sono stati progettati dei ripetitori di segnale, che dispongono di un raggio di azione cento volte superiore a quello di una normale antenna Wi-Fi. Questi ripetitori sono, fondamentalmente, della scatolette che possono essere attaccate a palloni aerostatici oppure inseriti in gallerie nel sottosuolo. Grazie ad essi è teoricamente possibile costruire con poca spesa una rete di telefonia mobile completamente libera. Naturalmente, il problema di questi ripetitori è che, mentre tutti gli altri componenti della rete sono gratuiti, questi hanno un costo. In realtà, non si tratta nemmeno di un prezzo eccessivamente elevato: sarebbero sufficienti 300.000 dollari per lanciare sul mercato un prodotto "pronto all'uso" con un costo ridotto al minimo.

COME FUNZIONA SERVAL Scarichiamo, installiamo e avviamo l'app Serval. Indichiamo il nostro numero di telefono e un nickname confermando con OK. Tocchiamo Switch ON per connetterci ad una rete Wi-Fi disponibile e identificare altri dispositivi nei dintorni. Tappiamo Call per effettuare la nostra prima telefonata.

Cos'è: Rete che usa la tecnologia mobile per la comunicazione.

Come funziona: Sfrutta la scheda Wi-Fi degli smartphone Android per creare una rete di comunicazione con altri dispositivi.

A cosa serve: A realizzare un sistema di comunicazione in zone colpite da terremoti, alluvioni e altre calamità naturali.

Trucca il tuo router e naviga gratis!

Lo accendi e senza inutili configurazioni accede a tutte le reti Wi-Fi... anche fino a 10km di distanza

Fino ad un paio di anni fa, le numerose connessioni quotidiane a Internet venivano rappresentate da un inestricabile groviglio di cavi che avvolgevano l'intero pianeta. Oggi la situazione è radicalmente cambiata: tranne in alcuni specifici casi, infatti, tutte le connessioni avvengono ormai mediante reti wireless e gli inutili ed ingombranti cavi sono stati definitivamente mandati in soffitta. Una grande comodità per noi utenti che, anche in mobilità con il nostro smartphone e il tablet, oltre che con un normale computer desktop, possiamo rimanere sempre connessi ovunque ci troviamo.

Attenti a quel router

Peccato, però, che l'eterea natura dei collegamenti Wi-Fi, per quanto pratici, veloci e sempre più efficienti, abbia portato con sé nuovi e più seri pericoli relativi alla protezione delle nostre comunicazioni su Internet. Quando le connessioni avvenivano via cavo la vita degli spioni digitali era leggermente più complicata: per riuscire ad origliare le altrui conversazioni on-line, infatti, avrebbero dovuto prima intrufolarsi in un server e solo successivamente sniffare il traffico dati che passava sui dati alla ricerca di informazioni e dati personali di ogni tipo. Adesso, per i novelli pirati informatici è tutto più semplice: basta avere un computer portatile (ma in alcuni casi va benissimo anche un tablet o addirittura un telefonino) dotato di antenna Wi-Fi per intercettare migliaia di connessioni a Internet! I pirati, però, non sono soliti fare le cose in maniera approssimativa: ecco quindi che hanno trovato il modo di utilizzare a loro vantaggio un particolare router wireless per bucare e intrufolarsi nelle reti di ignare vittime che abitano anche a decine di chilometri di distanza da loro. Il nome di questo "gingillo" è Beini CP-150JP: a guardarlo bene sembra un normalissimo router Wi-Fi, se non fosse che il suo "cuore" è una mini distribuzione Linux che integra e automatizza tutti i tool necessari per il crack delle reti Wi-Fi. Se a questo si aggiunge anche la presenza di una porta USB a cui collegare un hard disk contenete diversi dizionari di password pronte per essere utilizzate in attacchi di tipo brute force, si capisce perché il dispositivo stia andando letteralmente a ruba tra i pirati informatici e gli spioni digitali.

Attacchi di ogni genere

I cacciatori di dati personali, comunque, hanno anche la possibilità di intercettare decine di connessioni wireless a Internet restando comodamente seduto sulla panchina di un corso pieno di gente. E senza neanche spendere un centesimo! Certo, non è semplice come bersi un drink ad un bar, ma con i moderni strumenti software non servono più competenze tecniche particolarmente avanzate: in alcuni casi, addirittura, anche uno sprovveduto potrebbe riuscire ad intercettare una connessione Wi-Fi e decifrarne tutti i dati in transito. Negli ultimi tempi, sui canali underground della Rete ha riscosso un enorme successo una particolare distribuzione Linux molto amata dai pirati informatici e dai cacciatori di dati personali. E il perché è presto detto. XiaoPan OS Linux, questo il suo nome, include tutti gli strumenti e i plug-in necessari per crackare qualsiasi rete Wi-Fi. In alcuni casi, poi, gli sviluppatori della distribuzione hanno realizzato anche delle interfacce grafiche per alcuni tool storici di cracking come AirCrack che ne hanno permesso di semplificare l'utilizzo riducendolo a pochi clic del mouse. Protocolli e interfacce di rete, codici binari e algoritmi di codifica sono ormai solo un lontano ricordo. Come se non bastasse, si sono anche presi il lusso dell'ironia chiamando questi tool con nomi a dir poco irriverenti. Il più "divertente"? Si chiama Feeding Bottle, che in italiano significa biberon. Ci sarebbe da ridere, se non fosse che grazie a questo strumento bastano un paio di clic del mouse per mettere in chiaro anche le chiavi WPA dei nostri router Wi-Fi ritenute finora estremamente sicure!

IL GRIMALDELLO DELLE PASSWORD

Con un tool come Ufo Wardriving i pirati hanno gioco facile a mettere in chiaro le password predefinite dei router forniti dai principali provider. Tutorial a pag. 22

LE SUPER ANTENNE

I pirati non si accontentano di violare le reti Wi-Fi dei vicini di casa: con l'antenna Kasens-990WG riescono a bucare reti wireless fino a dieci chilometri di distanza! Tutorial a pag. 22

ATTACCHI A FORZA BRUTA...

... ma portati a termine usando il biberon! Si chiama proprio Feeding Bottle (biberon in italiano) il tool che rende semplicissimi anche gli attacchi di tipo brute force Tutorial a pag.22

Le nostre contromisure

Per fortuna, le armi di difesa per le nostre martoriate reti Wi-Fi non mancano! La prima è il buon senso. Se ci colleghiamo a Internet dallo smartphone o dal tablet, ad esempio, installiamo almeno un antivirus in versione mobile capace di segnalarci eventuali anomalie e comunque evitiamo di usare la connettività wireless per usare i servizi di home banking o per trasferire dati sensibili. Se proprio abbiamo necessità di farlo, usiamo almeno la rete 3G del dispositivo, molto più difficile da intercettare.

Un'altra soluzione decisamente più raffinata consiste, invece, nell'allestire una finta rete Wi-Fi aperta da usare come esca per lo spione di turno: si chiama honeypot e, proprio come un vasetto di miele, serve per attirare il malintenzionato che così finisce invischiato nella nostra astuta trappola. A quel punto, possiamo analizzarne le mosse e bloccare i suoi tentativi di intrusione nella rete prima che sia troppo tardi. Ma non perdiamo altro tempo: nelle pagine seguenti analizzeremo le mosse dei pirati per prendere le nostre giuste contromisure.

ATTACCO VIA ROUTER

Con il router Beini CP-150JP e un dizionario di password, i pirati riescono a bucare qualsiasi rete senza fili in pochi clic. Tutorial a pag. 18

OCCHIO AL WPS

Con Inflator qualunque dispositivo collegato alla nostra rete wireless mediante WPS è a rischio attacco e potrebbe trasformarsi in una porta di accesso a tutta la rete
Tutorial a pag. 24

UNA TRAPPOLA PER I PIRATI

Configurando una finta rete wireless "aperta" possiamo attirare in trappola gli intrusi e scoprire quali sono le loro intenzioni per bloccarli e renderli innocui prima che facciano danni seri
Tutorial a pag. 26

NON È IL SOLITO ROUTER

Il Beini CP-150JP sembra un normalissimo router Wi-Fi. A differenza di altri, però non ha un firmware di controllo, ma una mini distribuzione Linux preinstallata che integra e automatizza tutti i tool necessari per il crack delle reti wireless. In questo modo, il dispositivo è in grado di sferrare un attacco di tipo brute force in piena autonomia, sfruttando un dizionario interno già precaricato nella sua memoria flash. Qualora non fosse sufficiente, il pirata può comunque utilizzare un dizionario esterno (il Web pullula di "password list" che contengono svariati GB di combinazioni alfanumeriche) collegando una pendrive o un disco rigido esterno all'ingresso USB presente sul device.

1 DISPLAY
Da questo piccolo display i pirati possono configurare il Beini CP-150JP, senza neanche collegarlo ad un computer

2 INVIO
Questo pulsante a sfioramento permette di confermare le impostazioni scelte dal pirata

3 ANTENNA
Qui è possibile collegare l'antenna fornita in dotazione con il router o una potenziata per estenderne in raggio d'azione

4 USB
A questa porta USB il pirata può collegare una pendrive o un hard disk esterno in cui ha memorizzato i dizionari con le password

ATTENZIONE!!!

Ricordiamo che violare le reti altrui è un reato perseguibile penalmente dalla legge italiana (art. 615-ter del codice penale).

Le procedure da noi descritte pertanto devono essere utilizzate esclusivamente al fine di testare la sicurezza della propria connessione Wi-Fi e, intervenendo sulle impostazioni dei dispositivi, renderla invulnerabile a qualsiasi attacco esterno.

Attenti a quel router Wi-Fi!

Cosa ci occorre

20 MIN. DIFFICILE

ROUTER WI-FI
BEINI CP-150JP
Quanto costa: € 49,70
Sito Internet:
www.aliexpress.com

Si chiama Beini CP-150JP ed è il preferito dai pirati: perché? In pochi clic permette a chiunque di bucare qualsiasi rete senza fili

A guardarlo sembra un semplice router. Uno di quelli senza pretese che, al massimo, consentono di condividere la connessione a Internet con uno o due PC. Eppure, dietro al suo aspetto da "pivello" si cela un lato oscuro... talmente oscuro da catturare l'attenzione dei pirati di tutto il mondo. Stiamo parlando del Beini CP-150JP un piccolo device equipaggiato con un'antenna esterna, una porta USB e un display che ha una particolarità che lo rende abbastanza invitante agli occhi dei malintenzionati: è infatti in grado di bucare, in piena autonomia (o quasi), qualsiasi rete senza fili, indipendentemente se essa sia protetta da una chiave WEP o WPA. In effetti il pezzo forte del Beini CP-150JP è il software che batte al suo interno, una mini distribuzione GNU/Linux che integra e automatizza tutti i tool necessari per il crack delle reti Wi-Fi. L'attacco, di tipo brute force, viene sferrato, come già detto, in piena autonomia, sfruttando un dizionario interno (già precaricato nella memoria flash del router). Qualora non fosse sufficiente, il pirata può comunque utilizzare il suo dizionario personale (il Web pullula di "password list" che contengono svariati GB di combinazioni alfanumeriche).

È facile, ma illegale!

Come? Semplicemente collegando una pendrive o un disco rigido esterno all'ingresso USB presente sul device. Ma è davvero così facile bucare una rete Wi-Fi? Per verificarlo ne abbiamo allestito una serie di test nei nostri laboratori proteggendola con una chiave WPA che abbiamo modificato diverse volte per renderla man mano più complessa. Dopodiché, abbiamo iniziato a sferrare gli attacchi con il Beini, verificando una facilità d'uso del router davvero disarmante: le password più banali, quelle composte ad esempio dalla nostra data di nascita, sono state scovate in pochissimo tempo! Un'occasione in più per ricordare che con un minimo di attenzione e utilizzando password "robuste" possiamo ottenere un livello di sicurezza sufficientemente elevato. Se siamo curiosi di testare la sicurezza della nostra rete Wi-Fi, possiamo mettere in atto quanto descritto nell'articolo per tentare di violare il router; purché sia quest'ultimo sia la linea ADSL siano di nostra proprietà! È bene ricordare, infatti, che accedere alle reti Wi-Fi altrui senza permesso è un reato perseguito penalmente dalla legge italiana (art.615-ter del Codice Penale) che, tra le pene inflitte, contempla anche il carcere!

Si controlla dal menu

1 Seguendo le orme dei pirati, accendiamo il Beini CP-150JP e attendiamo affinché il boot venga completato. Al termine, appare un menu composto da quattro icone: spostiamoci sulla seconda utilizzando le frecce poste in basso a sinistra del display e confermiamo con *Invio*.

La chiave è WEP o WPA?

2 Appare la schermata *AP TYPE*: è questo il primo passo che porta al crack della rete Wi-Fi bersaglio. Utilizzando sempre il pulsante che raffigura due frecce, spostiamoci sul tipo di protezione applicata alla rete senza fili da bucare (ad esempio *WPA*) e confermiamo con *Invio*.

Ecco la rete bersaglio

3 Inizia la scansione delle reti disponibili nei paraggi. L'antenna esterna (fornita in dotazione) è molto potente ed è in grado di ricevere il segnale di reti Wi-Fi distanti anche diverse centinaia di metri. Selezioniamo la rete bersaglio (nel nostro caso *Tux-Fi*) e confermiamo con *Invio*.

Attacco di rete in corso

4 Inizia il crack della rete Wi-Fi appena selezionata: a questo punto, il router comincia ad inviare dei pacchetti all'hot spot da bucare. Se sulla rete bersaglio c'è un minimo di traffico Web, in pochi secondi il Beini CP-150JP sarà in grado di sferrare il suo attacco finale!

C'è sia il dizionario interno...

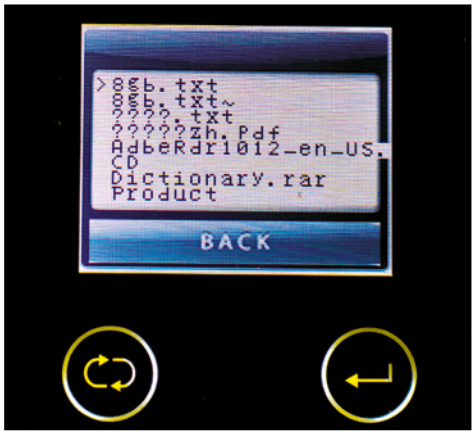
5 Se l'invio dei pacchetti ha avuto un esito positivo, il router preferito dal pirata comincia immediatamente a tentare il login utilizzando delle password predefinite presenti nella sua memoria interna: un piccolo dizionario composto da un centinaio di parole di uso comune.

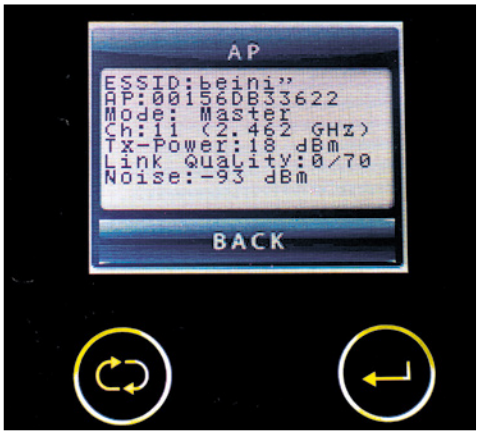
... che quello esterno!

6 Per ovvie ragioni, il più delle volte le chiavi presenti nella memoria interna del Beini CP-150JP non sono sufficienti. Appare dunque una nuova schermata nella quale viene chiesto se utilizzare un disco USB collegato al device. Confermiamo con *Yes*.

La chiavetta "magica"

7 A questo punto, tiriamo fuori dal cassetto una pendrive nel quale è presente un buon dizionario (scaricato in precedenza dal Web) e colleghiamola all'ingresso USB posto sul lato del router (proprio accanto all'interfaccia Ethernet e al connettore d'alimentazione).





Basta selezionare il file giusto

8 Sul display del Beini CP-150JP appare l'elenco dei file presenti all'interno della pendrive USB che abbiamo appena collegato al device. Non ci rimane dunque che selezionare il file dizionario (nel nostro caso *8gb.txt*) e confermare premendo il tasto *Invio*.

La rete è stata bucata!

9 Se la password viene scovata (potrebbero passare ore o, addirittura, settimane) sul display del router appare un nuovo menu con due icone. Selezionando la prima, effettuiamo una connessione definitiva con la rete Wi-Fi bersaglio. Ovviamente, decidiamo di optare per questa scelta.

Missione compiuta

10 Viene attivato automaticamente un nuovo Access Point, nominato *Beini*, privo di ogni protezione e grazie al quale potremo navigare da tutti i device che abbiamo in casa (PC, smartphone, tablet ecc.). Almeno fino a quando non decideremo di cambiare password...

Reti Wi-Fi crackate fino a 10 km

Alla scoperta delle nuove distribuzioni create per scardinare qualsiasi rete wireless: bastano davvero un paio di clic per farlo!

Nessuno, ormai, rinuncerebbe più ad un collegamento a Internet senza fili: la tecnologia Wi-Fi è talmente diffusa che molte persone si ritrovano in casa un router wireless senza nemmeno saperlo. È il caso degli anziani, che accettano di passare al VoIP per le telefonate senza essere interessati a Internet: il gestore telefonico fornisce loro un router che, ovviamente, ha tra le varie funzioni anche il Wi-Fi. Ma questo è comunque soltanto un esempio. Praticamente, tutto quel che facciamo sul Web, come visitare i social network, controllare il conto corrente bancario, leggere la posta elettronica e acquistare dagli store on-line, passa attraverso queste scatolette nascoste in qualche punto della casa o dell'ufficio. Chi riesce a entrare nella nostra rete Wi-Fi, quindi, non soltanto può scroccarci la connessione ADSL, ma di fatto avrà accesso a tutta la nostra vita privata!

Attacchi più semplici

Fatta questa premessa, è lecito porsi una domanda: quanto è sicura questa tecnologia? Fino a poco tempo fa i rischi che potevamo correre erano abbastanza limitati. Per attaccare il nostro router, infatti, un pirata doveva trovarsi fisicamente vicino a noi (quindi, un ragazzino posteggiato sotto casa col notebook sulle ginocchia poteva destare qualche sospetto...); inoltre, erano richieste competenze tecniche non alla portata di tutti (la suite AirCrack, ad esempio, usata per crackare le reti Wi-Fi, funziona soltanto a riga di comando nella shell Linux). Oggi, è tutto cambiato! I pirati possono acquistare a poche decine di euro antenne Wi-Fi potentissime con le quali riescono a vedere le reti senza fili di un intero isolato (i tempi del "wardriving" in giro col notebook sono ormai finiti)! E non solo: non devono nemmeno essere degli esperti di Linux!

Il mercato nero dei pirati

Attaccare una rete Wi-Fi è infatti diventata un'operazione tutto sommato semplice e per portarla a termine non servono neanche strumenti fantascientifici. Innanzitutto, un eventuale malintenzionato deve procurarsi un notebook per avvicinarsi il più possibile alla vittima (a meno che non si disponga di un'antenna Wi-Fi potenziata), un adattatore wireless (va benissimo quello integrato nel notebook o su chiavetta USB), una pendrive da 4 GB (per fare il boot da USB di XiaoPan OS PRO), alcuni particolari file di testo (i cosiddetti "dizionari") con dentro le password più comuni (si scaricano da Internet o si possono creare ad hoc col PC) e un hard disk esterno (sul quale archiviare i dizionari, che possono pesare anche svariati GB). Dal punto di vista software, invece, il malintenzionato può utilizzare uno dei nuovi sistemi operativi apparsi in Rete come XiaoPan OS Pro e Beini: entrambi dotati di semplici interfacce grafiche, che consentono anche ad un bambino di scardinare qualsiasi rete Wi-Fi.

È tutto integrato

Ad esempio, grazie al tool integrato Ufo Wardriving, permette di mettere in chiaro in un batter di ciglia le password predefinite dei router Wi-Fi forniti in comodato d'uso dai provider come Alice, Fastweb e Infostrada.

ECCO COME ABBIAMO SIMULATO UN ATTACCO ALLA NOSTRA RETE WI-FI

Le tecniche descritte in questa inchiesta sono state applicate a router di nostra proprietà. Nello specifico abbiamo eseguito un test "a doppio cieco": una squadra si è occupata dell'allestimento delle reti Wi-Fi con diversi tipi di sicurezza (WEP, WPA/WPA2), mentre l'altra squadra ha cercato di forzarle utilizzando antenne potenziate (e non) e le nuove distribuzioni Linux dedicate al crack del Wi-Fi. Ovviamente, nessuna delle due squadre sapeva cosa stesse facendo l'altra (per evitare di partire in qualche modo avvantaggiati). Questo simula la situazione tipica di un attacco reale, perché di solito pirati e vittime non si conoscono. Il risultato? Se fino a qualche anno fa era abbastanza complicato reperire e utilizzare gli strumenti necessari per penetrare in una rete Wi-Fi protetta, oggi è quasi banale. Se sei curioso di testare la sicurezza della tua rete Wi-Fi, puoi mettere in atto quando descritto nell'articolo per tentare di violare il tuo router; purché sia quest'ultimo sia la linea ADSL siano di tua proprietà! È bene ricordare, infatti, che accedere alle reti Wi-Fi altrui senza permesso è un reato perseguito penalmente dalla legge italiana (art.615-ter del Codice Penale) che, tra le pene inflitte, contempla anche il carcere!

I DIZIONARI CON LE PASSWORD PER ATTACCHI DI TIPO "FORZA BRUTA"

Un attacco a dizionario consiste nel provare tutte le possibili password per accedere a una rete Wi-Fi, utilizzando parole di senso compiuto (che le persone usano per ricordarle più facilmente). Un attacco di tipo brute force, invece, viene eseguito provando tutte le combinazioni di lettere, numeri e simboli possibili, a prescindere dal fatto che abbiano senso o meno. Il vantaggio del brute force è che, prendendo in considerazione tutte le combinazioni possibili, l'attacco avrà certamente successo, mentre lo svantaggio è dato dalla grande quantità di tempo necessario a compiere un attacco di questo tipo. Tuttavia, gli attacchi a dizionario e quelli brute force sono praticamente la stessa cosa: cambia soltanto il dizionario utilizzato, che nel primo caso contiene solo parole di senso compiuto, nel secondo qualsiasi combinazione di caratteri. Per l'occasione abbiamo sviluppato un programma chiamato ***bf-words*** (www.winmagazine.it/link/2951) che costruisce dizionari per il brute force. Utilizzarlo è semplice: basta estrarre il file ZIP in una cartella ed entrare in essa con il ***Prompt dei comandi***. Poi, si può dare un comando del tipo

bf-words.exe 1 5 q qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM1234567890-_.>> temp.txt

per registrare nel file temp.txt (che copieremo sull'hard disk esterno) tutte le combinazioni possibili dei simboli compresi la q e il . indicati nel comando) che abbiano una lunghezza da 1 a 5 caratteri, cominciando con la lettera q. Il terzo parametro (la lettera q) consente di cominciare da una combinazione precisa. La prima combinazione è data dalla prima lettera (in questo caso q). Questo argomento è utile per non dover ricominciare daccapo. Se, per esempio, abbiamo dovuto fermare il comando precedente prima che fosse terminato, e l'ultima combinazione prodotta è i7rj0, possiamo riprendere da dove ci siamo fermati dando il comando:

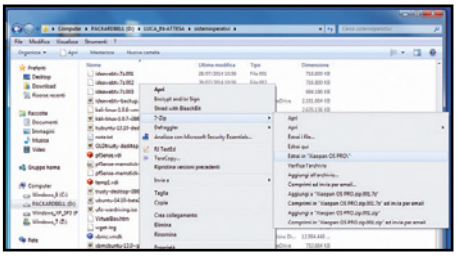
bf-words.exe 1 5 i7rj0 qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM1234567890-_.>> temp.txt

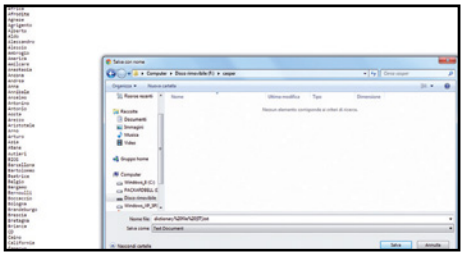
A seconda della velocità del PC su cui eseguiamo bf-words, potrebbero essere necessarie un paio di ore per calcolare tutte le combinazioni possibili di così tanti caratteri. Un comando più rapido e molto utile può essere: ***bf-words.exe 1 10 0 1234567890-./ >> temp.tx***t. Infatti, tutte le combinazioni lunghe fino a dieci caratteri basate s ulle cifre e sui pochi simboli di base rappresentano qualsiasi possibile data. È molto utile perché spesso le persone scelgono come password la propria data di nascita, che può essere scritta nel formato ***01011970, 010170, 1/01/1970, 01-01-70*** e così via.

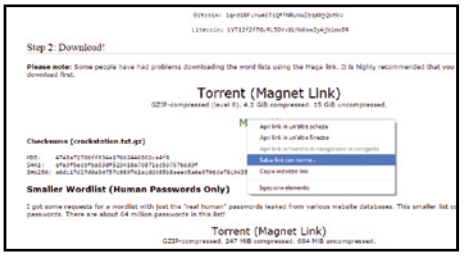
Per farlo, vengono utilizzati i cosiddetti "Magic Numbers", cioè dei numeri che mettono in relazione il nome (SSID) della rete e l'identificativo MAC Address del router, due informazioni che variano da provider a provider e da un modello di router a un altro. Nella dotazione software di XiaoPan non poteva mancare una versione ad hoc di AirCrack: la complessità di questo "grimaldello" delle chiavi di accesso WPA2 di una rete wireless viene di fatto annullata grazie all'interfaccia grafica Feeding Bottle (biberon in italiano) che ne semplifica l'utilizzo. E come se non bastasse, XiaoPan OS Pro può funzionare da chiavetta USB, senza dover installare nulla. Pazzesco! Ma scopriamone di più con la nostra inchiesta esclusiva.

A L'occorrente per un attacco

La squadra attrezzata per l'attacco ha già tutti gli strumenti che servono per crackare le reti Wi-Fi e quello che gli manca... lo scarica gratis! Ecco come procurarsi XiaoPan OS Pro e i dizionari con le password.







1 Funziona tutto da USB

Innanzitutto, scarichiamo i tre file ZIP di Xiaopan OS PRO (dal Win DVD-Rom) ed estraiamo il file *Xiaopan OS PRO.zip.001* per ricomporre l'archivio. Otterremo la ISO da scrivere su pendrive con UNetbootin (sezione ***Speciali*** del Win DVD-Rom): indichiamo il percorso della ISO, l'unità della pendrive collegata al PC e premiamo ***OK***. Al termine eseguiamo il boot del PC dalla chiavetta USB.

2 Un dizionario in italiano

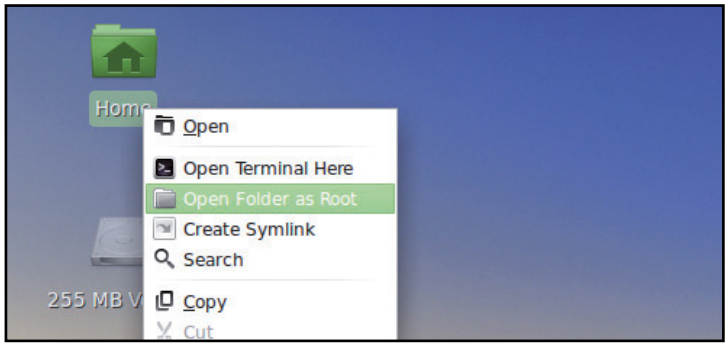
Per crackare le chiavi WPA usiamo l'attacco a dizionario: occorre un elenco di possibili password da provare durante le fasi di crack. È possibile scaricarne uno in lingua italiana dal sito www.winmagazine.it/link/2953 e salvarlo sul disco USB. Si tratta di un semplice file TXT leggibile con il ***Blocco Note***; ma essendo molto grande bloccherebbe Windows, quindi evitiamo di farlo!

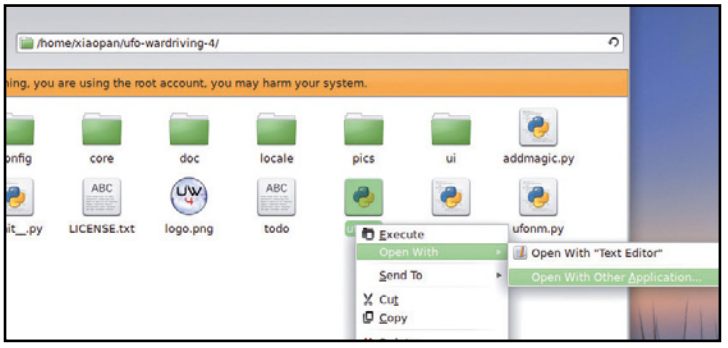
3 Le chiavi non bastano mai

Il dizionario con le parole più comuni in lingua italiana potrebbe non essere sufficiente per portare a termine l'attacco. Conviene quindi dotarsi di altri dizionari più completi come www.winmagazine.it/link/2954 e www.winmagazine.it/link/2955. Questi file pesano rispettivamente 15 GB e 33 GB, quindi conviene scaricarli tramite i link BitTorrent per poi copiarli sull'hard disk esterno.

Router & provider: WPA sgamate!

I router degli operatori ADSL usano password predefinite, ma l'algoritmo che le genera è stato scoperto dai pirati... Con il tool Ufo Wardriving integrato in XiaoPan OS Pro si crackano in 2 secondi netti!



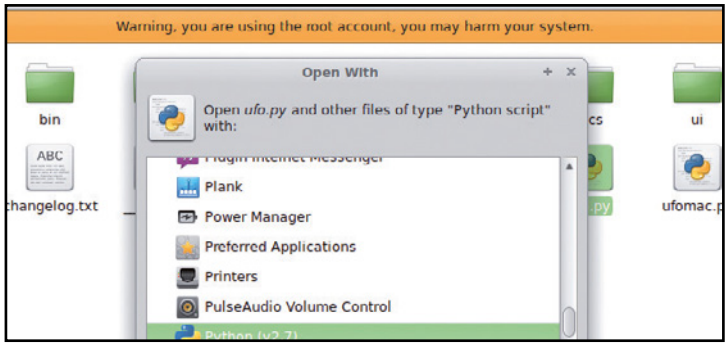


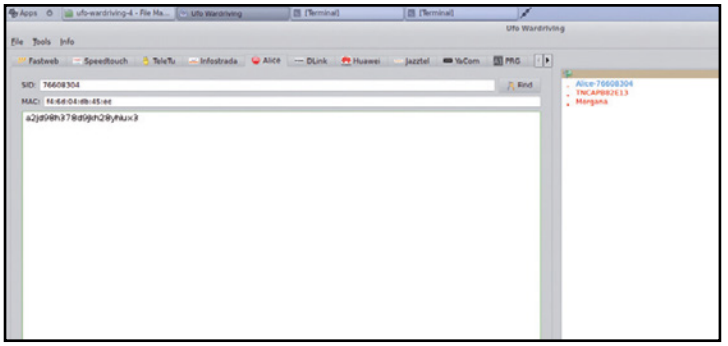
1 Lavorare come amministratore

Il programma Ufo Wardriving non è presente nel menu delle applicazioni di XiaoPan, ma si trova nella cartella *Home*. Occorre però aprirla con i privilegi di root, perché altrimenti il programma non avrà accesso alla scheda Wi-Fi. Clicchiamo quindi sulla cartella *Home* col tasto destro del mouse e scegliamo la voce *Open folder as Root*.

2 Un semplice script…

Verrà richiesta la password di root di Xiaopan: digitiamo *rocksolid*. Quando il gestore dei file si apre, entriamo nella cartella *ufo-wardriving-4*. Il programma non può essere avviato con un semplice doppio clic perché non è un vero eseguibile. Clicchiamo quindi col tasto destro del mouse sul file *ufo.py* e scegliamo la voce di menu *Open with/Open With Other Application*.





3 … pronto all'uso

Siccome si tratta di uno script Python, dobbiamo aprirlo con l'apposito interprete. Quando si apre la finestra per selezionare il programma da usare, scegliamo *Python (v2.7)*. È importante selezionare la versione 2.7 e non la 3, perché Ufo Wardriving integrato in XiaoPan OS Pro non è compatibile con la versione più recente del famoso linguaggio di programmazione.

4 Scansione completata

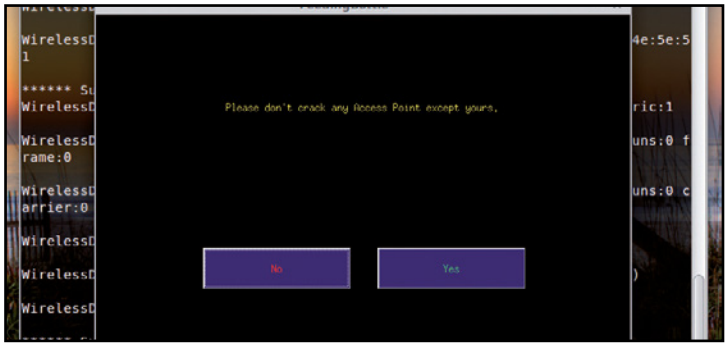
Quando il programma Ufo Wardriving si apre, basta premere i tasti *Ctrl+S* per far apparire lo scanner. Nella lista verranno presentate tutte le reti Wi-Fi identificate: un semplice doppio clic sulla rete vittima (nel nostro esempio abbiamo testato un router Alice) avvierà il calcolo della password di default, che comparirà nella casella di testo posizionata a sinistra.

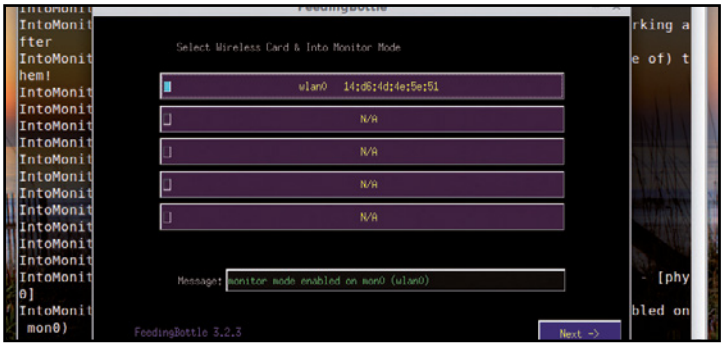
SUPER ANTENNE WIRELESS DA 15 EURO

Se un pirata vuole crackare una rete Wi-Fi deve trovarsi nelle vicinanze del router. Esistono però delle antenne ad alta potenza, come la Kasens-990WG (www.winmagazine.it/link/2956), che costa appena 15 euro ma consente di raggiungere molti più router fino a una decina di chilometri di distanza (in situazioni ottimali). Si tratta di una normale antenna Wi-Fi in standard n (basata sul chip Ralink RT3070), ma con un sistema di amplificazione (60 dBi) del segnale decisamente migliore di quello adottato per le antenne Wi-Fi integrate nei PC. Attenzione, però: il limite, in Europa, è di 20 dBm. I dBm totali vengono calcolati come somma tra i dBm puri dell'antenna più i dBi di amplificazione. Per esempio, una antenna con 17 dBm e 2 dBi ha una potenza totale di 19 dBm. Ciò significa che la Kasens-990WG, a prescindere dalla sua potenza di base, ha già un'amplificazione tre volte superiore al massimo consentito. Il suo utilizzo in Italia è quindi illegale (non il possesso, naturalmente). La potenza di questa antenna, in Watt, è più o meno di 6000 mW (6 Watt) e quindi potrebbe risultare persino pericolosa per la salute. Per dare un'idea, questa antenna è un centinaio di volte meno potente dell'emettitore di un normale forno microonde. Si tratta sempre di radiazioni che appartengono allo spettro infrarosso e che provocano quindi un'elevata vibrazione delle molecole d'acqua scaldando dall'interno qualsiasi cosa contengano.

Crackare il Wi-Fi col biberon

In XiaoPan OS Pro esiste anche un tool che consentirebbe persino a un poppante di eseguire attacchi dizionari o brute force! Bastano un paio di clic del mouse e un po' di pazienza per forzare qualsiasi chiave WPA.



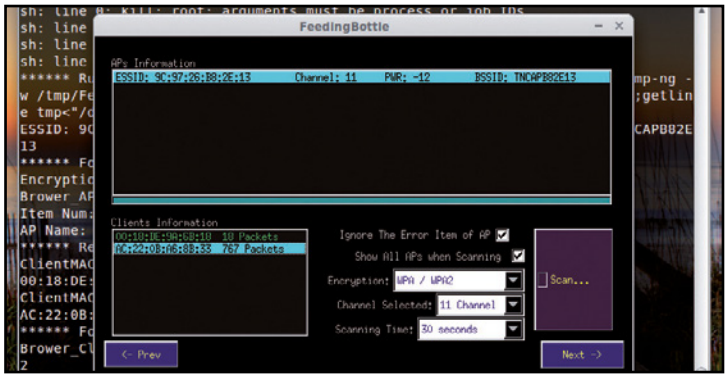


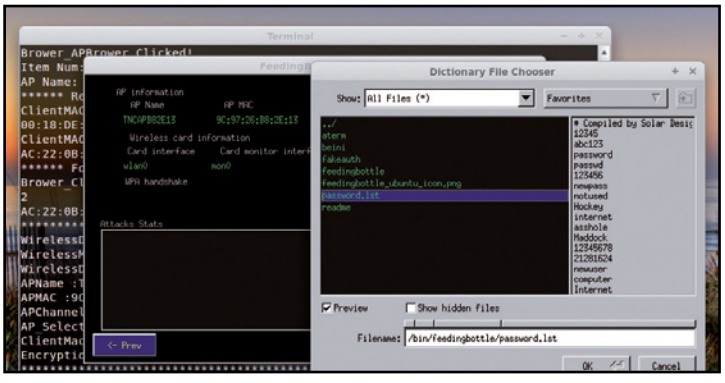
1 Un'app per il crack

Feeding Bottle (biberon in italiano) è un'interfaccia grafica del tool di cracking AirCrack (menu *Applicazioni/Internet* di XiaoPan). Per avviarlo sono richiesti i privilegi di root: clicchiamo sul suo nome e nella schermata che appare digitiamo la password di root: quella di Xiaopan è *rocksolid*. Alla prima domanda del programma rispondiamo *Yes*.

2 Un monitor per l'attacco

Indichiamo quindi l'interfaccia di rete da utilizzare. Selezioniamo la scheda Wi-Fi che abbiamo inserito nel PC (presumibilmente WLAN0) e attendiamo che nella casella *Messages* appaia la scritta *monitor mode enabled on mon0 (wlan0)*. La scheda deve infatti essere attivata in modalità monitor per poter eseguire l'attacco.



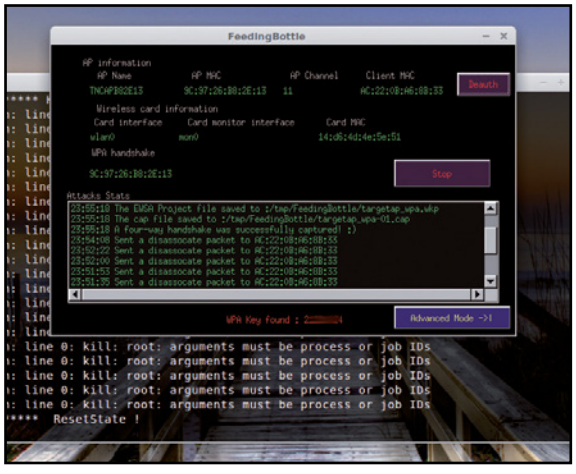


3 Alla ricerca delle reti Wi-Fi

A questo punto eseguiamo una scansione delle reti disponibili: prima selezioniamo il tipo di cifratura (*WPA/WPA2* è oggi la più comune) e poi premiamo *Scan*. Il programma cercherà tutte le reti a portata della loro antenna, indicandole nell'apposita lista. Per ogni rete vengono indicati anche i client connessi: selezioniamo quindi con un clic il client con più pacchetti (*packets*).

4 Ecco il dizionario

Selezionata la rete e il client "vittima" su cui lavorare (ovviamente tutto di nostra proprietà), premiamo *Next* e poi *Start*. Comparirà una finestra per la selezione del dizionario: digitiamo */media/xiaopan/* per vedere tutti i dischi collegati al sistema (anche USB). Possiamo entrare in quello che contiene i dizionari (preparato in precedenza) e selezionare il file che vogliamo.



5 Basta aspettare!

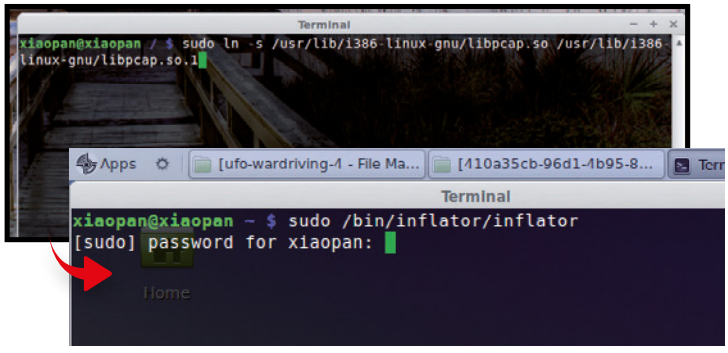
Scelto il dizionario, l'attacco comincia. Per velocizzare la cattura dell'handshake facciamo saltare la connessione del client "vittima" costringendolo a riconnettersi: basta premere *Deauth* a intervalli di 10-30 secondi finché non si ottiene l'handshake. Al termine, se la password è nel dizionario verrà trovata (*WPA key found*); in caso contrario selezioniamo un nuovo dizionario.

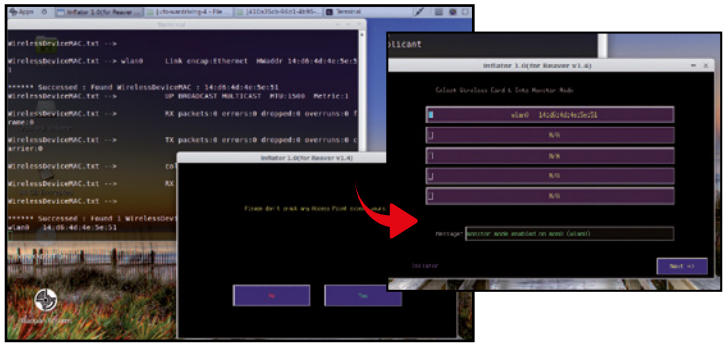
CRACKARE LE VECCHIE CHIAVI WEP

Il vecchio standard WEP ha un difetto di progettazione che rende più semplice scoprire la password alfanumerica (che, tra l'altro, ha lunghezza fissa di 10 caratteri) senza nemmeno la necessità di un dizionario. Si può sfruttare l'attacco ***P0841 Replay Attack*** fornito da Feeding Bottle (oppure ***ARP Replay Attack***: più veloce, ma non sempre funziona) che, nel giro di qualche minuto, riesce a calcolare la password corretta basandosi sule risposte che il router gli invia quando viene provata una password errata (*Initialization Vector o IV*).

No alla connessione semplificata

Il sistema WPS, ideato per la semplificazione delle connessioni Wi-Fi, ha un punto debole sfruttabile dai pirati. Grazie ad esso è possibile entrare in pochi minuti anche in una rete WPA protetta.



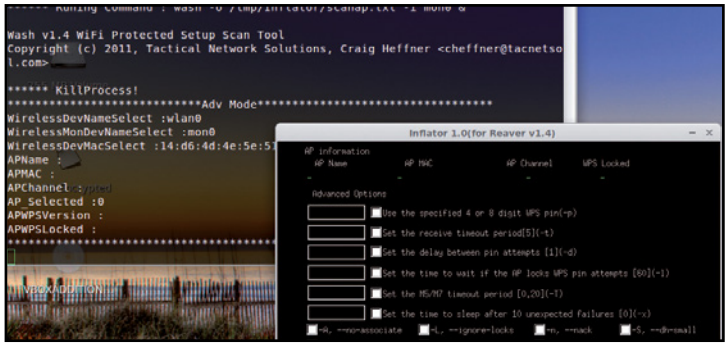


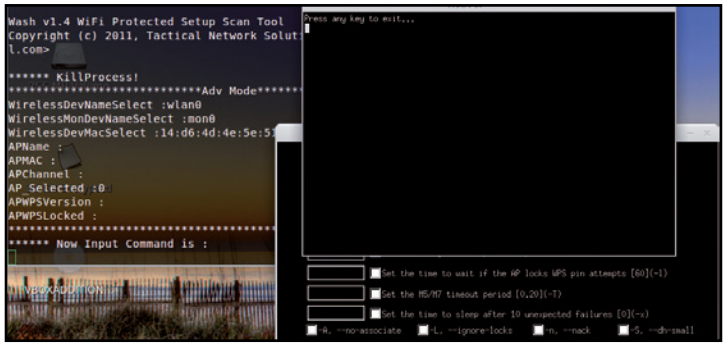
1 Il tool per le intrusioni

Per avviare Inflator occorre creare il collegamento a una libreria chiamata *libpcap*. Apriamo Terminal Emulator e diamo il comando *sudo ln -s /usr/lib/i386-linux-gnu/libpcap.so /usr/lib/i386-linux-gnu/libpcap.so.1*. Come password di root scriviamo *rocksolid* e premiamo *Invio*. Ora, per lanciare il programma, scriviamo *sudo /bin/inflator/inflator*.

2 La scheda di rete giusta

Inflator ci chiede di non crackare reti Wi-Fi che non ci appartengono. Poiché stiamo testando la sicurezza del nostro router premiamo tranquillamente *Yes*. Scegliamo poi l'interfaccia wireless su cui lavorare. Per le prove ne abbiamo collegata una sola al PC, quindi sarà *wlan0*. Prima di procedere attendiamo che venga abilitata la modalità monitor su questa scheda di rete.





3 Scansione e crack

Il passo successivo è ben diverso da quanto abbiamo visto finora. Sono infatti presenti tutta una serie di opzioni, che consentono di tenere in considerazione tutte le varie modalità WPS esistenti. Per cominciare, ci conviene lasciare non spuntate tutte le caselle e premere subito il pulsante *Run* per avviare la procedura di crack.

4 In attesa del PIN WPS

Comparirà la finestra di Reaver che si occupa di eseguire il crack. Se il router è vulnerabile, comparirà la password di accesso. In caso contrario, è possibile chiudere Reaver e, tornando alla finestra precedente, mettere la spunta a qualche casella riprovando ad avviare (*Run*) la procedura per verificare se, con impostazioni differenti, sia possibile crackare il router.

LE FUNZIONI DI AIRCRACK USATE DURANTE UN ATTACCO

FOUR WAY HANDSHAKE
È il processo con cui un computer si presenta al router per richiedere una connessione; e il router risponde. I messaggi sono cifrati, ma possono essere facilmente intercettati con una scheda in modalità monitor.

AP NAME
È il nome dell'Access Point, ovvero il nome della rete, grazie al quale è possibile riconoscerla (per esempio, una rete di Telecom Italia potrebbe avere un nome del tipo "Alice-128928").

AP MAC (O BSSID)
È l'identificativo univoco della scheda di rete del router. Questo codice consente al nostro PC di riconoscere il router (il nome della rete può cambiare, il MAC Address no).

PWR
È la potenza del segnale. Questo valore è indicato in scala inversa, quindi un valore pari a zero è il massimo e indica che il router si trova praticamente accanto al nostro PC, mentre un valore inferiore (-10 o -70) indica che il router è più distante.

BEACONS
Sono gli intervalli periodici con cui il router invia, tramite onde radio, le informazioni su se stesso (come il nome della rete, per esempio), per consentire agli altri computer di identificarlo.

CIPHER
È il tipo di crittografia WPA utilizzata dal router. Di solito, sui router "comuni" viene usata la AES-CCMP, ma in alcuni access point pubblici si sfrutta la TKIP. La prima è più facile da crackare.

#DATA
Si tratta della quantità totale di dati trasmessi dal router.

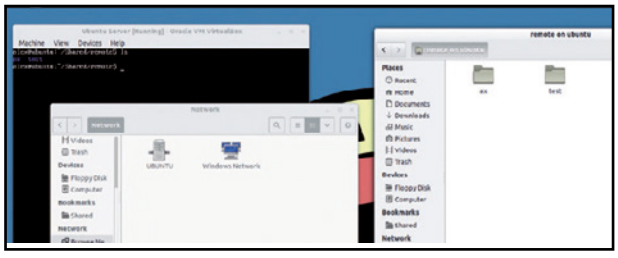
#/S
È la media di dati scambiati dal router per secondo. Un numero grande indica che c'è molto traffico, e quindi potrebbero esserci molte più occasioni per sniffare una handshake e crackare la rete.

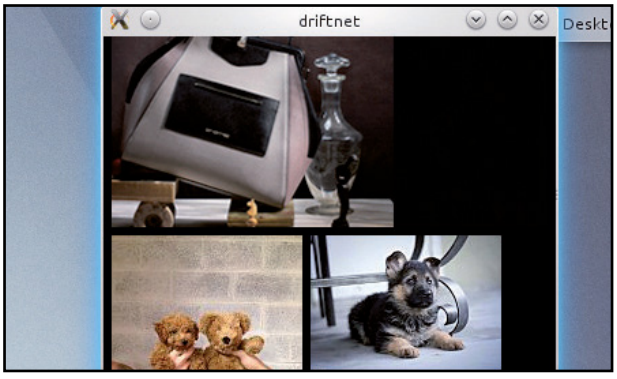
ASDL SCROCCATE: ECCO GLI EFFETTI INDESIDERATI

Trovata la chiave Wi-Fi del router, il pirata può persino spiarci! Ecco alcuni esempi pratici di ciò che rischiamo.

SPIARE TRA FILE E CARTELLE

Molti utenti condividono file e cartelle nella rete locale per accedervi dagli altri computer. È utile, ma se un pirata riesce ad entrare nella LAN sono guai per la nostra privacy, ancor più se non abbiamo condiviso soltanto una cartella ma l'intero disco *C:* (se abbiamo salvato un file di testo con l'elenco delle password, il pirata lo troverà!). In Xiaopan OS Pro, infatti, è integrato Samba, un protocollo che consente l'accesso alle cartelle condivise di Windows. Per vedere queste cartelle basta aprire il file manager e scegliere la voce *Network*.



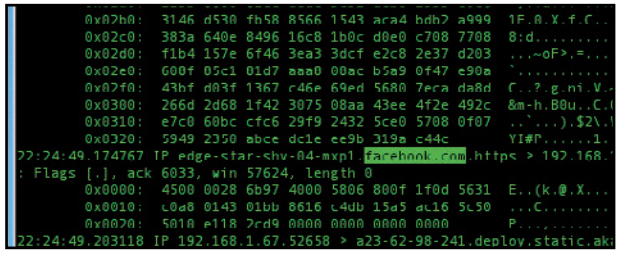


INTERCETTARE IL TRAFFICO DI RETE

Quando due computer comunicano (ad esempio il PC e il router) avviene uno scambio di richieste e risposte *ARP* (*Address Resolution Protocol*), tramite il quale ogni dispositivo sa con chi ha a che fare. Per esempio: A ha un indirizzo *MAC 00:00:00:00:00:AA* ed IP *192.168.1.3*, mentre B è *00:00:00:00:00:BB* con IP *192.168.1.5*. Quando i due sistemi cominciano a comunicare A invia a B la richiesta ARP: *"chi è 192.168.1.5?"*. B risponderà *"192.168.1.5 è 00:00:00:00:00:BB"*. Ovviamente, B farà lo stesso, ed entrambe registreranno le risposte ricevute nella ARP cache. In questo modo, ogni volta che A vorrà parlare con B andrà a leggere la propria cache e vedrà che deve contattare *00:00:00:00:00:BB*. Ma c'è un problema: un dispositivo accetterà una risposta ARP anche se non ha fatto alcuna domanda. Inoltre, nel sistema ARP una nuova risposta sostituisce sempre quella vecchia nella cache (se entrambe si riferiscono allo stesso IP). Ciò significa che mentre due PC stanno comunicando, un malintenzionato potrebbe inviare a uno dei due una risposta ARP appositamente costruita per sostituirsi all'interlocutore e ricevere al posto suo tutte le informazioni che l'altro sistema sta inviando. Questa debolezza può essere sfruttata per realizzare un attacco Man In The Middle (MITM) con la tecnica dell'ARP spoof. In XiaoPan OS Pro è sufficiente avviare Terminal Emulator e digitare *arpspoof -i eth0 -t 192.168.1.3 192.168.1.1* dove *192.168.1.3* è il computer "vittima", mentre l'altro è il router. Divenuto un MITM, il pirata può leggere tutta la comunicazione col comando *tcpdump -i wlan0 -X*. Esistono addirittura programmi più comodi come dsniff -n che cerca di individuare tutte le password che circolano, o driftnet -i wlan0 che mostra al pirata tutte le immagini (non troppo pesanti) che l'utente invia o riceve tramite il Web.

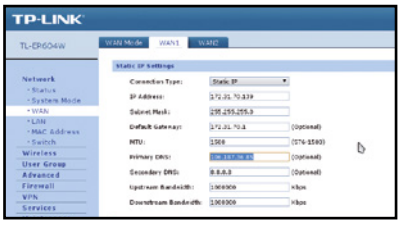
PASSWORD RUBATE

Il protocollo HTTPS viene utilizzato dai siti (store on-line, Facebook ecc.) per cifrare la connessione. Tuttavia, un pirata che si trova nella nostra rete Wi-Fi può dirottare i pacchetti ARP (o TCP) e inoltrare le richieste HTTPS per intercettare tutta la nostra comunicazione. Per eseguire un attacco di HTTPS hijacking, dal Terminal Emulator di XiaoPan il pirata abilita il forwarding dei pacchetti sul proprio PC, in modo da essere un intermediario: *echo "1" > /proc/sys/net/ipv4/ip_forward* poi suggerisce ad iptables di dirottare i pacchetti che arrivano sulla porta 6000 (che otterrà dal server) sulla porta 80, in modo da farli avere alla vittima su una connessione HTTP: *iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 6000*. Fatto ciò avvia sslstrip per ricevere sulla porta 6000 i pacchetti che gli interessano: *sslstrip -l 6000*. A questo punto, su un altro Terminal Emulator (senza chiudere i sslstrip) si pone come Man In The Middle con il classico ARP spoof: *arpspoof -i eth0 –t 192.168.1.3 192.168.1.1* (*192.168.1.3* è la vittima; *192.168.1.1* è il router). Ora il cracker deve soltanto avviare tcpdump, meglio se in ascolto sulla porta 6000 in modo da intercettare solo quello che vuole.



DIROTTAMENTO DEI DNS

Gli attacchi Man In The Middle "tradizionali" possono essere svolti finché il pirata si trova nella LAN della vittima. Ma esiste un trucco per continuare a essere un MITM anche a distanza... Ogni router ha dei server DNS predefiniti, attraverso i quali i PC della LAN riescono a tradurre i nomi dei siti Web in indirizzi IP realmente raggiungibili. I server DNS, quindi, possono leggere quasi tutto il nostro traffico sul Web e agire come dei veri Man In The Middle. Pertanto, se invece di passare da un DNS "ufficiale" (Google, Telecom ecc.), il nostro traffico arriva a un server DNS realizzato dal pirata, è ovvio che potrà controllare tutto ciò che noi facciamo su Internet. E, se è entrato nella nostra LAN, il pirata non deve fare altro che aprire il pannello di controllo del router e sostituire i DNS di default con l'indirizzo del suo server.



XIAOPAN SU VIRTUALBOX

Se siamo curiosi, possiamo provare XiaoPan anche su VirtualBox (www.virtualbox.org). Basta avviare la macchina virtuale dall'immagine ISO di Xiaopan OS PRO, scaricata da SourceForge. La macchina virtuale dovrà obbligatoriamente avere l'accelerazione grafica 3D abilitata. Inoltre, sarà opportuno collegare al computer un adattatore Wi-Fi USB (può andare bene anche uno dei classici modelli D-Link che si trovano nei supermercati) e renderlo disponibile alla macchina virtuale cliccando sul menu Dispositivi/USB. Se la schermata appare bloccata, è sufficiente ridimensionarla (cliccando una o due volte sul pulsante "massimizza" della finestra di Windows). Le guest additions sono già presenti in Xiaopan PRO, quindi il sistema è già pronto per operare e mettere alla prova la nostra rete domestica.

Cure miracolose per il Wi-Fi lento

Cosa ci occorre
20 MIN.
FACILE
ANALIZZATORE DI RETE
EKAHAU HEATMAPPER
Lo trovi su: ☑DVD
SOFTWARE COMPLETO
Sito Internet:
www.ekahau.com

Non sentiamoci imbarazzati: quasi tutti soffriamo per una WLAN poco prestante. Ora finalmente è arrivato il rimedio per tutti i mal di... rete!

I router Wi-Fi sono sempre più diffusi e con loro anche i problemi di rallentamenti nel trasferimento dei dati, soprattutto quando PC, tablet o smartphone sono collocati lontani dallo stesso router WLAN. Non di rado l'umore si rabbuia o procura scatti d'ira, come quando i filmati scorrono in modo scattoso. Ciò nonostante anche lievi malesseri possono essere curati, così come le gravi insufficienze. Vi spieghiamo ora come tutto questo può avvenire: la terapia può spaziare da validi rimedi casalinghi a leggeri interventi sulla rete WLAN (Wireless Local Area Network), fino ad apportare guarigioni miracolose impiegando i nuovi adattatori Wi-Fi Powerline, che abbiamo sperimentato nei nostri laboratori.

Formuliamo la diagnosi

Prima di dare corso alla terapia occorrerà stabilire il focolaio della malattia: quali sono i punti dell'abitazione in cui la rete senza fili non è sufficientemente veloce? Per la cura della WLAN il "dottore" consiglia un'esplorazione approfondita dell'abitazione utilizzando un notebook ed un programma di analisi di rete come Ekahau HeatMapper, di facile utilizzo anche per coloro che non sono medici informatici. Se impiegato accuratamente, il programma è in grado di rappresentare graficamente il segnale Wi-Fi su una mappa in cui i colori variano a seconda della potenza della WLAN: una specie di risonanza magnetica per la rete Wi-Fi! Il colore rosso, ad esempio, indica un segnale scadente: in questo caso la rete è gravemente ammalata e può anche contagiare chi la usa procurando eritemi e stimolando la produzione di cortisolo, detto anche ormone dello stress, che raggiunge livelli intollerabili a causa di download lentissimi e navigazioni a passo di lumaca.

La Terapia

A seconda del tipo e della gravità dei sintomi, sono molteplici i metodi terapeutici, tutti efficaci, che possiamo applicare alla rete Wi-Fi:

- **Semplice rimedio casalingo** Già una diversa collocazione della WLAN può apportare dei miglioramenti. I rimedi che descriviamo in queste pagine costituiscono la terapia alternativa, quando il router è posizionato non lontano dai dispositivi. La causa del cattivo funzionamento è in molti casi un radiodisturbo, causato da reti WLAN dei vicini di casa o da altri dispositivi. Il rimedio casalingo più semplice suggerisce di posizionare il router in un altro punto dell'abitazione o di passare ad un altro canale di trasmissione della WLAN! Questo intervento può in molti casi alleviare i sintomi o addirittura eliminarli.
- **Interventi lievi** Al pari della chirurgia mini-invasiva laparoscopica, che lascia tracce quasi invisibili, anche le prestazioni di un ripetitore di qualità possono essere di aiuto per migliorare la trasmissione di dati. Il vantaggio è costituito dal fatto che questo dispositivo, con prezzi che variano da 30 a 50 euro, è abbastanza economico.
- **Guarigione miracolosa** La terapia più moderna si fonda sugli adattatori Powerline per la rete WLAN. Come un bypass per il cuore, provvedono a convogliare attraverso la linea elettrica il flusso dati dal router, dove richiesto dalla rete WLAN, aggirando in tal modo le pareti che creano ostacoli. La differenza, rispetto alla terapia tradizionale della medicina classica, è che la maggior parte degli adattatori Powerline normali trasferisce i dati solo attraverso queste "arterie". Gli adattatori utilizzati per il test sono invece equipag-

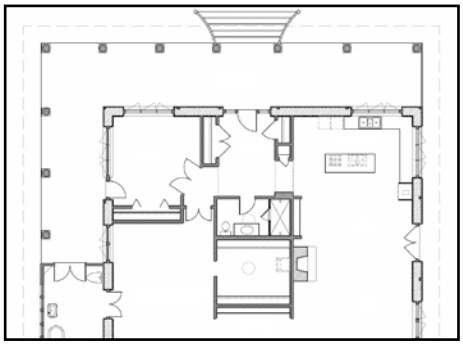
CURE MIRACOLOSE CONTRO LA WLAN ANEMICA

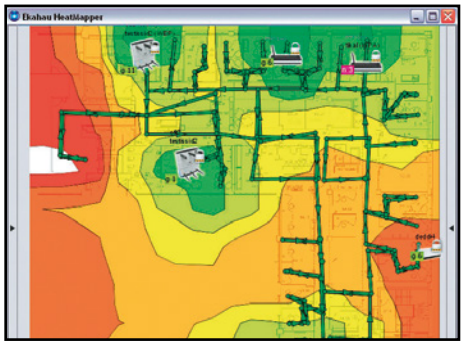
PER PICCOLI APPARTAMENTI

Qui la potenza di trasmissione del router è spesso sufficientemente adeguata. Una buona ricezione del router WLAN può essere spesso impedita da un posizionamento sfavorevole del dispositivo o da interferenze causate da altre reti wireless. Semplici accorgimenti possono apportare notevoli miglioramenti (pag. 27).

Quanto è potente la tua WLAN?

Prima di scegliere la terapia occorre formulare la diagnosi, che dovrà accertare il punto debole della rete wireless. Per farlo bastano un notebook e un programma come Ekahau HeatMapper. Ecco come procedere





1 La pianta dell'appartamento

Disponendo della piantina dell'appartamento sarà molto più facile stabilire una diagnosi. Se abbiamo solo una stampa, effettuiamone una scansione e salviamo l'immagine in formato *JPEG*. In caso contrario, basterà anche uno schizzo e potremo orientarci con la griglia fornita dal programma.

2 Subito operativi

Installiamo il software su un notebook e attiviamo la connessione alla rete wireless. Scegliamo se lavorare su una piantina (*I have a map image*) o con la griglia inclusa nel programma (*I don't have a map image*). Fissiamo con un clic la nostra posizione, contrassegnata da un punto verde.

3 Analizziamo la rete

Spostiamoci per l'appartamento e fissiamo altre posizioni. Al termine clicchiamo col tasto destro sull'immagine a video: HeatMapper visualizzerà la rete WLAN. Le superfici di colore verde indicano buona ricezione, quelle di colore arancione/rosso evidenzieranno invece una cattiva connessione.

giati con una veloce e potente Wi-Fi in standard "n".

Effetti collaterali

In quasi tutti i casi l'applicazione di questi metodi può, con una WLAN veloce, essere causa di un inaspettato ed eccessivo trasferimento di dati. Anche una eventuale congestione di dati nella rete WLAN può essere curata. Spesso, semplici messe a punto da eseguire sul router possono già essere di aiuto e anche un ripetitore WLAN può ampliare notevolmente la portata del collegamento a onde radio. Gli adattatori Powerline con trasmettitore WLAN integrato, sono invece in grado di convogliare una potente rete WLAN esattamente nel punto dove è richiesto maggiore segnale. In tutti i casi, la nostra connessione a Internet ci ringrazierà per l'efficace cura ricostituente!

PER APPARTAMENTI GRANDI

Ogni parete tende ad attutire la rete WLAN, provocando una riduzione della velocità di trasferimento dei dati. Utilizzando un ripetitore WLAN (pag. 27), potrete incrementare la portata della rete WLAN, che vi consentirà di eseguire nuovamente veloci download e streaming di dati.

CONTRO I BLOCCHI DELLA RETE WLAN

Tramite gli adattatori Powerline (pag. 29), la rete WLAN potrà essere trasferita nel punto dove è richiesta. Anche i soffitti in cemento armato non saranno di alcun ostacolo, perché verranno aggirati da questo dispositivo combi intelligente, attraverso la rete elettrica di casa.

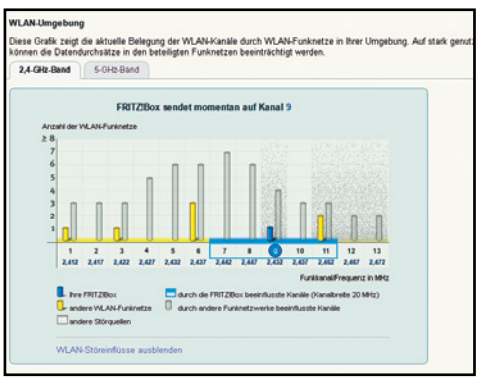
SOLUZIONE NUMERO 1

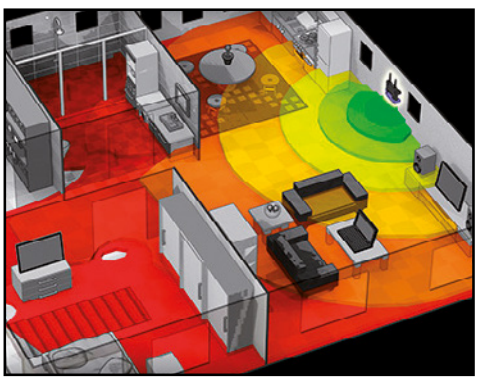
OTTIMIZZARE LA WLAN

METODO DI CURA 1
SEMPLICE RIMEDIO CASALINGO

Tentar non nuoce: alcuni acciacchi della rete WLAN possono essere curati con rimedi omeopatici, senza alcun rischio ed effetti collaterali.

Anche quando la rete WLAN sembra non dare alcun segno di vita può succedere che, dopo avere cambiato canale di trasmissione, il trasferimento dei dati riprenda a funzionare correttamente su una frequenza meno disturbata. Se, malgrado l'impiego di router moderni, i video trasferiti via WLAN sono visualizzati in modo scattoso, tutto questo potrà essere in parte evitato sfruttando più canali (la procedura è detta "channel bundling"). Ricorrendo ai rimedi illustrati in basso, riusciremo a risolvere numerosi problemi, non attribuibili alla trasmissione di dati attraverso le pareti.





1 Scelta del canale

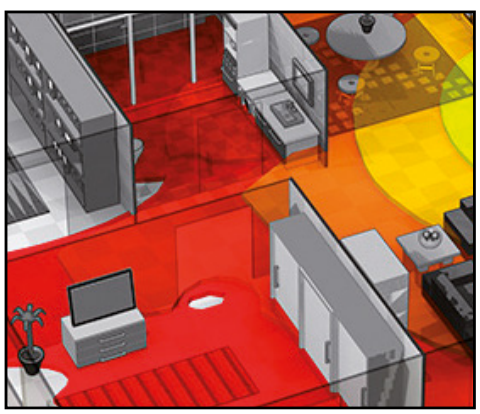
Se tutti gli utenti si avvalgono dello stesso canale radio, le reti WLAN vicine tra di loro tendono a ostacolarsi. Dal menu per le impostazioni del router, provvedete ad attivare la funzione di ricerca automatica per il miglior canale, che, per i dispositivi AVM troverete alla voce ***WLAN***, ***Canale di trasmissione***. Risultato: aumento della velocità.

2 Cambio della radio

Chi dispone di un router dual band potrà passare alla meno disturbata banda da 5 Gigahertz, eliminando gli ingorghi di dati. Accertiamoci che il router continui a trasmettere anche su 2,4 GHz, visto che non tutti i dispositivi WLAN sono in grado di funzionare con 5 GHz.

3 CHANNEL BUNDLING

I dispositivi funzionano tutti correttamente con lo standard Wireless N (802.11n)? Se sì, potete allora usare il channel bundling del vostro router WLAN e lasciare che trasmetta contemporaneamente su due canali (dal menù digitate: ***Impostazioni***, ***WLAN***, ***canale radio***, ***300 Mbps***).



4 Spostare il router

Per godere di prestazioni ottimali, il router con funzioni di access point dovrebbe stare in un punto libero da ostacoli, lontano da fonti di disturbo, come i telefoni DECT. ***Ekahau HeatMapper*** vi aiuterà a trovare la posizione migliore.

5 Un router nuovo

Il router WLAN ha più di sei anni? In caso affermativo, possiamo pensare di comprarne uno nuovo con il veloce standard Wireless N. A meno di 100 Euro possiamo trovare il veloce Fritz Box 3272.

SOLUZIONE NUMERO 2

AMPLIFICHIAMO IL SEGNALE WI-FI

L'intero appartamento è servito dalla rete WLAN, ma in alcune stanze la trasmissione dati avviene solo in modo discontinuo? Spesso un ripetitore WLAN può fare miracoli.

Quando i rimedi casalinghi non sono sufficienti, saremo costretti a chiamare uno specialista anziché il medico di base. Potremmo, ad esempio, ricorrere ad un amplificatore per la rete WLAN, il cosiddetto ripetitore. Ne esistono già a partire da 40 euro e rappresentano la soluzione semplice e affidabile per ampliare il campo di ricezione della rete WLAN.

Ripetere conviene

Il ripetitore può essere inserito in una presa elettrica, in un qualsiasi punto della casa, tra il router WLAN e il modulo ricevitore. Il dispositivo provvederà a captare i segnali da e per il router e a ritrasmetterli in modo amplificato, creandosi una propria rete WLAN. Questa nuova WLAN funzionerà da ponte tra il router e i dispositivi di ricezione, ad esempio un notebook, che consentirà una velocità di trasferimento dati più elevata, anche su grandi distanze. Una rete WLAN in prossimità del ripetitore è logicamente più potente rispetto a quella offerta dal router, la cui efficacia sarà già stata attenuata dalle pareti dell'appartamento.

"Un ripetitore wireless può guarire molti mali. Casomai, è meglio scegliere una via di mezzo"

Semplici impostazioni

Nel momento in cui il ripetitore si attiva, ogni dispositivo si collega automaticamente con la WLAN più potente a cui può connettersi. Se il dispositivo si trova vicino al ripetitore, si collegherà alla rete WLAN di quest'ultimo. Spesso, il ripetitore e il router hanno la stessa password per il dial-up, e usano anche lo stesso nome di rete. Ciò significa che, per uno smartphone o un notebook, sarà difficile distinguere se sono loggati alla WLAN del router o a quella del ripetitore. È però possibile usare anche nomi e password diversi per la rete WLAN. Se un dispositivo è loggato ad una delle WLAN, mantiene comunque anche l'accesso a tutta la rete.

Dove posizionare il ripetitore?

Il punto debole di ogni ripetitore dipende dal fatto che quest'ultimo, per ricevere i segnali del router, necessita di ricorrenti pause per la trasmissione, che riducono il flusso dati. Ragione per cui, quanto meglio sarà posizionato il ripetitore, tanto meno pesante sarà questo calo. Come regola generale, il ripetitore dovrebbe essere collocato a metà strada tra il router e il ricevitore della rete WLAN. In questo modo la trasmissione dati, attraverso il ripetitore WLAN, sarà più veloce di quella tramite il debole collegamento con il router WLAN.

Non sempre la fedeltà ripaga

Numerosi notebook, smartphone e tablet rimangono "fedeli" alla rete WLAN alla quale si sono loggati la prima volta. Ne consegue che questi dispositivi continuano a rimanere ostinatamente legati a questo scadente collegamento, anche se potrebbero usufruire di un collegamento di gran lunga migliore, tramite un ripetitore WLAN. Tutto questo accade quando al ritorno a casa colleghiamo per prima cosa il nostro smartphone al potente router WLAN e poi ci spostiamo in salotto, dove il ripetitore è molto più potente. Per risolvere questo problema, possiamo attivare brevemente la funzione di ricerca per la WLAN e cambiare manualmente la rete.

VELOCE E SEMPLICE Il ripetitore WLAN Fritz 310 (42 Euro) offre una portata più ampia, con una spesa limitata. Basterà inserirlo nella presa, premere i tasti WPS del router e del ripetitore e il gioco è fatto. La velocità è sufficiente per trasferire video in HD in tutta la casa. All'occorrenza, il ripetitore, purché collegato ad un router Fritz Box, potrà essere messo in pausa durante la notte.

SOLUZIONE NUMERO 3

LA LAN DIVENTA ELETTRICA

Se la rete WLAN non ne vuol sapere di attraversare le pareti, si potrà farla passare attraverso la presa elettrica.

Quando spesse pareti in cemento armato bloccano totalmente il flusso dati alla rete WLAN, neppure un ripetitore WLAN può migliorare la situazione. Il rimedio miracoloso per questi problemi potrebbe essere la trasmissione dei dati attraverso la linea elettrica (tecnologia Powerline) di casa, incanalandola ulteriormente attraverso la rete WLAN. Il principio di funzionamento della Powerline è semplice: dovremo semplicemente provvedere a collegare un adattatore al router, affinché i dati possano essere trasferiti attraverso i cavi elettrici di casa. Potranno essere posizionati anche altri adattatori nei punti dove è richiesto un collegamento con la rete. Questi dispositivi provvederanno a ripescare i dati dalla linea elettrica. Fino ad oggi uno svantaggio di questa tecnologia era costituito dal fatto che i dispositivi entravano in collegamento con la rete solo tramite cavo LAN perché in effetti lo standard Powerline non prevede una rete Wi-Fi. Con i nuovi adattatori Powerline per WLAN la situazione cambia, poiché essi si creano una propria rete. In tal modo è quindi possibile, collegare smartphone, notebook o tablet, che non dispongono di una porta di connessione per la LAN. Si collegano al router e a Internet attraverso l'adattatore WLAN e la linea elettrica e, inoltre, anche agli altri dispositivi della LAN domestica, come una stampante o un disco virtuale on-line.

Ripetitore o adattatore Powerline?

Gli adattatori con funzione WLAN, con prezzi da 70 a 140 euro, sono più costosi di un ripetitore (a partire da 40 euro). Il costo eccedente si ricompensa, però, quando la rete smette di funzionare in alcune stanze a causa della presenza di ostacoli o in appartamenti e abitazioni molte ampie. I kit adattatori offrono anche un altro vantaggio rispetto ai ripetitori WLAN, la cui velocità di trasferimento dati dipende fortemente dal punto in cui sono stati posizionati. Quanto più lontani saranno collocati dal router, tanto più bassa sarà la velocità.

Come funziona l'installazione?

Per ogni abitazione sono necessari almeno due adattatori. L'adattatore semplice Powerline viene posizionato sul router, mentre il modello con funzione di WLAN può essere collocato in ogni punto, dove è richiesta una buona rete WLAN. Grazie ad una password standard preimpostata, gli adattatori stabiliscono il collegamento criptato attraverso la linea elettrica. Tale password andrà modificata solo se utilizzeremo prese di corrente esterne. In caso contrario, gli utenti non autorizzati potranno connettersi alla nostra LAN di casa, inserendo un adattatore Powerline.

ROUTER

La cura basata sul cambio di canale ha eliminato i disturbi alla rete WLAN causati dal vicino di casa. Risultato: la rete WLAN vicina al router è il metodo più veloce per accedere alla rete (blu). I trasferimenti di dati sono stati più lenti tramite il ripetitore (rosso) e l'adattatore Powerline con funzione WLAN (verde).

100 Mbps
50 Mbps
35 Mbps

SALOTTO

La cura con il ripetitore ha reso possibile un tale aumento di velocità, da non bloccare il trasferimento di video attraverso la rete (rosso). Tutto questo ad un costo limitato.

36 Mbps
48 Mbps
35 Mbps

STUDIO

Dove il router arriva con poca potenza (blu) e anche il ripetitore offre una ricezione debole (rosso), l'adattatore Powerline con funzione WLAN è in grado di gestire velocemente il flusso dati (verde).

15 Mbps
25 Mbps
35 Mbps

Powerline con funzione WLAN | Ripetitore WLAN | Rete WLAN

Windows diventa hotspot!

✓ Posso condividere la connessione Internet del PC con altri dispositivi hi-tech?

✓ Come sfruttare il router virtuale di Windows 8?

SERVE A CHI...
... vuole creare un hotspot Wi-Fi con Windows 8 per condividere la connessione (wireless, cablata o 3G) con tutti i dispositivi

Generalmente per creare un hotspot Wi-Fi si ricorre a un router dotato di access point wireless. Questo genere di dispositivi è ormai divenuto un accessorio indispensabile per ogni abitazione. Oltre ai notebook, una rete senza fili ci consente di collegare a Internet smartphone, console, player multimediali, Smart TV e altri dispositivi. Tutti noi dovremmo avere un access point in casa e se proprio ne siamo sprovvisti possiamo acquistarlo spendendo pochissimi euro. Nonostante un access point sia il modo più semplice per creare una rete senza fili, non è indispensabile se abbiamo un notebook recente, in quanto possiamo condividere la connessione con tutti i dispositivi Wi-Fi che abbiamo in casa usando esclusivamente il nostro PC desktop.

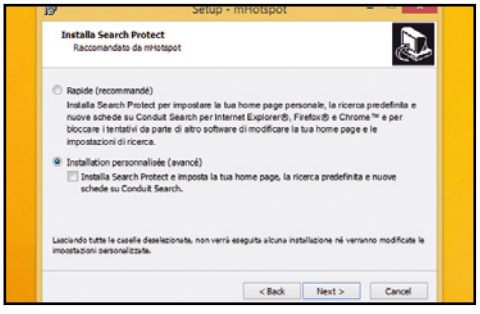
Access point... ma virtuale!

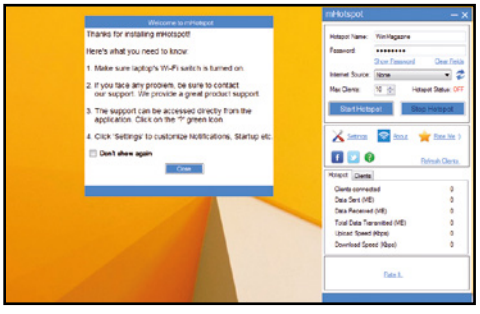
A partire da Windows XP, Microsoft ha dotato i propri sistemi operativi della possibilità di creare reti ad hoc in modo da collegare tra loro i dispositivi sfruttando il modulo wireless. Con l'arrivo di Windows 7 questa caratteristica è stata migliorata in modo da permettere al computer di condividere anche la connessione a Internet oltre che le risorse locali. In pratica, grazie alla presenza di un router virtuale, l'utente può collegare il portatile a Internet con il cavo ethernet o con una chiavetta 3G e condividere la connessione con altri dispositivi tramite un hotspot Wi-Fi gestito dal sistema operativo stesso. Non se ne capisce bene il motivo, ma fatto sta che Microsoft ha deciso di non includere la stessa funzione anche nell'ultimo dei suoi sistemi operativi. Per dirla tutta, la caratteristica è presente in Windows 8, solo che non è abilitata e per farlo è necessario agire dal Prompt dei comandi, soluzione del tutto anacronistica e scomoda, soprattutto se abbiamo intenzione di utilizzarla frequentemente. Per fortuna che a semplificarci le cose ci hanno pensato gli sviluppatori di mHotspot, un software leggerissimo che una volta configurato ci permetterà di abilitare/disabilitare il router virtuale in un paio di clic. mHotspot è in grado di trasformare il PC in un punto di accesso wireless protetto dal protocollo WPA2 (il più sicuro attualmente in circolazione) per condividere qualunque tipo di connessione, fungendo anche da ripetitore del segnale (range extender). Inoltre, offre un pannello di controllo che consente di monitorare costantemente il traffico e i dispositivi collegati e non appesantisce affatto il sistema.

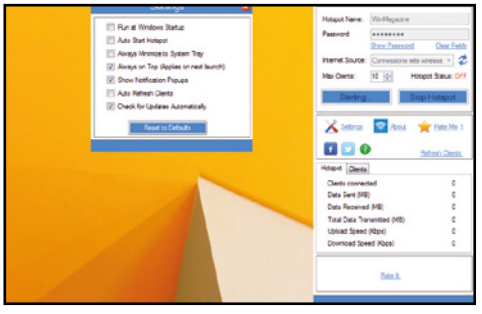
MHOTSPOT
Il software completo lo trovi sul ☑DVD

CONDIVIDIAMO LA CONNESSIONE
Se dopo l'attivazione dell'hotspot notiamo che i dispositivi riescono a collegarsi ma non a navigare, è necessario agire sulla connessione principale e abilitare la condivisione. Clicchiamo con il tasto destro del mouse sulla connessione Internet del PC e selezioniamo *Apri Centro connessioni di rete e condivisione*. Clicchiamo su *Modifica impostazioni scheda*, apriamo le proprietà della scheda di rete che collega il PC a Internet, spostiamoci nella scheda *Condivisione* e spuntiamo *Consenti ad altri utenti in rete di collegarsi tramite la connessione Internet di questo computer*, confermando con *OK*.

Trasformiamo il nostro amato PC in un hotspot Wi-Fi pronto all'uso







1 Estraiamo l'archivio ***mHotspot.zip*** (lo trovi sul nostro Win DVD-Rom) e avviamo l'eseguibile. Proseguiamo l'installazione, scegliamo l'opzione ***Installation personnalisee*** rimuovendo la spunta da ***Installa Search Protect*** e ***AVG PC TuneUP*** e clicchiamo ***Install/Finish***.

2 Clicchiamo su ***Scarica e installa*** questa funzionalità qualora comparisse questa richiesta in seguito all'avvio di mHotspot. Avviamo il programma e diamo un nome alla rete locale (***Hotspot name***) e impostando un password di almeno 8 caratteri alfanumerici.

3 Selezioniamo la connessione da condividere (***Internet source***), clicchiamo su ***Start Hotspot*** e connettiamo a esso i dispositivi. Se vogliamo che l'hotspot sia sempre raggiungibile, da ***Settings*** spuntiamo le caselle ***Run at Windows sturtup*** e ***Auto start Hotspot***.

Naviga gratis con Facebook

Parti in vacanza e resta connesso a Internet. Gli hotspot Wi-Fi e le chiavi di accesso le trovi sulla tua bacheca!

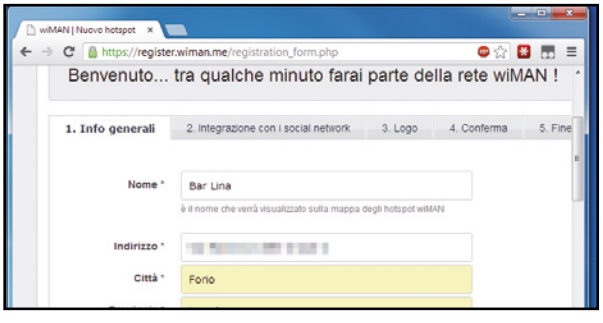
Anche in Italia cominciano a diffondersi gli hotspot Wi-Fi pubblici, a cui è possibile accedere per navigare liberamente su Internet dovunque ci troviamo. In questo modo, anche in vacanza non dovremo rinunciare a controllare la casella di posta, le notizie dei quotidiani e a rimanere in contatto con gli amici di Facebook. E proprio il social network può trasformarsi in una chiave universale di accesso a Internet: il merito è di wiMAN, il social Wi-Fi che permette di collegarsi ad un hotspot autenticandosi col proprio account Facebook, senza doversi più preoccupare di identificarsi con un documento o inserire complicate password ricevute via SMS. Il "miracolo" è possibile grazie ad un router con firmware modificato che sempre più locali pubblici stanno installando in tutta Italia, creando la prima rete Wi-Fi social per l'accesso libero a Internet. Scopriamo di cosa si tratta e, se siamo gestori di un locale, impariamo ad installare il router wiMAN per fornire un ottimo servizio ai nostri clienti!

Apriamo la confezione

1 All'interno del pacco che wiMAN ci invierà a casa, oltre al router troveremo dei badge adesivi per pubblicizzare il Wi-Fi Free della nostra rete wireless e un foglio illustrativo che ci spiega come attivare wiMAN. Iniziamo installando le due antenne sul retro del router.

Registriamo il dispositivo

2 Connettiamo il computer al router mediante un altro cavo Ethernet, da collegare questa volta a una delle porte LAN (quelle in giallo), attendiamo che Windows rilevi la rete, dopodiché avviamo il browser e puntiamolo alla pagina di registrazione wiMAN (https://register.wiman.me).



Installazione fulminea

3 Colleghiamo un cavo Ethernet proveniente dal modem alla porta Wan del router wiMAN (quella in blu), inseriamo l'adattatore in una presa di corrente e colleghiamo il jack alla porta *Power* del dispositivo. A questo punto il router è già connesso a Internet e non resta che configurarlo.

Nome e indirizzo

4 I dati di accesso li troviamo su un bollino sotto al router. Digitiamoli nei rispettivi campi e clicchiamo *Login*. Il primo passo della registrazione sarà quello di fornire nome, indirizzo e dati dell'attività, un'e-mail e impostare la password di accesso al pannello di controllo wiMAN.

Cosa ci occorre

20 MIN. FACILE

ROUTER WI-FI
WIMAN SOCIAL WI-FI ROUTER
Quanto costa: € 79,00
Sito Internet: www.wiman.me/it

BUONI CONSIGLI

TUTTO IN UN FIRMWARE

Il router wiMAN non è altro che un dispositivo TP-Link (più precisamente si tratta del modello TL-WR842ND) cui è stato installato un firmware modificato. Necessario per il funzionamento di wiMAN, il firmware modificato ha però ridotto notevolmente le capacità del router e non offre alcun tipo di accesso agli strumenti presenti invece nel pannello di controllo TP-Link. Questo significa che non sarà possibile modificare la password WPA2 della rete WiFi riservata, ne tantomeno gestire le funzionalità avanzate del router, come, ad esempio, la porta USB.

SSID SU MISURA

Di default l'SSID, ovvero il nome, della rete pubblica wiMAN è wiMAN@free. Se vogliamo personalizzarlo con il nome nostro o del nostro locale, basta accedere al pannello di controllo (https://my.wiman.me), spostarsi nella sezione Settings e digitare il nome nella casella Ssid name. Salviamo (Save) e riavviamo il router per applicare la modifica.

1 AC PLUG
Qui va collegato l'alimentatore elettrico fornito in dotazione col router

2 PORTA WAN
È la porta a cui collegare in cascata il nostro modem/router ADSL mediante cavo Ethernet

3 PORTA LAN
Queste quattro porte permettono di collegare altri PC o dispositivi di rete al router

4 PORTA USB
Al momento è disabilitata. In futuro servirà per collegare un pendrive di ripristino

5 LED FUNZIONAMENTO
Mostra l'attività del router e aiuta l'utente ad eseguire un'analisi veloce del dispositivo

6 ATTIVITÀ WI-FI
Il lampeggiamento di questa spia suggerisce all'utente eventuali anomalie o il corretto funzionamento della rete wireless

7 ATTIVITÀ LAN
Indica visivamente la presenza di traffico in transito dal nostro router

8 CONNESSIONE INTERNET
La luce fissa della spia indica il corretto collegamento del router alla Rete

9 ATTIVITÀ USB
Segnala l'utilizzo delle porte presenti sul retro del router

10 SICUREZZA ATTIVA
Quando è accesa segnala il corretto funzionamento della protezione di rete sulla nostra LAN

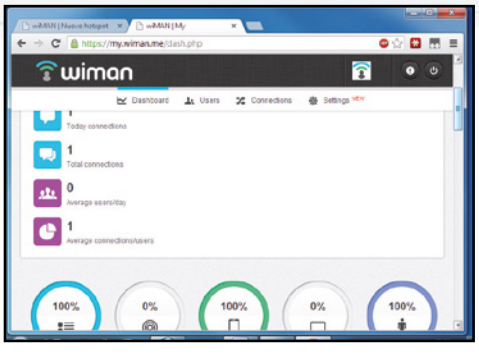
BUONI CONSIGLI

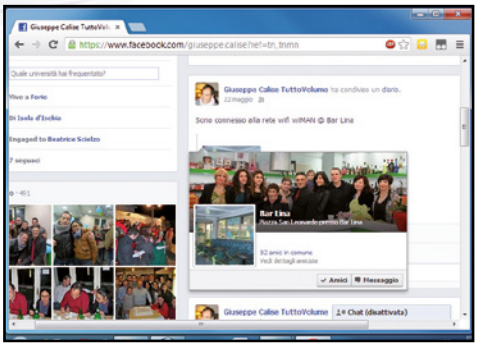
PUBBLICITÀ GRATUITA

wiMAN si rivela anche un ottimo mezzo per la promozione del locale. Infatti, quando qualcuno si connette al nostro hotspot invia automaticamente un post sul proprio profilo dove è indicato il nome, l'immagine e il link alla pagina pubblica del nostro locale.

IDENTIFICARE IL COLPEVOLE

Il log degli accessi nel pannello di controllo conserva solo parte dell'ID Facebook degli utenti. Le informazioni complete per risalire all'identità di un cliente, nel caso di un illecito attuato utilizzando la nostra rete, sono a disposizione degli inquirenti che potranno richiedere tutti i dettagli di un profilo agli amministratori di wiMAN.





Per i locali 2.0

5 La procedura prosegue richiedendo di fornire l'URL della nostra pagina pubblica Facebook (o quella del locale) o il profilo Twitter. Inseriamo i dati richiesti o saltiamo se ne siamo sprovvisti, clicchiamo *Avanti* e confermiamo la registrazione cliccando sul link recapitatoci via e-mail.

Utenti sotto controllo

6 Clicchiamo sul pulsante *Inizia* a usare il tuo pannello di controllo e autentichiamoci con i dati usati in fase di registrazione (**Passo 4**). Il pannello di controllo wiMAN ci consente di monitorare gli accessi e conoscere utenti e tipologia di dispositivi collegati al nostro hotspot.

Un hotspot per due reti

7 Le reti WiFi create da WiMAN sono due: una privata cui si accede utilizzando la password WPA2 che troviamo nella confezione del router e una libera (*FREEwiMAN@wifi*) che, in seguito alla connessione, richiede al cliente di autenticarsi con i dati del proprio profilo Facebook.

Per conoscere tutti i punti di accesso wiMAN in Italia è sufficiente collegarsi al sito www.winmagazine.it/link/2164.

450 hotspot
già attivi in tutta Italia

1.000 unità
sono gli ordini per i prossimi mesi

30.000 utenti
hanno usato il servizio wiMAN

30% gli utenti stranieri
che si sono collegati a Internet con wiMAN

300.000 le connessioni
generate mediante gli hotspot wiMAN

I SEGRETI DI WIMAN: UNA RIVOLUZIONE TUTTA ITALIANA

Abbiamo chiesto a Michele Di Mauro (CTO) e Massimo Ciuffreda (CEO) di parlarci del loro progetto, il primo social Wi-Fi Europeo.

Win Magazine Parlateci di wiMAN e di come è nato!
wiMAN Tutto inizia qualche anno fa, quando abbiamo cominciato a lavorare su un progetto volto a creare un hotspot nel nostro paese, Mattinata, piccolo centro nel cuore del Gargano. Nella nostra zona il problema del digital divide è molto sentito e così abbiamo pensato a come poter rispondere a quelle che erano le esigenze del territorio. In pochi mesi siamo riusciti a realizzare una serie di hotspot, offrendo un ottimo servizio a basso costo sia ai nostri concittadini sia ai tanti turisti che arrivano nei mesi estivi. L'idea iniziale è andata bene e così abbiamo cominciato ad allargare il progetto arrivando a coprire l'intero Gargano. Ma creare una rete di hotspot così estesa avrebbe richiesto oltre un milione di euro come costi di realizzazione della infrastruttura (senza contare i costi di manutenzione e di gestione). Inoltre, avevamo gli stessi limiti della maggior parte degli hotspot presenti in Italia (e non solo): la lunga fase di registrazione che va ripetuta per ogni nuovo hotspot, il fatto che ogni registrazione restituisce delle credenziali di accesso e che ogni hotspot è accessibile con credenziali diverse tra loro e quindi difficili da ricordare. In pratica sono le stesse le problematiche che hanno limitato lo sviluppo della connettività Wi-Fi nel nostro Paese. Ci voleva dunque un servizio sicuro, poco costoso e soprattutto innovativo! Da qui è partita l'avventura della nostra startup made in Puglia: wiMAN - The social wifi network (dove "wi" sta per Wi-Fi e "man" per uomo).

Win Magazine Quale idea sta dietro al progetto?
wiMAN È molto semplice: offrire agli utenti la possibilità di connettersi a una rete Internet in maniera facile e veloce, eliminando la laboriosa fase di registrazione che caratterizza i normali hotspot. Pensato in primis per le attività commerciali che vogliono dare sia un servizio aggiuntivo alla propria clientela, può tornare utile anche in tutti quegli ambiti domestici in cui si desidera condividere la connessione ADSL.

Win Magazine Quali vantaggi offre la vostra soluzione di accesso libero senza fili a Internet?
wiMAN Il commerciante/gestore offre un servizio molto richiesto e ottiene anche una grande visibilità. Ad ogni connessione alla rete wiMAN verrà generato un post nella bacheca Facebook. Il post generato contiene logo, nome e link diretto alla pagina del locale che offre il servizio di connettività.

Win Magazine I gestori dei locali che offrono il servizio wiMAN possono accedere alle informazioni personali dei loro utenti?
wiMAN I gestori di locali wiMAN hanno a disposizione un pannello di controllo che contiene importanti informazioni statistiche, ma non hanno accesso in nessun modo alle informazioni personali dei singoli utenti, del cui trattamento è titolare esclusivamente wiMAN s.r.l. Le uniche informazioni legate all'utente che sono visibili al gestore del locale sono il nome ed il cognome puntato (ad esempio Michele D.). Ovviamente Facebook non comunica la password legata all'account personale a nessuna applicazione di terze parti, né tantomeno a wiMAN.

Win Magazine Chi gestisce Sicurezza e Privacy?
wiMAN Quando wiMAN (o una qualsiasi applicazione di terze parti) ha bisogno di autenticare un utente, lo reindirizza sulla pagina di Facebook. Il processo di autenticazione è dunque interamente gestito dal social network e in questo modo possiamo identificare gli utenti verificati e abilitare la navigazione (ricordiamo che l'utente verificato è colui che ha associato un'identità reale a quella virtuale tramite inserimento di un numero di cellulare). Questo garantisce un ottimo livello di sicurezza. Inoltre, WiMAN è responsabile del trattamento dei dati personali e della privacy. Il gestore del locale che offre accesso pubblico a Internet mediante la sua rete wireless è completamente sollevato da questa responsabilità.

Win Magazine Dove è possibile acquistare il router wiMAN e, quindi, sottoscrivere contestualmente un account al vostro progetto?
wiMAN Attualmente è possibile acquistare il router wiMAN direttamente dal nostro sito www.wiman.me/it cliccando sul pulsante Acquistalo ora. L'utente verrà automaticamente reindirizzato sulla piattaforma di Amazon.it dove potrà completare l'acquisto.

Grazie ad un ripetitore wireless ti bastano pochi minuti per portare Internet in tutte le stanze di casa. Ecco come fare

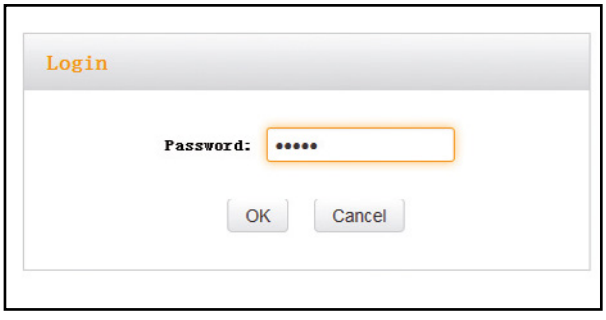
Estendi il segnale della rete Wi-Fi

La tecnologia Wi-Fi ha permesso di liberare i nostri appartamenti da inutili grovigli di fili: basta avere un router wireless per collegarsi a Internet senza il fastidio del cavo Ethernet, stampare dal cellulare, navigare col tablet, accedere a numerosi contenuti Web direttamente dal televisore del salotto e tanto altro ancora. Il problema è che le mura di casa, a volte, ostacolano il segnale Wi-Fi rendendo difficoltoso collegarsi dalle stanze più lontane dal router. In questi casi può tornarci utile un semplice range extender come il Tenda A301 Wireless-N300 Range Extender in grado di catturare il segnale dal router e propagarlo negli "angoli bui" di casa. Vediamo assieme come configurarlo e utilizzarlo al meglio.

Cosa ci occorre

10 MIN. FACILE

RIPETITORE WIRELESS
TENDA A301 WIRELESS-N300 RANGE EXTENDER
Quanto costa: **€ 31,97**
Sito Internet: www.telcominstrument.com

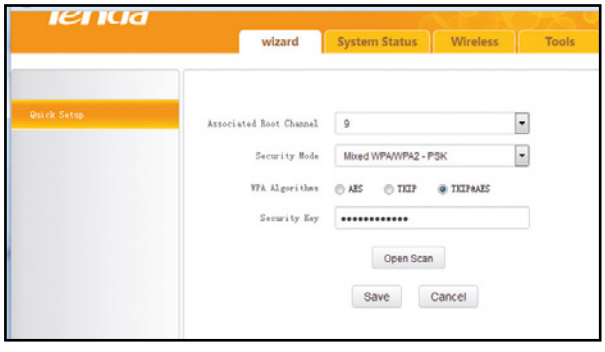


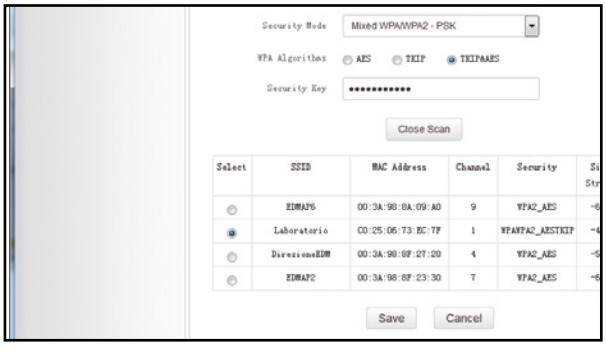
Effettuiamo i collegamenti

1 Prima di cominciare, verifichiamo che il router Wi-Fi sia acceso e abbia il collegamento a Internet attivo. Colleghiamo quindi il range extender ad una presa di corrente a muro e poi, utilizzando il cavo Ethernet in dotazione, ad una porta di rete del computer: il LED *Lan* inizierà a lampeggiare.

Ecco il pannello di controllo

2 Spostiamoci sul computer, avviamo il browser, digitiamo *re.tendacn.com* nella barra degli indirizzi e premiamo *Invio* per collegarci all'interfaccia Web di gestione del dispositivo. Nella schermata di login usiamo *admin* come *Password* e clicchiamo *OK* (o premiamo *Invio*) per effettuare l'accesso.





Alla ricerca del Wi-Fi

3 Dall'interfaccia Web di configurazione del range extender rimaniamo nella sezione *wizard*, scorriamo la finestra *Range Extender Mode* e clicchiamo sul pulsante *Open Scan*. Dopo qualche secondo il dispositivo individuerà le reti Wi-Fi disponibili: selezioniamo la nostra e clicchiamo su *OK*.

Siamo connessi

4 Digitiamo in *Security Key* la chiave WPA/WPA2 per accedere alla nostra rete wireless. Al termine, clicchiamo *Save* per confermare l'operazione e poi *OK* per riavviare il dispositivo. Il nostro PC è ora connesso al router Wi-Fi grazie al range extender ed è pronto per collegarsi a Internet!

BUONI CONSIGLI

IN WI-FI CON LO SMARTPHONE

Grazie al range extender possiamo collegarci al router Wi-Fi dalle altre stanze di casa anche con il nostro smartphone, con il tablet o con qualunque altro dispositivo wireless. In realtà non dobbiamo fare altro che collegarci normalmente alla nostra rete predefinita: il range extender, infatti, è "invisibile" agli altri dispositivi e nell'elenco delle connessioni wireless disponibili sullo smartphone (o sugli altri dispositivi) comparirà l'SSID della nostra rete alla quale potremo collegarci con un semplice tap!

CONFIGURAZIONE CON UN TOCCO

Se il nostro router Wi-Fi ha il modulo WPS attivo, possiamo configurare il range extender in maniera semplicissima: basta infatti premere il pulsante WPS sul router per attivare la funzione e poi premere e tenere premuto per circa 3 secondi il pulsante Sync sul range extender.

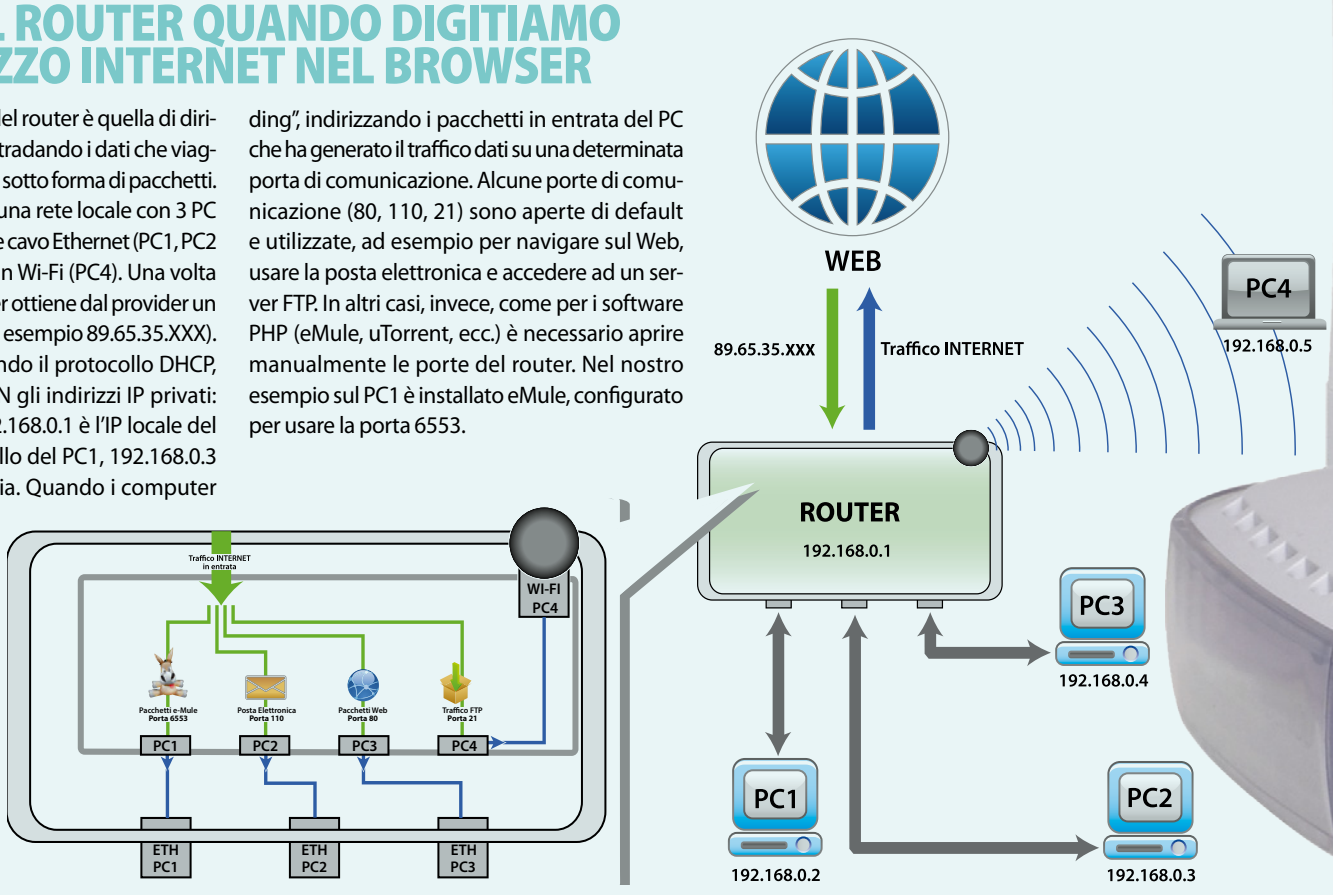
Router: guida all'uso

Scopri tutti i segreti del dispositivo che consente al tuo PC di accedere a Internet

Tra i dispositivi di rete quello sicuramente più importante, più usato e conosciuto è il router. È proprio grazie a questo apparecchio che, se in casa oppure in ufficio abbiamo più computer connessi ad Internet tramite la LAN, da ognuno di essi siamo in grado di navigare sul Web, consultare la nostra casella di posta elettronica ed eseguire tutte le operazioni che siamo soliti effettuare in Rete. I dati viaggiano sulle reti informatiche sotto forma di pacchetti, ossia appositamente frammentati in tante piccole unità caratterizzate ciascuna da una serie di informazioni aggiuntive come l'indirizzo IP del dispositivo o computer che lo ha inviato (sorgente) e quello che lo deve ricevere (destinazione). Quando un router riceve un pacchetto esamina l'indirizzo IP di destinazione, lo cerca in un elenco (tabella di routing) che ha memorizzato e, in base alle informazioni trovate, individua il percorso migliore per inviarlo. Nel caso di router domestici tale percorso è obbligato, in quanto tutto il traffico uscente viene direttamente inviato al provider: questi invece è in grado di confrontare un elevato numero di percorsi e scegliere quello migliore per inoltrare il pacchetto. Se per qualche motivo non esiste un percorso valido, allora viene restituito un messaggio di errore all'IP sorgente. Una volta trovato il percorso, il nostro router effettua la cosiddetta NAT (Network Address Translation), cioè traduce l'indirizzo IP sorgente del PC (ad esempio 192.168.1.2) contenuto nel pacchetto in un indirizzo pubblico (quello assegnato dal provider), quindi aggiunge ad esso altre informazioni necessarie per la trasmissione.

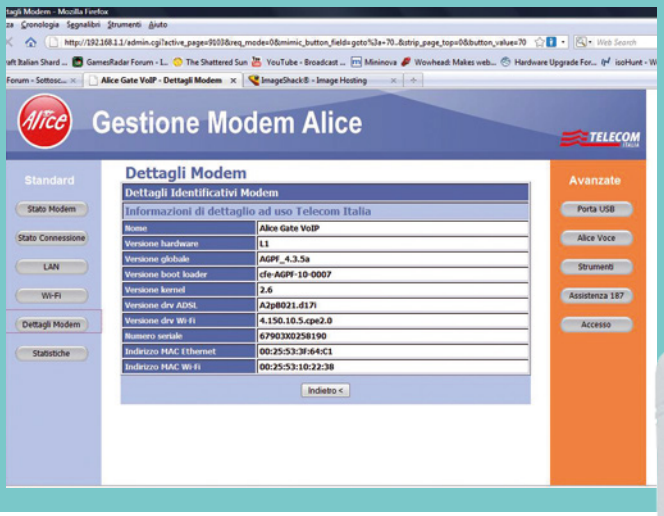
COSA FA IL ROUTER QUANDO DIGITIAMO UN INDIRIZZO INTERNET NEL BROWSER

La funzione principale del router è quella di dirigere il traffico di rete instradando i dati che viaggiano da e verso Internet sotto forma di pacchetti. Immaginiamo di avere una rete locale con 3 PC connessi al router tramite cavo Ethernet (PC1, PC2 e PC3) e uno collegato in Wi-Fi (PC4). Una volta connesso al Web, il router ottiene dal provider un indirizzo IP pubblico (ad esempio 89.65.35.XXX). Allo stesso tempo, usando il protocollo DHCP, assegna ai PC della LAN gli indirizzi IP privati: nel nostro esempio 192.168.0.1 è l'IP locale del router, 192.168.0.2 quello del PC1, 192.168.0.3 quello del PC2 e così via. Quando i computer accedono a Internet, il router effettua la NAT, ossia sostituisce all'interno dei pacchetti in uscita il loro IP privato con quello pubblico e viceversa per quelli in entrata, consentendo così ai PC della LAN di accedere al Web. Per alcuni servizi il router deve adottare il sistema del "port forwarding", indirizzando i pacchetti in entrata del PC che ha generato il traffico dati su una determinata porta di comunicazione. Alcune porte di comunicazione (80, 110, 21) sono aperte di default e utilizzate, ad esempio per navigare sul Web, usare la posta elettronica e accedere ad un server FTP. In altri casi, invece, come per i software PHP (eMule, uTorrent, ecc.) è necessario aprire manualmente le porte del router. Nel nostro esempio sul PC1 è installato eMule, configurato per usare la porta 6553.

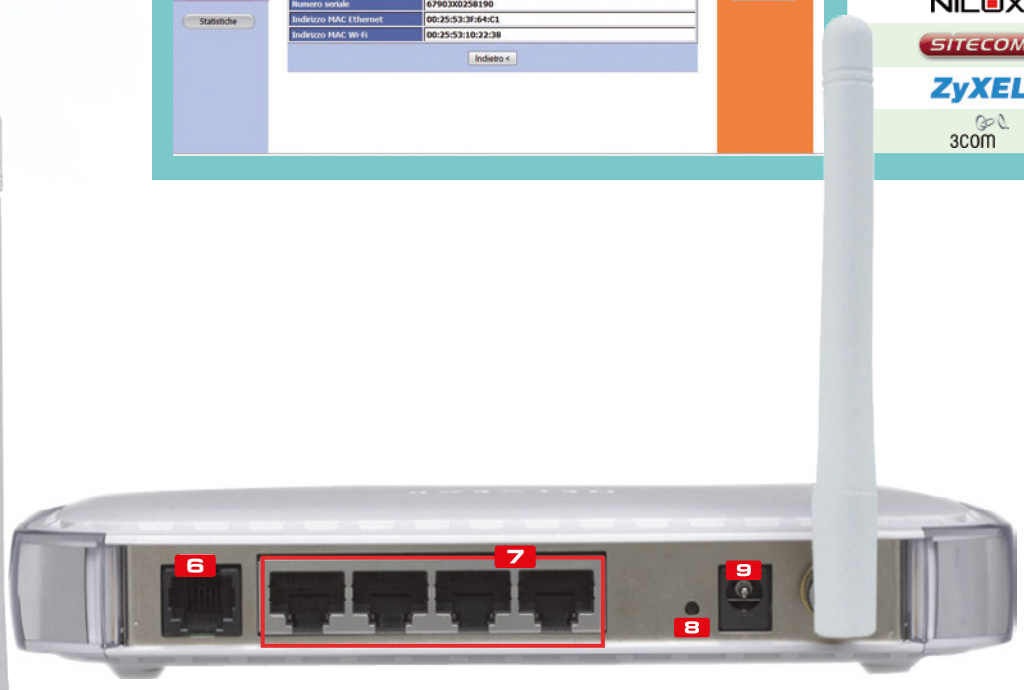


DRITTI NEL CUORE DEL ROUTER ADSL

Tutti i modelli di router hanno un software di gestione che permette di aprire le porte del dispositivo, impostare una password di accesso per il Wi-Fi, attivare un servizio DDNS ed altro ancora. Per accedere al pannello di gestione occorre digitare l'indirizzo nel browser che varia da modello a modello (vedi tabella a fianco).



MARCA	INDIRIZZO	USER	PASSWORD
Alice	192.168.1.1	nessuna	nessuna
ASUS	192.168.1.1	admin	admin
Atlantis Land	192.168.1.254	admin	atlantis
belkin	192.168.2.1	nessuna	nessuna
BUFFALO	192.168.11.1	root	nessuna
digicom	192.168.1.254	nessuna	admin
D-Link	192.168.1.1	admin	admin
FRITZ!	192.168.178.1	nessuna	nessuna
LINKSYS	192.168.1.1	admin	admin
NETGEAR	192.168.0.1	admin	password
NILOX	192.168.1.1	Admi n	Admin
SITECOM	192.168.0.1	admin	admin
ZyXEL	192.168.1.1	nessuna	1234
3com	192.168.1.1	nessuna	admin



1 ECO MODE
Segnala se il dispositivo è alimentato dalla corrente elettrica

2 LED TEST
Quando è acceso vuol dire che il router è in fase di inizializzazione

3 LED WIRELESS
Quando questo LED è accesso, è attiva la rete Wi-Fi

4 LED INTERNET
Indica lo stato della connessione ADSL

5 LED LAN
Segnala l'attività delle porte RJ-45 alle quali sono collegati i computer della rete locale

6 ADSL
A questa porta va collegato il doppino proveniente dalla presa telefonica

7 LAN
Queste quattro porte RJ-45 consentono di connettere il router ai PC della LAN

8 RESET
Consente di riportare il dispositivo alle impostazioni di fabbrica

9 POWER
In questa presa va inserito lo spinotto dell'alimentatore del router

Router no problem!

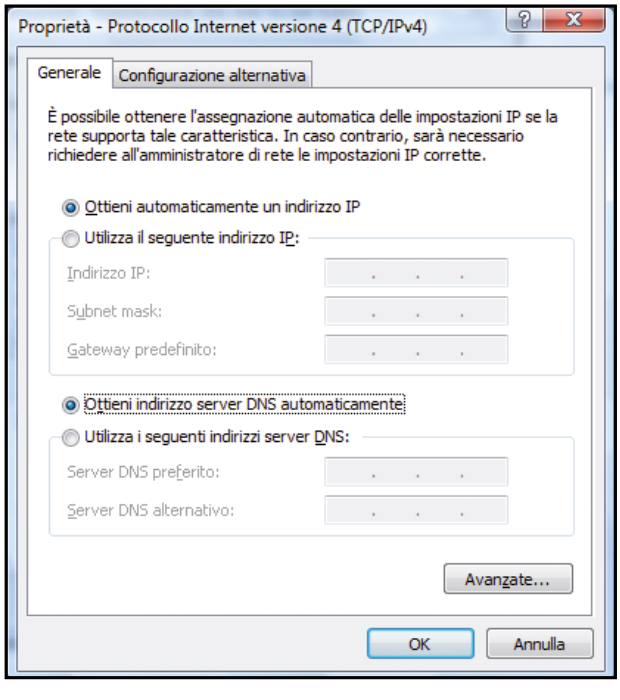
La connessione Internet non va o il PC non si collega alla LAN? Ecco i trucchi degli esperti per essere sempre connessi!

Una delle classiche situazioni da "panico informatico" in cui ci siamo spesso trovati è di sicuro questa: il modem si sincronizza all'ADSL, il LED è acceso (quindi dovremmo riuscire a navigare), ma la connessione fallisce e va in timeout! "E ora che si fa"? Tutti conoscono la frustrazione che i router wireless o i modem ADSL possono causare. Del resto Internet è diventata così importante per la vita di tutti i giorni, lavorativa e non, che restarne senza, anche per un breve periodo di tempo, farebbe sprofondare chiunque nella disperazione. Le nostre reti domestiche, con cui mettiamo in comunicazione computer, tablet, smartphone e stampanti di casa, a un tratto smetterebbero di darci i vantaggi e le comodità cui difficilmente siamo disposti a rinunciare. Difficoltà a connettersi al modem Wi-Fi, oppure a collegare in LAN la multifunzione; rumori di fondo durante le conversazioni al telefono o password smarrite per accedere alle funzionalità del router, sono soltanto alcuni dei problemi che affliggono chi in casa ha un modem/router. Nella maggior parte dei casi, non si tratta di problemi insormontabili, tutt'altro, e basterebbero alcuni semplici accorgimenti per risolverli definitivamente da soli.

IL ROUTER NON È ACCESSIBILE

Spesso capita che, a causa di una non corretta configurazione della scheda di rete del PC, non riusciamo ad aprire col browser la pagina di configurazione del router. Ecco come risolvere.

Ogni router, quando si installa per la prima volta, è configurato in modalità DHCP, ovvero assegna gli IP ai computer collegati in modo completamente automatico. In questo caso basta collegare il PC al router tramite cavo Ethernet, andare in *Start/Pannello di controllo/Rete* e *Internet/Centro connessioni di rete e condivisione*, cliccare *Modifica impostazioni scheda*, premere col tasto destro sulla scheda *Ethernet* e selezionare *Proprietà*: nelle Proprietà del *Protocollo Internet versione 4 (TCP/IPv4)* selezioniamo *Ottieni automaticamente un indirizzo IP* e confermiamo con *OK*. Se anche in questo caso non fosse possibile accedere al pannello di controllo, è necessario un reset del dispositivo.



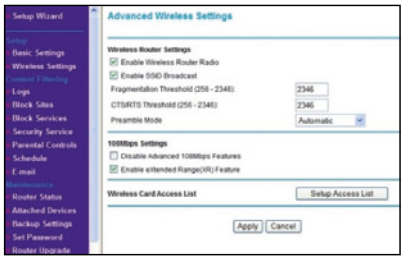
SE LA RETE VA LENTA

Anche se i nostri PC sono dotati di schede di rete da 1 Gigabit, il trasferimento file nella LAN può risultare ugualmente lento. Vediamo perché.

Generalmente un trasferimento lento dei dati all'interno della LAN dipende dallo switch integrato nel router. Se esso è da 100 Mbps la velocità non potrà superare quella consentita dal router. Se anche lo switch è da 1 Gigabit, invece, accertiamoci di utilizzare cavi CAT 6 o CAT 5E (ma non CAT 5), per sfruttare appieno la velocità.

SPEGNERE IL WI-FI CON UN TASTO

Per disattivare la connessione Wi-Fi del router generalmente bisogna accedere all'interfaccia del dispositivo. In taluni casi è possibile farlo senza usare il PC.



Molti dei nuovi router in vendita permettono di disattivare la connessione Wi-Fi senza necessariamente entrare nel menu del router tramite browser. Ad esempio ci sono dei modelli di Netgear che consentono di attivare/disattivare la modalità wireless a nostro piacimento semplicemente interagendo con un tasto dedicato (Wireless on/off) e comunque, sempre, a PC spento.

IN RETE CON TABLET E SMARTPHONE

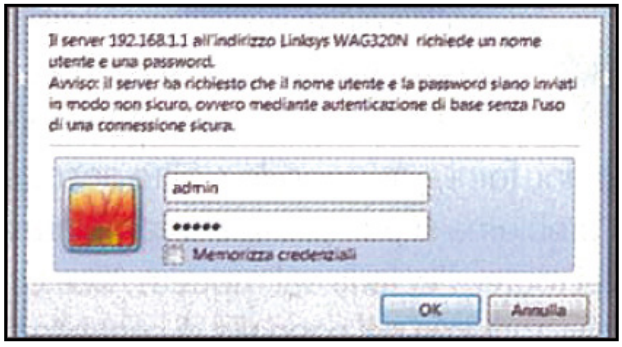
Se abbiamo un router Alice Gate VoIP Plus Wi-Fi e non riusciamo a navigare sul Web con i dispositivi mobile collegati tramite Wi-Fi (l'iPad ad esempio potrebbe segnalarci che la connessione non è disponibile) possiamo risolvere il problema eseguendo alcune semplici verifiche.

Le reti wireless possono essere disturbate dai dispositivi elettronici che usano la stessa banda (2.4 GHz) del router (come telefoni cordless, telefonini, forni a microonde e altro ancora). Per risolvere il problema possiamo provare a cambiare il canale Wi-Fi del

router. Per farlo sui modem Alice Gate VoIP 2 Plus Wi-Fi andiamo nel pannello di controllo digitando nella barra degli indirizzi del browser l'indirizzo *192.168.1.1*. Inseriamo login e password di accesso se richiesti. Una volta fatto il login spostiamoci nella sezione *Wi-Fi* e premiamo *Configura Rete Wi-Fi*. Impostiamo il nuovo canale in *Canale Radio* e premiamo *Salva*. Se i problemi permangono, disabilitiamo uno per volta i dispositivi di casa che possono creare problemi, per identificare il colpevole e prendere provvedimenti. Altra soluzione consiste nel ricorrere ad un router wireless di tipo dual band che, oltre alla normale banda di trasmissione a 2,4 GHz usa anche quella a 5 GHz come il modello di Linksys WAG320N (www.linksysbycisco.com).

IL CENTRO COMANDI DEL ROUTER

I router dispongono di un'interfaccia Web per effettuare tutte le configurazioni del caso. Ecco come accedere ad essa.

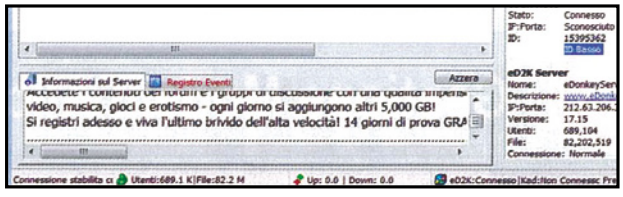


Avviamo il browser Web, inseriamo l'indirizzo IP del router nel campo URL e premiamo *Invio*. In molti casi è necessario inserire username e password d'accesso (quelle predefinite si possono recuperare dal manuale d'uso del prodotto e sono consultabili nella tabella che trovi a pagina sinistra).

PORTE APERTE AL FILE SHARING

Se scarichiamo dal Web usando ad esempio un client P2P come eMule è necessario aprire sul router le porte giuste. In questo modo eviteremo lunghe code di attesa e download lenti.

Prima di aprire le porte nel router è necessario assegnare un IP statico al computer sul quale è installato eMule. Dal menu *Start/Pannello di controllo/Rete* e *Internet/Connessioni di rete*, facciamo clic col tasto destro del mouse sulla scheda di rete e poi su *Proprietà*. Dall'elenco che compare nella finestra selezioniamo *Protocollo Internet versione 4* e premiamo *Proprietà*. In *Generale* spuntiamo la voce *Utilizza il seguente indirizzo IP:* in *Indirizzo IP* impostiamo un IP compreso nella sottorete del router (ad esempio *192.168.1.102*); in *Subnet Mask* lasciamo invece quello proposto da Windows; in *Gateway predefinito* e in *DNS preferito* immettiamo l'IP del router (*192.168.1.1*). Fatto ciò, salviamo e usciamo da questra finestra. Accediamo adesso al pannello di controllo del modem Alice e spostiamoci nella sezione *Port Mapping*. Da *Applicazioni* selezioniamo *eMule*; in *IP destinazione* scegliamo l'IP *192.168.1.102* e premiamo *Attiva*. Avviamo quindi il Mulo, facciamo clic su *Opzioni* e selezioniamo *Connessione*. In *TCP* scriviamo *4662*, in *UDP* immettiamo *4672*, premiamo il pulsante *Applica* e poi *OK*.



COLLEGARE MOLTI COMPUTER AL ROUTER

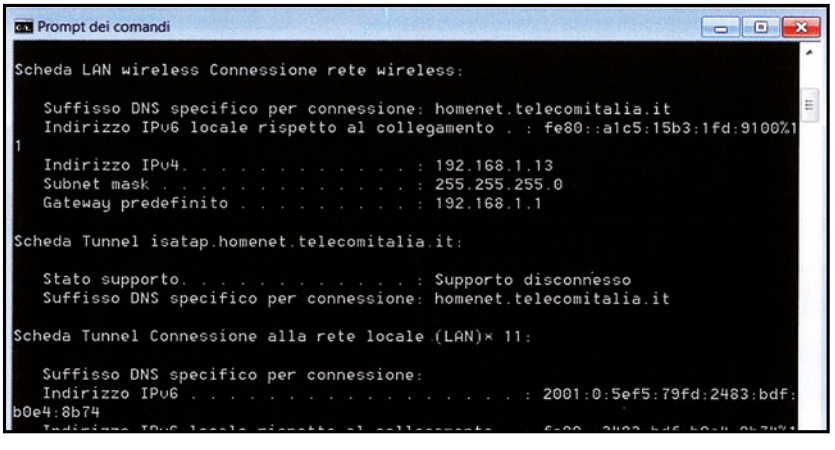
Il router generalmente dispone di alcune porte LAN, ma basta collegare ad esso tutti i computer di casa per occuparle tutte. Per collegare al router altri PC basta usare uno switch.

Quando bisogna aumentare il numero di PC da collegare al router, una soluzione pratica è quella di ricorrere ad uno switch a 4,8 o più porte LAN. Una volta connesso al router, questo dispositivo hardware fu nziona in modo trasparente, ovvero non viene rilevato dai computer della LAN, e gestisce in modo efficiente il traffico dati instradando correttamente i pacchetti all'interno della rete locale.

SCOPRIRE L'IP DEL COMPUTER NELLA LAN

Per conoscere l'indirizzo IP che il router assegna al nostro PC quando ci colleghiamo alla LAN di casa basta eseguire un semplice comando dal Prompt dei comandi. Ecco come.

Andiamo in *Start/Tutti i programmi/Accessori/Prompt dei comandi,* digitiamo nell'apposito box il comando *ipconfig* e premiamo il tasto *Invio*. L'indirizzo IP assegnato dal router al computer è quello indicato alla voce *Indirizzo IPv4*. In *Gateway predefinito*, invece, è riportato l'IP del router.



Internet doppia velocità

Tutti i trucchi per sfruttare contemporaneamente le connessioni 3G e ADSL e scaricare a 2X

Cosa ci occorre

15 MIN. FACILE

SISTEMA OPERATIVO
PFSENSE
Quanto costa: gratuita
Sito Internet: www.pfsense.org

INTERNET KEY
HUAWEI E173
Quanto costa: € 39,00
Sito Internet: www.huawei.com

APP ANDROID
SUPER DOWNLOAD LITE – BOOSTER
Quanto costa: gratuita
Note: la versione free non effettua download di file superiori a 50 MB

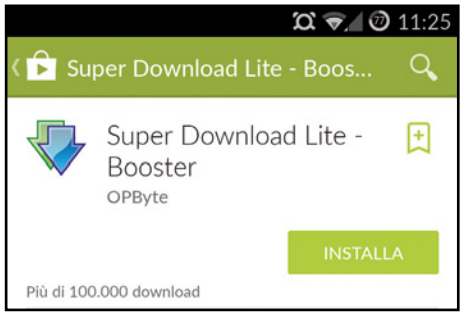
Rispetto a qualche anno fa, i luoghi dove è possibile disporre di una "doppia" connessione ad Internet sono in continuo aumento. Complice soprattutto della diffusione delle nuove tecnologie mobile: 3G ed LTE in primis. Poiché la banda a disposizione non è mai sufficiente per soddisfare in toto le nostre esigenze, una soluzione valida potrebbe essere quella di utilizzare contemporaneamente la connessione ADSL di casa e quella mobile in modo da sommare le loro velocità quando effettuiamo un download da Internet con il nostro smartphone o con il nostro PC. Samsung ha integrato nel suo ultimo dispositivo, il Galaxy S5, una funzione che prende il nome di Download Booster. Una volta attivata permette di scaricare file da Internet, con il proprio smartphone, utilizzando contemporaneamente sia la rete Wi-Fi che quella mobile.

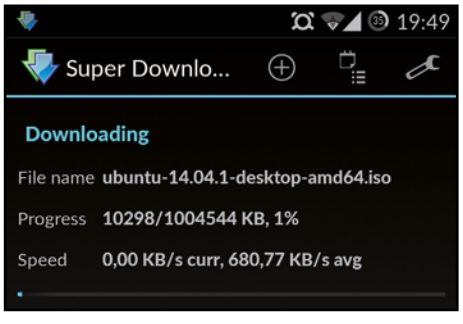
Download Booster per tutti

E per chi non dispone di un Samsung Galaxy S5? Fortunatamente Android è un sistema operativo completamente open source, ciò significa che tutti sono liberi di implementare applicazioni ed aggiungere nuove funzionalità. Sul play store ufficiale abbiamo scovato un'app "magica" (solo per i dispositivi del robottino verde) che consente di sfruttare le due reti (Wi-Fi/3G) contemporaneamente emulando in modo analogo l'impostazione Download Booster del Samsung Galaxy S5. L'applicazione si chiama Super Download Lite Booster, ed è disponibile in due versioni, quella gratuita (che permette di scaricare file di dimensioni inferiori a 50 MB) e la versione a pagamento (senza limitazioni) ad 1.49 €. Per utilizzare la funzione occorre però assegnare al proprio smartphone i permessi di root, questo perché è la parte centrale del sistema operativo che si occupa della distribuzione del carico tra le varie reti disponibili e per questioni di sicurezza, il Kernel non è accessibile da un "normale" utente.

A Scaricare a mille col cellulare

Per accelerare i nostri download, avremo bisogno di un'app che ci permetta di sommare la rete Wi-Fi alla rete 3G/LTE dello smartphone. Ecco la soluzione gratuita per i dispositivi Android.





1 Un'app nello store

Colleghiamoci al Google Play Store, cerchiamo ed installiamo l'app Super Download Lite Booster. L'applicazione è gratuita ma si limita a funzionare con file non più grandi di 50 MB. In alternativa è possibile scaricare la versione completa (a pagamento 1.49 €) senza nessun tipo di limitazione.

2 Permesso… prego!

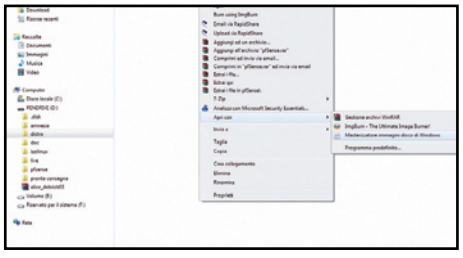
Come accennato in precedenza l'applicazione funziona solo su dispositivi su cui è stato abilitato il root. Al primo avvio di Super Download Lite Booster, infatti, ci verrà chiesto se assegnare o meno i permessi di root all'app. Ovviamente concediamogli questo privilegio cliccando su *Concedi*.

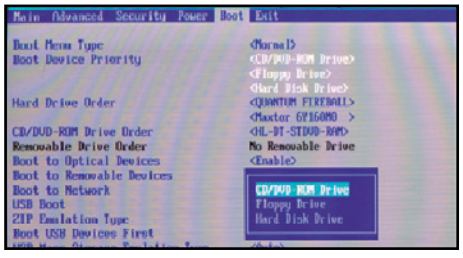
3 Siamo pronti!

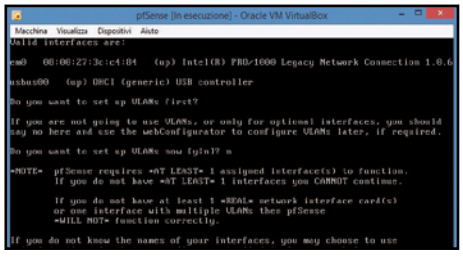
A questo punto non serve configurare più nulla, ci basterà navigare come sempre, ed ogni volta che avvieremo un nuovo download, questo verrà eseguito automaticamente dalla nuova applicazione che sfrutterà sia la connessione Wi-Fi che quella 3G.

Col PC l'ADSL raddoppia!

Vediamo come usare il software pfSense per trasformare un vecchio computer in router in grado di gestire due o più connessioni contemporaneamente. Avviamolo in modalità "live" ed impostiamo le prime scelte.







1 Prepariamo il disco

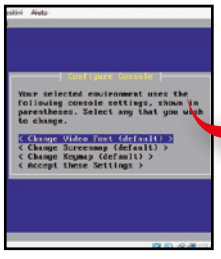
Estraiamo il file *pfSense.zip (lo trovi sul nostro Win DVD-Rom)* in una qualsiasi cartella dell'hard disk. Dobbiamo adesso masterizzare il file ISO su un CD vergine. Se usiamo Nero Burning Rom, dal menu *Masterizzatore* clicchiamo su *Scrivi Immagine disco*. Nella nuova schermata selezioniamo il file ISO, clicchiamo *Apri* e poi *Scrivi*.

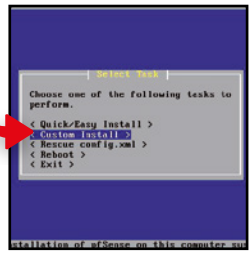
2 Boot da CD-ROM

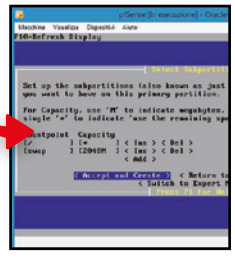
Sul PC che useremo per pfSense abilitiamo il boot da CD (l'operazione varia in base al tipo di scheda madre): all'accensione del PC premiamo *F2*, spostiamoci in *Boot/Boot Device Priority* e settiamo *CD/DVD-ROM Drive* come prima periferica d'avvio. Inseriamo il disco creato al **Passo 1** e attendiamo il caricamento del sistema operativo.

3 L'avvio

Nel menu d'avvio digitiamo *1*. Viene visualizzato l'elenco delle schede di rete compatibili installate nel PC. Digitiamo *em0* come nome della scheda da collegare ad un altro PC (LAN) per configurare la rete e confermiamo con *Invio*. Ripetiamo indicando il nome della scheda collegata fisicamente al router (*WAN*). Salviamo con *y*.







4 Installazione

Nella schermata di scelta, selezioniamo *99 (Install pfSense to a hard drive/memory drive, etc.)* e premiamo *Invio*. Mentre, nelle schermate successive, scegliamo in ordine le voci: *Accept these Setting* e *Custom Install*, confermando di volta in volta con il tasto *Invio*.

5 Selezioniamo l'hard disk

Dall'elenco dei dischi rigidi presenti nel PC, selezioniamo quello sul quale installare pfSense, diamo *Invio* e selezioniamo *Format this disk*. Nelle successive schermate, scegliamo in ordine: *Use this Geometry* e *Format ad0* confermando sempre con *Invio*.

6 Pochi altri passaggi

Il PC sarà un "super router" quindi non occorre partizionare il disco, saltiamo questo step con *Skip this Step*. Selezioniamo *Accept and Install Bootblocks* e confermiamo con *Accept and Create* attendendo la fine dell'installazione. Premiamo *reboot* e rimuoviamo il CD dal lettore.

C'è da dire che Super Download Booster può funzionare su di un singolo dispositivo, pertanto, dopo averla testata, abbiamo proseguito il nostro studio, alla ricerca di un metodo che ci permettesse di accelerare la velocità di download di un'intera rete, composta da più computer o dispositivi mobili. Per rendere possibile tutto questo, dobbiamo creare un "super router" (ossia un dispositivo in grado di decidere se e quando abilitare il traffico ad una seconda linea aggiuntiva) e utilizzare un sistema operativo capace di gestire funzionalità di rete avanzate, restando comunque semplice da configurare ed utilizzare.
Come super router, utilizzeremo un qualsiasi PC (anche uno di quelli riposti in garage tempo fa), sul quale installeremo una particolare distribuzione di FreeBSD come sistema operativo: pfSense. Grazie a questo software (totalmente gratuito), saremo in grado di utilizzare la linea ADSL di casa contemporaneamente ad una Internet Key. Sarà necessario che il super router resti sempre acceso per consentire l'accesso alla rete anche agli altri computer, in caso contrario, le due linee non saranno cumulate, quindi la velocità di download sarà quella standard.

Come funziona pfSense?

Il principio di funzionamento è semplice: il software ottimizza il traffico di rete bilanciando le richieste di download e navigazione, tra le diverse connessioni disponibili. Se ad esempio la linea ADSL di casa è sovraccarica, perché stiamo giocando on-line con la nostra console, o perché ci stiamo gustando un film in streaming, le altre richieste di navigazione verranno automaticamente smistate sulla linea ausiliaria (che nel nostro caso sarà la chiavetta Internet). Grazie a questa configurazione, saremo in grado di sfruttare ogni singolo bit delle linee a nostra disposizione. Vediamo come procedere.

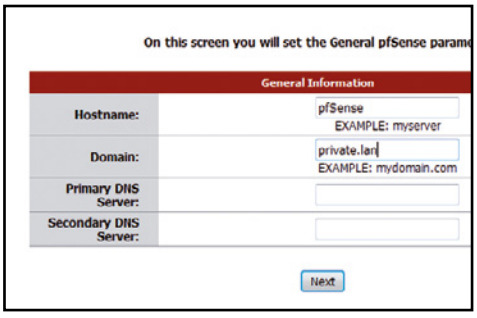
BUONI CONSIGLI

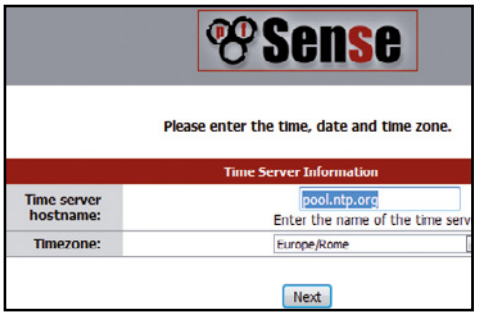
DOWNLOAD BOOSTER SU S5

La funzione si attiva accedendo alle *Impostazioni* del Samsung Galaxy S5 entrando nell'opzione *Download Booster*. Funziona solo sotto copertura LTE (non è compatibile con la rete 3G) e non può essere utilizzata per guardare video su YouTube o in streaming.

Configuriamo il Super Router

Da un altro PC collegato in LAN accediamo all'interfaccia di configurazione di pfSense. Abilitiamo il server DHCP per far gestire al router-PC tutti gli indirizzi IP dei computer collegati e attiviamo alcuni servizi fondamentali.





1 Inizia la configurazione

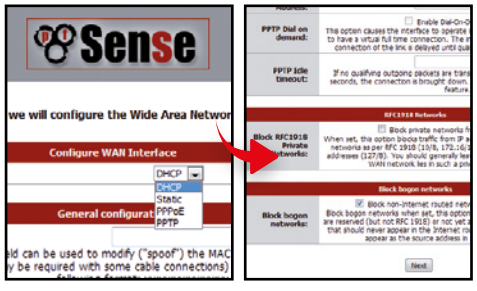
Tramite cavo Ethernet, colleghiamo il super router ad un altro PC (tramite la scheda di rete em0) da quest'ultimo, avviamo il browser web e colleghiamoci all'indirizzo *192.168.1.1* per caricare l'interfaccia di configurazione di pfSense. Avviamo la configurazione di base cliccando su tasto *Next*.

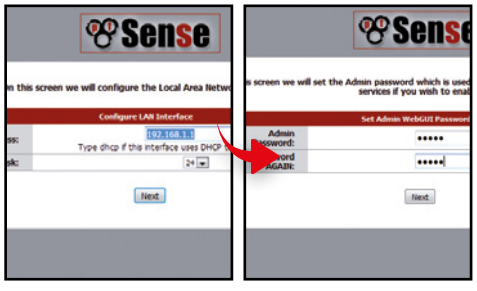
2 Parametri fondamentali

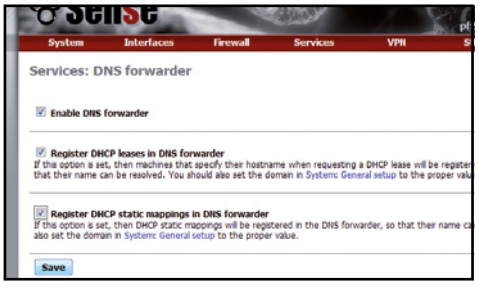
Nel campo *Hostname*, assegniamo un nome univoco al Pc, in modo da indentificarlo all'interno della nostra rete (nel nostro caso *pfSense*), compiliamo il campo *Domain name* con il testo *private.lan*. Per ora, lasciamo invariati i campi relativi ai server DNS e confermiamo cliccando sul tasto *Next*.

3 Sincronizziamoci

Per impostare la data e l'ora di sistema, pfSense si connette ad un server on-line che fornisce dei dati costantemente aggiornati. Compiliamo dunque il campo *Time server hostname* con l'indirizzo *pool.ntp.org*. Dal menu a tendina *Timezone* selezioniamo la voce *Europe/Rome*. Confermiamo con *Next*.







4 DHCP

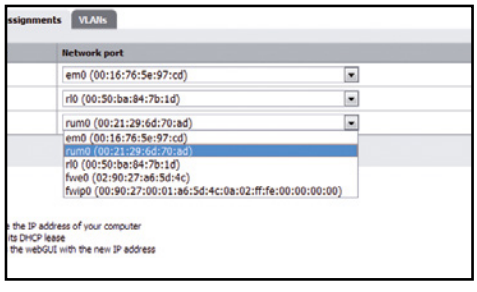
A questo punto, dal menu a tendina *SelectedType*, selezioniamo DHCP e lasciamo invariati gli altri campi. Scorriamo fino in fondo questa pagina di configurazione e mettiamo il segno di spunta all'opzione di *Block bogon net-works*. Confermiamo il tutto cliccando come sempre il tasto *Next*.

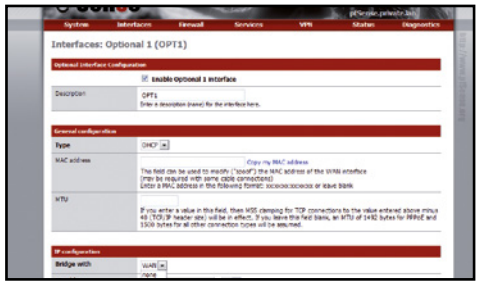
5 L'indirizzo del router PC

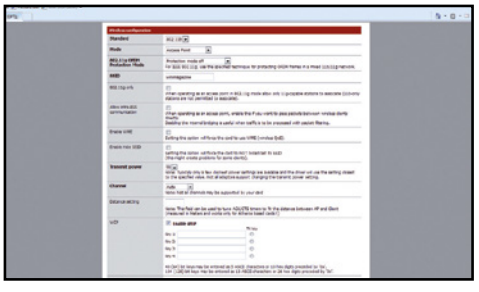
Compiliamo il campo *LAN IP Address* con l'indirizzo statico *192.168.1.1* e selezioniamo *24* dal menu a tendina *Subnet Mask*. Confermiamo con *Next*, indichiamo una password di protezione e, infine, clicchiamo sul pulsant *Next*.

6 Ultimi ritocchi

Ricarichiamo la pagina cliccando su *Reload* ed inseriamo la password scelta al passo precedente. Selezioniamo *DNS forwarder* dal menu *Services*. Abilitiamo le voci *Enable DNS forwarder, register DHCP leases* in *DNSforwarder* e *Register DHCP static mapping* in *DNS forwarder*. Confermiamo con *Save*.







7 Inseriamo il Wi-Fi

Inseriamo una scheda Wireless USB compatibile nel super router. Dal Pc connesso in LAN invece, sempre dall'interfaccia di *pfSense* (*192.168.1.1*), spostiamoci su *Interfaces/Assign*. Clicchiamo *Add* e dal menu a tendina selezioniamo la voce relativa alla periferica wireless (*rum0*). Confermiamo con *Save*.

8 Configuriamo il Wi-Fi

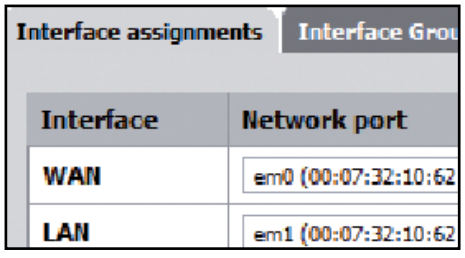
Selezioniamo la voce *OPT1* dal menu *Interfaces* e spuntiamo l'opzione *Enable Optional 1 interface*. Verifichiamo che il campo *Type* sia impostato su *DHCP* e cerchiamo la sezione *IP configuration*. Da qui selezioniamo la voce *WAN* dal menu a tendina *Bridge with*.

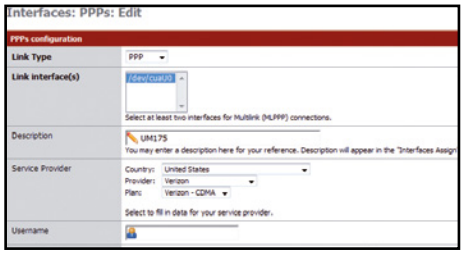
9 Proteggiamo la rete

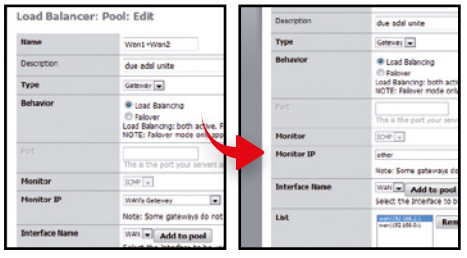
In *Wireless Configuration*, selezioniamo *Access Point* dal menu *Mode*. Scegliamo un nome per la rete e spuntiamo il campo *Enable WPA* per abilitare la protezione della rete. Digitiamo una psw e clicchiamo *Save*. Da adesso ogni dispositivo Wi-Fi in casa, sarà in grado di connettersi alla rete.

ADSL + Internet Key: si può!

Colleghiamo la linea ADSL e la Internet Key, in modo da unire le due connessioni con il Balancing e abilitiamo la gestione automatica dello smistamento dei dati.







1 Colleghiamo la chiavetta

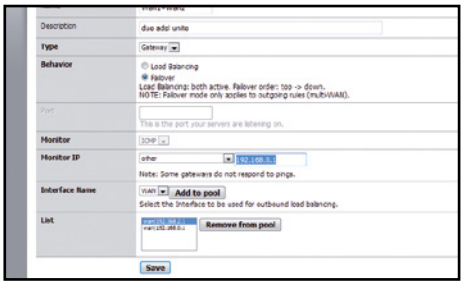
Inseriamo la chiavetta nel super router ed attendiamo che venga riconosciuta. Dall'altro PC, entriamo nella configurazione di pfSense come al **Macropasso 7** del punto precedente, accediamo ad Assign dal menu Intefaces, clicchiamo sull'icona *Add* e dal menu a tendina selezioniamo *PPP0*, quindi confermiamo con *Save*.

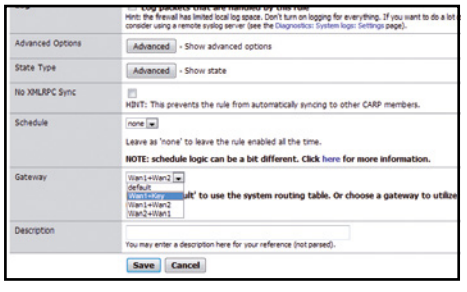
2 Impostiamo i parametri

Sempre da *Interfaces*, alla voce *PPPs*, scegliamo la voce *PPP* dal menu a tendina *Link Type* e verifichiamo che accanto a *Link interface(s)* venga visualizzato il percorso del modem 3G inserito (*dev/cuaU0*). Inseriamo quindi eventuali parametri di connessione, come ad esempio *Username*, *Password* ed *APN*.

3 Settiamo la linea principale

Da *Services*, clicchiamo su *Add* alla voce *Load Balancer*. Su *Name* digitiamo *Wan1 + Key*, da *Type* selezioniamo *Gateway*, abilitiamo *Load Balancing* in *Monitor IP*, quindi clicchiamo su *Add to pool* in... Da *Monitor Ip* selezioniamo *other* e digitiamo *192.168.0.1*. Scegliamo *WAN* ad Interface *Name* e clicchiamo *Add to Pool* e *Save*.





4 Tocca alla linea secondaria

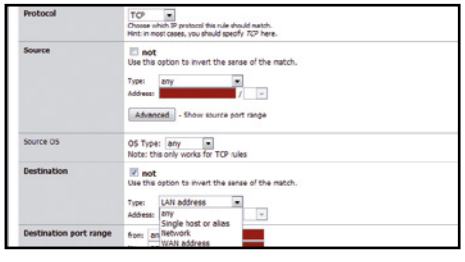
Ripetiamo il **passo 3**, inserendo come nome *Key+Wan1*. Inseriamo un *Gateway* con *Failover*. Da *Monitor IP* scegliamo *other* con l'indirizzo *192.168.0.1* e confermiamo con *Add to pool*, selezioniamo *Wan's Gateway* e aggiungiamolo con *Add to pool*. Salviamo.

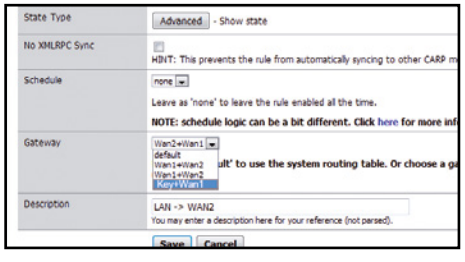
5 Smistiamo il traffico

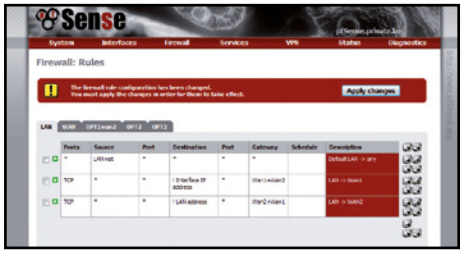
Dall'interfaccia Web selezioniamo *Firewall/Rules*. Dal menu *Action* selezioniamo *Pass* e spostiamoci in *Destination*. Qui mettiamo il segno di spunta sull'opzione *not* (stiamo ben attenti a non confonderci con *Source*); da *Type*, selezioniamo l'opzione *OPT1wan2 address*.

6 Scegliamo il gateway

Nella stessa pagina di configurazione, ricerchiamo la sezione *Gateway* e dal menu a tendina, selezioniamo *Wan1 + Key* (che abbiamo creato in precedenza). Inseriamo se vogliamo una descrizione generica nel campo *Description* e salviamo le modifiche apportate cliccando sul tasto *Save*.







7 Sull'altra linea

Clicchiamo su *Add* per creare una nuova regola. Selezioniamo *Pass* dal menu a tendina *Action* e spuntiamo l'opzione not di fianco a *Destination*. A differenza del **Passo 1**, dal menu *Type* selezioniamo *LAN Address*.

8 Quasi come prima

Ripetiamo la procedura attuata al **passo 2**, questa volta però scegliamo dal menu a tendina, la voce *Key + Wan1* nella sezione *Gateway*. Inseriamo la consueta descrizione per evitare di fare confusione. Salviamo quindi tutte le modifiche apportate cliccando sul tasto *Save*.

9 Controlliamo il tutto

Nel menu *rules di Firewall*, possiamo vedere uno schema riassuntivo di tutte le regole create. Se è andato tutto ok in LAN ci saranno 3 diverse regole. Se sono presenti clicchiamo su *Apply changes*. Il PC si riavvierà col turbo dei download inserito.

L'antifurto per il Wi-Fi

Ecco come creare una finta rete wireless "aperta" per attirare in trappola gli intrusi e scoprire quali sono le loro intenzioni

Cosa ci occorre

30 MIN.
DIFFICILE

STRUMENTO DI PROTEZIONE
HONEYDRIVEL
SOFTWARE COMPLETO
Lo trovi su: ☑DVD
Sito Internet:
http://bruteforce.gr/honeydrive

DIFESA

Per un pirata non è difficile riuscire a "bucare" le reti Wi-Fi altrui e intrufolarsi nella vita privata delle sue vittime per rubare dati personali di ogni tipo. Per fortuna esistono degli strumenti software particolari, come la distribuzione XiaoPan OS Pro, e alcuni dispositivi hardware a basso costo, facilmente reperibili su Internet, per allestire una finta rete Wi-Fi simile in tutto e per tutto a quelle che ognuno di noi utilizza quotidianamente a casa propria per collegare il PC, la Smart TV, lo smartphone e il tablet a Internet.

Esche per i pirati

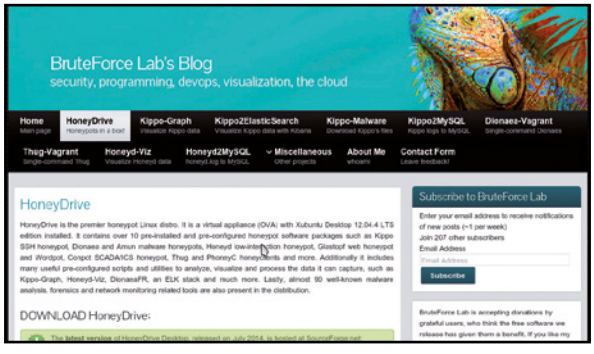
In questo articolo analizzeremo, invece, le tecniche di difesa che qualunque utente può mettere in pratica per intercettare e bloccare intrusioni non autorizzate alla propria LAN Wi-Fi. In particolare, vedremo come utilizzare il sistema operativo Honeydrive (basato sulla distribuzione Linux Xubuntu) che, come il nome stesso lascia intuire, serve per creare degli honeypot. Il termine inglese honeypot significa, letteralmente, vaso di miele e serve quindi a indicare una vera e propria trappola informatica per pirati. In poche parole, grazie agli strumenti integrati in Honeydrive riusciremo a configurare finti server costruiti volutamente in modo maldestro e insicuro proprio per invogliare i pirati ad attaccarli.

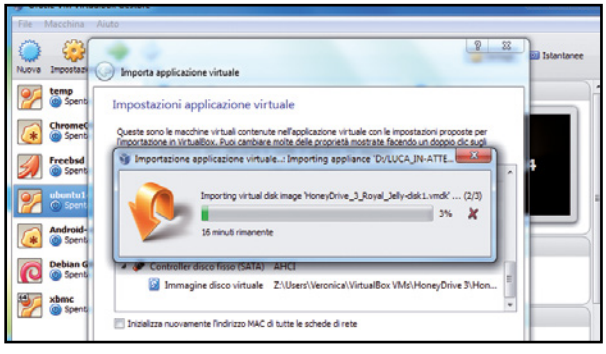
Uno strumento avanzato

I motivi che giustificano l'utilizzo di un honeypot sono sostanzialmente due: distogliere l'attenzione dal vero server e quindi, nel nostro caso, dal router Wi-Fi (il pirata at-

A Installiamo un honeypot in pochi

Per allestire una finta rete wireless con Honeydrive utilizzeremo una macchina virtuale creata con VirtualBox. Potremo così simulare la presenza di un server Web "attaccabile". Vediamo come.





1 Prepariamo la trappola

Scarichiamo la distribuzione Honeydrive dal nostro Win DVD-Rom: scompattiamo quindi l'archivio compresso per accedere all'immagine della distribuzione. Tale immagine, però, non è la solita ISO masterizzabile su DVD, ma si tratta di un'applicazione per macchine virtuali VirtualBox: al momento, quindi, archiviamola sull'hard disk.

2 Ecco la macchina virtuale

Sempre dal Win DVD-Rom scarichiamo anche VirtualBox e installiamolo. Al termine, potremo aprire il file di HoneyDrive con un doppio clic. Una semplice procedura guidata costruirà una macchina virtuale pienamente funzionante. Il file che abbiamo scaricato contiene un hard disk virtuale compresso, che viene estratto automaticamente.

COS'È L'HTTPS E A COSA SERVE IL PROTOCOLLO SSLSTRIP

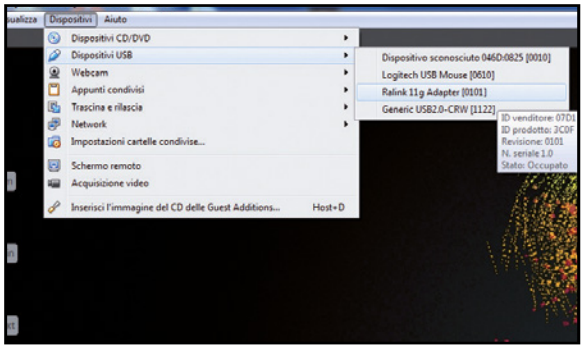
Il protocollo HTTPS è stato fondamentale per garantire la sicurezza del Web e la sua espansione: senza di esso sarebbe troppo rischioso scambiare informazioni confidenziali o fare acquisti online. E a parte qualche bug, come Heartbleed, ha svolto egregiamente il proprio lavoro. Fondamentalmente, si tratta di una versione crittografata di HTTP. Il tipo di traffico è lo stesso, si tratta pur sempre del Web, ma all'inizio della connessione il server e il client si scambiano dei certificati di sicurezza, tramite i quali possono crittografare i messaggi. In questo modo, solo quel server potrà leggere i messaggi inviati da quel client, e soltanto quel client potrà leggere le informazioni inviate dal quel server. Se qualcuno intercettasse la comunicazione, otterrebbe soltanto una sfilza di caratteri indecifrabili. Tuttavia, esiste un trucco per aggirare l'HTTPS: si chiama SSL STRIP (SSL è il nome della cifratura utilizzata in HTTPS). In poche parole, il pirata si inserisce come "Man In The Middle" nella comunicazione dell'utente vittima. Poi, quando rileva una richiesta HTTPS, finge di essere il server e di disporre solo di HTTP, così la vittima gli "parlerà" senza crittografia. A quel punto contatta il vero server Web e si fa inviare le pagine richieste dall'utente, inoltrandole poi alla vittima: l'unico modo che l'utente ha per accorgersi che qualcosa non funziona è controllare se il sito su cui stia navigando sia http:// o https://, cosa che quasi nessuno fa. Questo è l'unico modo per intercettare il traffico HTTPS, che è il più interessante per un pirata visto che al giorno d'oggi tutte le password viaggiano su di esso.

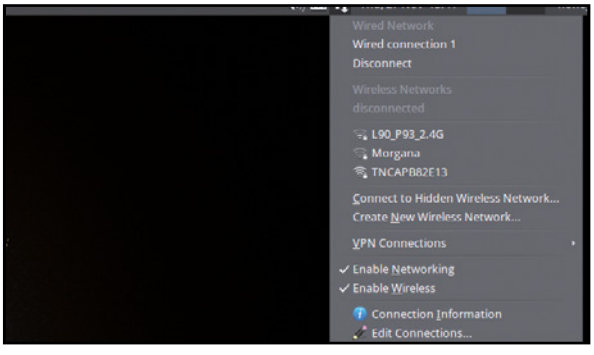
taccherà l'honeypot perché gli sembrerà più "dolce", ossia più facile da espugnare); registrare tutto ciò che accade nella finta rete locale (le informazioni ottenute durante l'attacco potranno essere utilizzate per riconoscere rapidamente il pirata quando tenterà di entrare nella LAN; in pratica, il pirata resterà "invischiato" nel miele). L'honeypot è dunque uno strumento di rete molto potente ma facilmente gestibile proprio grazie alla distribuzione Honeydrive che contiene già tutti gli strumenti necessari all'intercettazione del traffico Web degli utenti. Diversamente da un normale sistema GNU/Linux, però, viene fornito non come immagine ISO da masterizzare su DVD o da trasferire su pendrive USB, ma come macchina virtuale Virtual Box. Essendo infatti progettato per essere eseguito su un server, la cosa più logica consiste proprio nel virtualizzare il sistema operativo, in modo da poterlo eseguire in qualsiasi ambiente. Per realizzare una rete Wi-Fi "condivisa" sarà inoltre necessario disporre di un adattatore Wi-Fi USB che utilizzeremo come punto di accesso, in modo che l'hot spot creato sia visibile anche fuori dalle mura domestiche.

Occhio a non cascarci

Purtroppo, però, l'honeypot può trasformarsi facilmente in un'arma a doppio taglio: se da una parte può tornarci utile per creare una sorta di "area minata" a protezione della nostra rete Wi-Fi, dall'altra può essere sfruttato dai pirati per creare a loro volta finte reti wireless "aperte" alle quali potremmo essere tentati di collegarci quando siamo in giro con lo smartphone o il tablet: il rischio, in questo caso, è che tutto il nostro traffico Internet venga intercettato e sniffato dal pirata. Uno spiacevole risvolto degli honeypot che, però, ci suggerisce come fuori casa, in assenza di una rete Wi-Fi "fidata", è meglio usare la connessione 3G del nostro smartphone, che non può essere intercettata così facilmente! Fatta questa dovuta raccomandazione, rimbocchiamoci le mani e impariamo a proteggere al meglio la nostra rete domestica.

clic del mouse





3 Abilitiamo i dispositivi USB

L'avvio della macchina virtuale è abbastanza veloce: appena il desktop è pronto, possiamo collegare l'adattatore Wi-Fi esterno al PC. Poi, dobbiamo abilitarlo nella macchina virtuale cliccando sul menu *Dispositivi/Dispositivi USB di VirtualBox* e selezionando il nome dell'adattatore (se non lo facciamo, la macchina virtuale non avrà il Wi-Fi).

4 Attiviamo le connessioni di rete

Come ultima cosa clicchiamo sull'icona del Network Manager, che dovrebbe apparire come due frecce verticali antiparallele nella barra di stato di HoneyDrive. È importante verificare che sia attivata la connessione Ethernet (chiamata *Wired connection 1*). Dovremmo anche notare la disponibilità di alcune reti Wi-Fi presenti nella zona limitrofa al nostro PC.

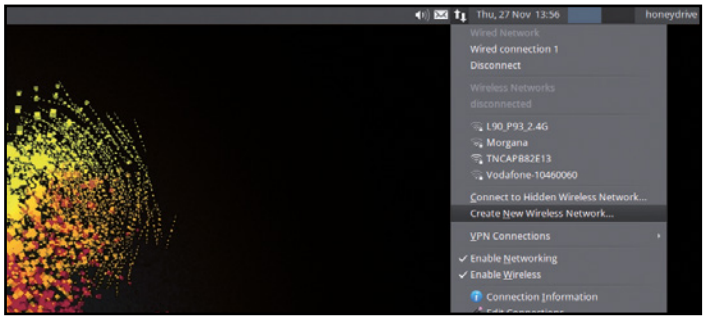
BUONI CONSIGLI

SPIARE DA WINDOWS

Anche con Windows è possibile realizzare delle reti condivise, anche se è un po' più complesso rispetto a HoneyDrive. Si deve entrare nel *Pannello di controllo*, cercare l'icona *Centro reti e condivisioni* e aggiungere una nuova connessione. Dalla procedura guidata che appare si deve poi scegliere la voce *Wireless Ad-hoc* e seguire le istruzioni. Si potrebbe, quindi, realizzare una trappola Wi-Fi anche su Windows. Il problema (per il pirata) è che, al momento, non esistono strumenti per Windows capaci di fare l'SSLstrip. Non si può quindi intercettare il traffico HTTPS. Esiste il programma Intercepter-NG (http://intercepter.nerf.ru), che dovrebbe svolgere automaticamente tutte le attività necessarie all'intercettazione del traffico Web. Tuttavia, al momento non funziona con l'HTTPS. Il software è molto comodo ed è quasi preoccupante perché se funzionasse renderebbe l'intercettazione talmente semplice da essere alla portata di chiunque.

B Dall'hot spot allo sniffing

Un honeypot permette di attirare in trappola un pirata per analizzarne e anticiparne le mosse. Ricordiamo che creare una rete condivisa è legale, ma non lo è sfruttarla per intercettare il traffico degli utenti connessi.

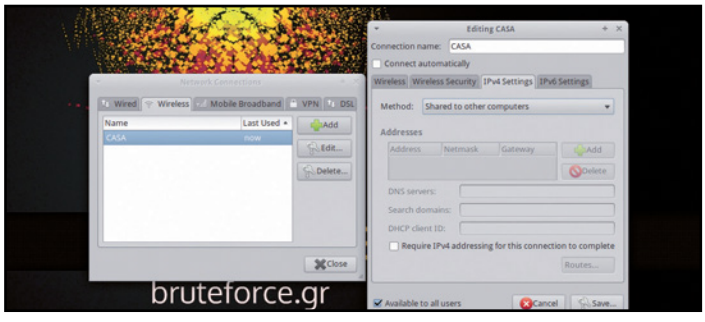


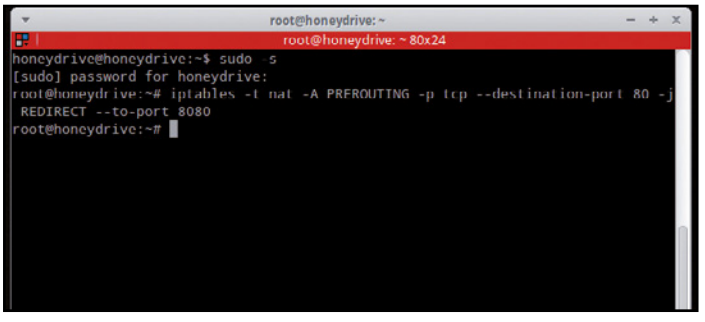
1 Una nuova rete ad hoc…

In Honeydrive, cliccando sull'icona del Network Manager è possibile creare una nuova rete. In particolare, ciò che ci interessa è creare una rete Wi-Fi ad-hoc: esistono diversi metodi per farlo ma, visto che non vogliamo inserire password di protezione, la procedura più semplice consiste nel cliccare sulla voce di menu *Create New Wireless Network*.

2 … senza password di accesso

Una finestra di dialogo ci chiede di specificare le caratteristiche della rete. Per rendere la nostra rete aperta a tutti dobbiamo impostare *Wireless Security* su *None*. Il nome della rete è importante: possiamo sceglierne uno qualsiasi, ma è meglio optare per uno banale che dia l'impressione di una rete creata da uno sprovveduto (per esempio *CASA* o *gianni*).



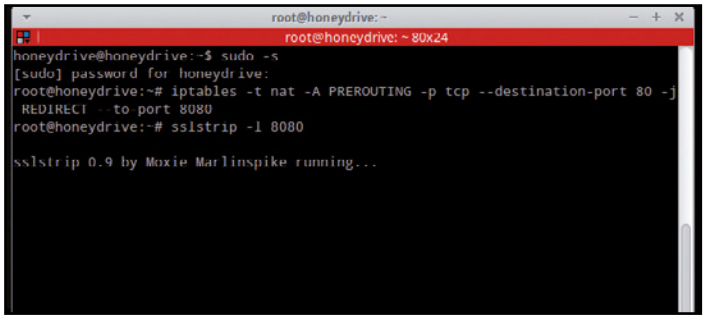


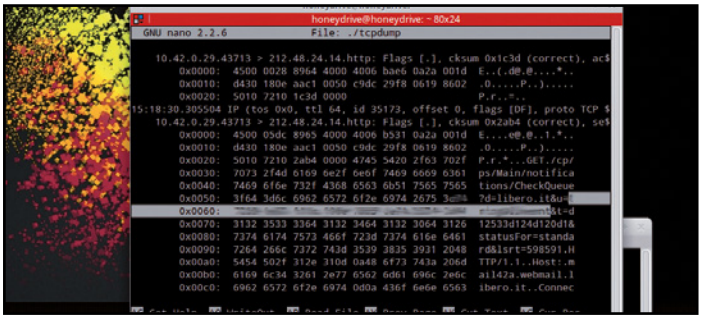
3 Condividiamo l'accesso

Dopo aver cliccato su *Create*, clicchiamo nuovamente sull'icona del *Network Manager* e scegliamo *Edit connections*. Nella scheda *Wireless* scegliamo la rete appena creata e clicchiamo su *Edit*. Dalla finestra che si apre, entriamo nella scheda *Ipv4 Settings* e assicuriamoci che *Method* sia impostato su *Shared to other computers*. Lo stesso vale per la scheda *IPv6*.

4 Teniamo d'occhio il pirata

Possiamo iniziare a sniffare il traffico Web dell'intruso (ricordiamo che lo sniffing di rete è illegale, quindi effettuiamolo solo all'interno della nostra rete). Per farlo, apriamo un terminale e digitiamo il comando *sudo iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080* per dirottare il traffico generato dall'intruso.





5 L'HTTPS è sconfitto

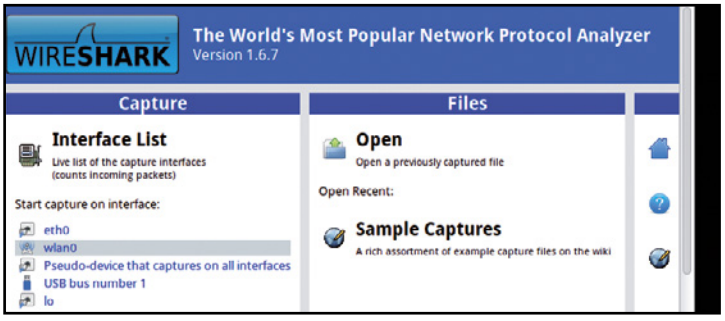
Posizioniamoci come "Man In The Middle" (uomo in ascolto) per intercettare il traffico tra l'intruso e il nostro server. Eseguiamo il comando *sudo sslstrip -l 8080* per tradurre le richieste HTTPS in HTTP e intercettare eventuali comunicazioni cifrate.

6 Ora tutto il traffico HTTP e HTTPS è visibile

In un altra finestra del terminale diamo il comando *sudo tcpdump -i wlan0 -v -X*: in questo modo potremo intercettare tutto il traffico degli utenti connessi, password comprese. Se aggiungiamo *> ./dump* alla fine del comando, i dati verranno registrati in un file dump nella home di Honeydrive.

L'altra faccia della medaglia

L'honeypot è un potente strumento utilizzabile per creare una trappola in cui attirare eventuali intrusi. Anche i pirati, però, potrebbero sfruttarne uno per fare abboccare noi all'esca e rubare i nostri dati personali.

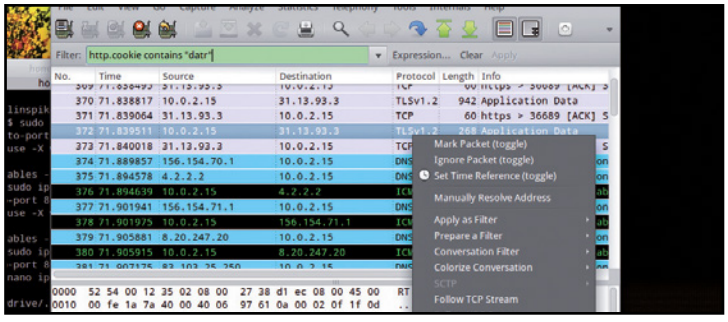


1 Basta uno script per il browser

Sfruttando un honeypot, un eventuale pirata potrebbe invogliarci ad entrare nella sue rete "libera" col solo scopo di intercettare la nostra navigazione, rubare i cookie che i siti Web inviano al nostro browser quando li visitiamo e "clonare" la nostra identità. Per farlo, gli basta usare Firefox, l'add-on Greasemonkey e lo script Original Cookie Injector.

2 Uno sniffer di rete

Il malintenzionato apre uno sniffer di pacchetti: al posto di tcpdump preferisce il più comodo Wireshark, che avvia con il comando ***sudo wireshark***. Alla schermata di benvenuto, il pirata sceglie l'interfaccia di rete con la quale vuole lavorare: ovviamente sceglierà ***wlan0***, perché rappresenta l'antenna Wi-Fi.



3 Bastano solo i cookie

I pacchetti Web che viaggiano sono moltissimi, ma al pirata interessano soltanto i cookie. Per visualizzare quelli di Facebook scrive nella barra del filtro la frase ***http.cookie contains "datr"***. In pratica, ogni volta che un sito invierà all'utente i cookie, il pirata li potrà intercettare: appena ne trova uno, ci clicca sopra col tasto destro del mouse.

4 Identità clonata!

Dal menu che appare, il pirata sceglie *Copy/Bytes/Printable Text Only*. Torna su Firefox e apre il sito www.facebook.com (senza però fare il login). Preme i tasti ***Alt+C*** e incolla il testo copiato nella casella che appare (***Ctrl+V***). Appena clicca ***OK***, si ritrova loggato in Facebook col profilo dell'utente a cui ha rubato il cookie!

COSA RISCHIAMO SE UN PIRATA CI RUBA I COOKIE O LE PASSWORD

ACCESSI NON AUTORIZZATI A FACEBOOK

Ottenuto l'SSLStrip, il pirata può rubarci qualsiasi password e qualsiasi cookie. Ciò che preoccupa, è pensare cosa possa fare un pirata quando dispone, ad esempio, dell'accesso completo al nostro profilo Facebook. Potrebbe leggere tutte le nostre conversazioni private, spiare le fotografie non pubbliche e scrivere messaggi a nostro nome, importunando i nostri amici.

ACQUISTI ILLECITI SU AMAZON

La questione si fa più seria nel caso in cui ci venga rubato l'accesso ad Amazon. Su questo sito, infatti, avremo di certo memorizzato i dati della nostra carta di credito per eseguire facilmente gli acquisti. Ciò significa che un pirata, con in mano il nostro account Amazon, può acquistare oggetti addebitandoli sulla nostra carta (ad esempio dei buoni regalo che non necessitano di spedizione). Se non siamo attenti, possono trascorrere dei giorni prima di accorgerci dell'esistenza di un pagamento "anomalo" sull'estratto conto.

SU GOOGLE C'È DI TUTTO E DI PIÙ!

L'account più "pericoloso", in caso di furto di credenziali, è quello di Google. Un pirata può accedere alla nostra Gmail, alla rubrica Android con decine di numeri di telefono privati, o accedere a Google Drive e spulciare tra documenti personali e di lavoro). Può leggere i nostri appuntamenti su Google Calendar e sfruttare la cosa per appostarci. Si è già verificato che maniaci e stalker sfruttino le tecnologie informatiche per perseguitare le persone verso cui provano un'attenzione morbosa.

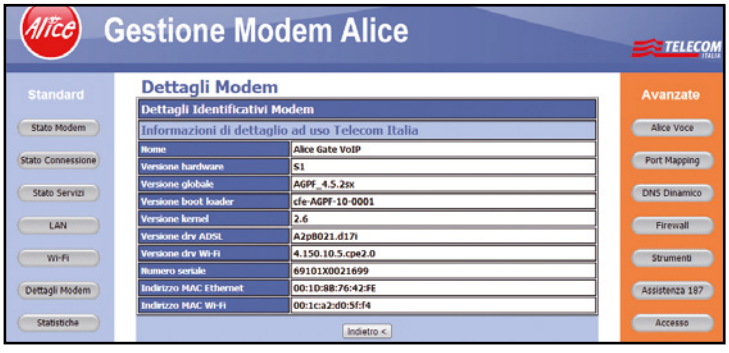
IL FURTO DELLA PEC

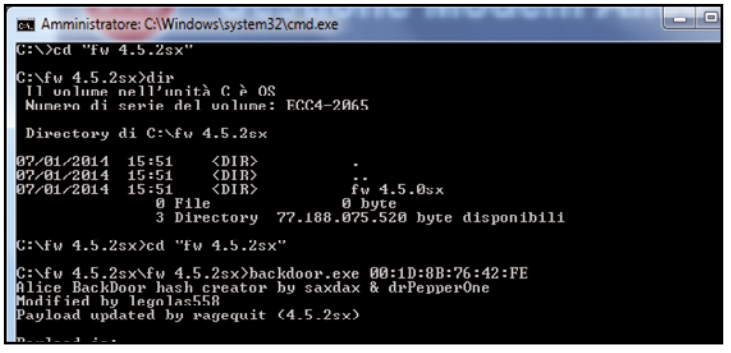
Oggi, molte persone dispongono di una casella di Posta Elettronica Certificata, con la quale si possono inviare documenti con valore legale anche dallo smartphone. Attenzione, però: se siamo caduti nella trappola Wi-Fi di un pirata, questo potrà scoprire la nostra password di accesso alla PEC. Il malintenzionato potrà così inviare email a chiunque per nostro conto, con un indirizzo di posta che ha valore legale per identificarci. In caso di problemi dovremo dimostrare di aver subito un furto di credenziali: e non è di certo facile. Solo per fare un esempio, il pirata potrebbe richiedere a nostro nome di rescindere o di attivare contratti con aziende e fornitori di servizi, semplicemente inviando un'e-mail.

"Così sblocco il router Alice"

Ecco come i pirati attivano un pannello di controllo avanzato per navigare più veloci senza smontare nulla

L'Alice Gate VoIP Plus Wi-Fi è uno dei router più diffusi e uno dei modelli preferiti dai pirati. Tale dispositivo può essere modificato abilitando funzionalità aggiuntive che lo trasformano in un NAS o in un perfetto media center. Ma, almeno fino a poco tempo fa, per sbloccare il proprio router il pirata era costretto a smontarlo, creare un ponticello tra due contatti elettrici e affrontare una lunga procedura di aggiornamento. Troppo macchinoso per i neofiti! Adesso, invece, sfruttando una vulnerabilità presente nella versione 4.5.2 del software installato sul router (abbiamo verificato nei nostri laboratori che con altre versioni la procedura è del tutto inutile), il processo di modding, cioè di modifica, può essere effettuato senza troppe difficoltà restando comodamente seduti di fronte al monitor. ***Ovviamente la procedura non è per nulla legale considerato che il router in questione è offerto in comodato d'uso gratuito dal maggiore provider ADSL italiano. Limitiamoci dunque ad analizzare le mosse del pirata evitando di metterle in pratica!***



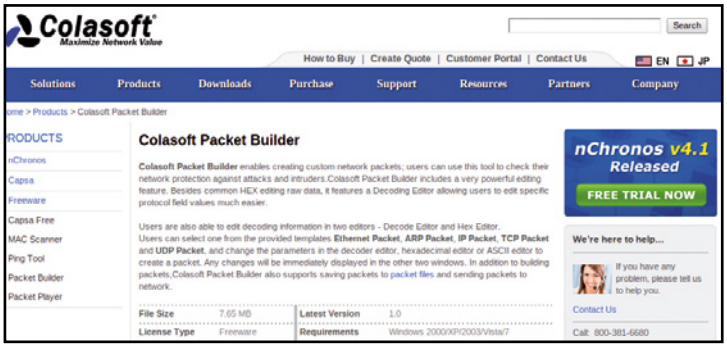


I requisiti devono essere soddisfatti

1 Il pirata avvia il browser e raggiunge l'interfaccia Web del router (*192.168.1.1*). Si sposta in *Dettagli Modem* e verifica che la *Versione globale* sia la *4.5.2*. In caso contrario la modifica non andrà a buon fine. Il pirata annota anche l'Indirizzo *MAC Ethernet* indicato.

Ecco il payload necessario per la modifica

2 Il pirata ricerca sul Web il pacchetto *backdoor_agpf_ 4.5.2.tar.gz*: dopo averlo estratto, avvia il Prompt dei comandi e raggiunge la directory nella quale è presente il file. Lancia il comando *backdoor.exe* seguito dal MAC annotato in precedenza e annota il *Payload* mostrato in output.

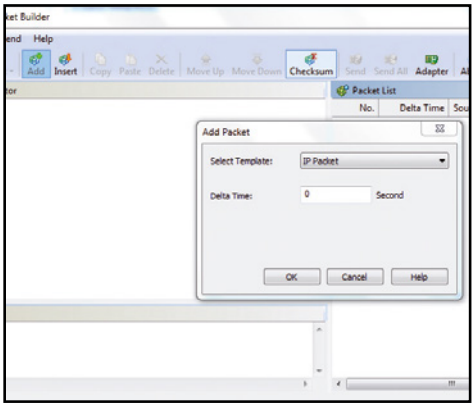


Il tool giusto per apportare le modifiche

3 Il pirata raggiunge la pagina Web www.colasoft.com/packet_builder ed effettua il download dell'ultima release disponibile del software, rigorosamente gratuito, Packet Builder. Al termine, effettua un doppio clic sul file appena scaricato e segue la procedura di installazione guidata.

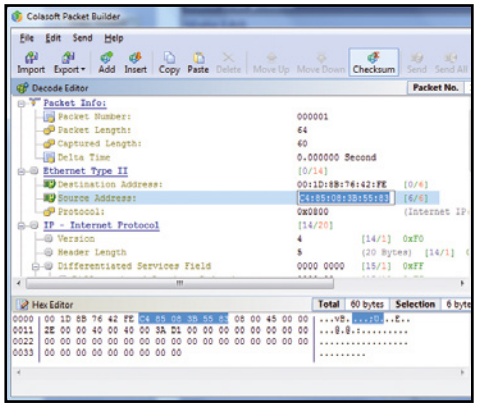
Il divertimento ha inizio!

4 A questo punto il pirata spunta l'opzione *Launch Colasoft Packet Builder 1.0* e clicca sul pulsante *Finish*. Tutto ciò che è necessario per portare a termine la modifica del router Alice Gate VoIP Plus Wi-Fi è ora pronto: non gli resta che entrare nel vivo dell'azione!



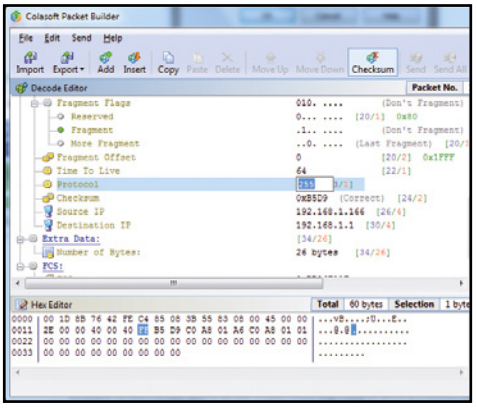
Pacchetto fai da te

5 Dall'interfaccia principale di Packet Builder il pirata clicca sul pulsante *Add* e dal menu a tendina *Select Template* seleziona la voce *IP Packet*. Si sposta quindi nel campo *Delta Time* e setta un valore pari a *0 secondi*. Non gli resta che confermare con clic su *OK*.



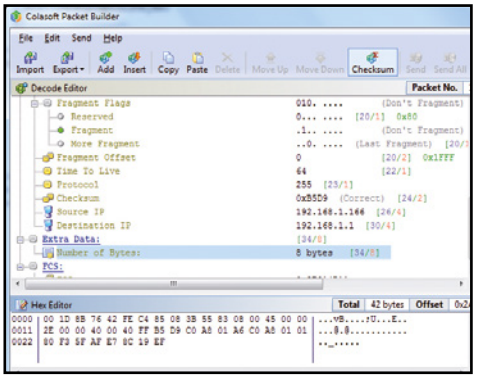
Il MAC del router Wi-Fi...

6 Da *Decode Editor* si sposta nella sezione *Ethernet Type II* e compila il campo *Destination Address* con il MAC del router annotato al **Passo 1**. Compila poi *Source Address* con il MAC della scheda di rete del computer che sta utilizzando per la procedura di sblocco del router.



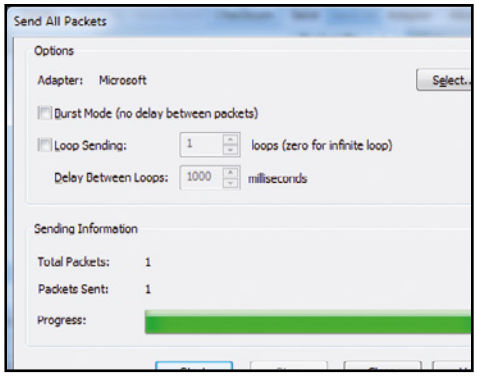
... e l'indirizzo IP del computer

7 Il pirata si sposta poco più in basso e nel campo *Protocol* setta un valore pari a *255*. Inserisce in *Source IP* l'indirizzo assegnato al proprio PC (nel caso in figura *192.168.1.166*). Al contrario, in *Destination IP*, indica quello del router (che di default è *192.168.1.1*).



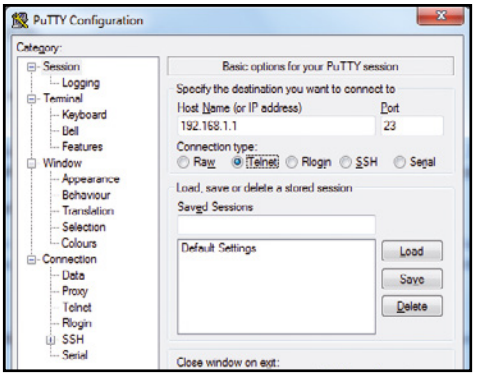
Serve il payload giusto!

8 Per il pirata è arrivato il momento di inserire il payload annotato al **Passo 2**. Si sposta in *Number of Byte* e sostituisce la prima coppia di zeri con la prima coppia esadecimale del payload proseguendo fino all'inserimento totale. Verifica poi che *Number of Bytes* diventi *8 bytes*.



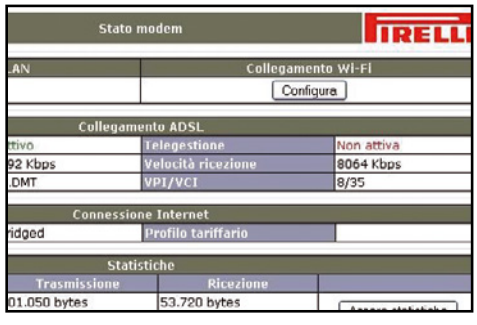
Il pacchetto è stato inviato…

9 Al pirata non resta che cliccare sul pulsante *Send All* e, nella nuova finestra che appare, premere su *Select*. Dal menu a tendina *Adapter* il pirata indica la scheda di rete in uso e conferma prima con *OK* e successivamente con *Start*. Il pacchetto è stato inviato al router!



... e il router è sbloccato!

10 Se tutto è andato per il verso giusto, il protocollo Telnet è ora attivo sul router. Per verificarlo, il pirata informatico scarica dal Web il software gratuito PuTTY e, dopo averlo avviato, compila il campo *Host Name* con *192.168.1.1* e seleziona *Telnet* da *Connection type*.



Ecco la nuova interfaccia

11 Se richiesti, indica *admin* come username e *riattizzati* come password. Il pirata digita *conf set /wbm/admin_on 1* seguito da *conf reconf 1*. Disattiva la telegestione del provider con *conf set /cwmp/enabled 0* e *conf reconf 1* e si gode la nuova interfaccia Web su 192.168.1.1/admin.html.

C'È SEMPRE UN PREZZO DA PAGARE!

La procedura di sblocco del router Alice Gate VoIP Plus WiFi mostrata nell'articolo è da considerarsi del tutto illegale. Come già detto, infatti, il router non è di proprietà dell'utente, ma viene concesso in comodato d'uso da Telecom. Inoltre, in caso di malfunzionamento della linea ADSL, l'operatore del centro assistenza non sarà in grado di accedere da remoto al pannello di amministrazione (utilizzando la cosiddetta telegestione, che però viene disabilitata dopo lo sblocco, **Passo 11**) e ciò determinerebbe un allungamento dei tempi di riparazione della linea telefonica stessa. Il pirata che decide di modificare il suo router, dunque, deve ben comprendere che non solo sta effettuando un qualcosa di illegale, ma che gli si potrebbe ritorcere anche contro. Il gioco vale davvero la candela?

Tutti hacker, ma per gioco!

In regalo il simulatore di hacking per divertirsi a mettere sotto scacco il Web. Ecco come funziona

Cosa ci occorre

30 MIN.
DIFFICILE

SIMULAZIONE HACKING
MOTHER
Lo trovi su: ☑DVD
Quanto costa: **Gratuito**
Sito Internet: **www.v4ldemar.net/projects/mother**

Diversi anni addietro la software house Inglese Introversion Software (www.introversion.co.uk) lanciava sul mercato il gioco Uplink (www.introversion.co.uk/uplink) che ancora oggi, a oltre un decennio dalla sua pubblicazione, è possibile acquistare nei diversi store dedicati ai videogiochi, come ad esempio Steam (http://steamcommunity.com/app/1510). La particolarità di questo videogame è quella di offrire al giocatore la possibilità di trasformarsi in pochi minuti in un abile hacker nel mondo di Internet dell'anno 2010, in un periodo caratterizzato da innumerevoli crimini tecnologici e spionaggio industriale. Il programmatore italiano Massimo "v4ldemar" Pinzaglia rimase talmente affascinato e attratto da questo titolo videoludico che diede vita al suo progetto Mother.

Il problema è risolto!

Mother è in pratica un simulatore di hacking ambientato in un futuro prossimo dove Internet, in seguito ad un collasso strutturale, non esiste più. Il suo posto è stato preso dalla rete Network nella quale le grandi corporazioni (lobby) fanno di tutto per regnare incontrastate. Ma Mother è anche il nome del nuovo sistema operativo rivoluzionario che utilizzeremo per emulare (senza violare alcuna legge nel mondo reale) le gesta di un vero hacker! Dimentichiamoci pertanto i classici "sparatutto" con decine di armi al seguito, qui la fa da padrona la pazienza e l'arte di nascondersi/mascherarsi poiché il campo di battaglia sarà proprio quella nuova rete sostituiva di Internet, il Network, che vede da un lato le diverse corporazioni e dall'altro i difensori della libertà di informazione senza se e senza ma!

Installiamo Mother sul PC

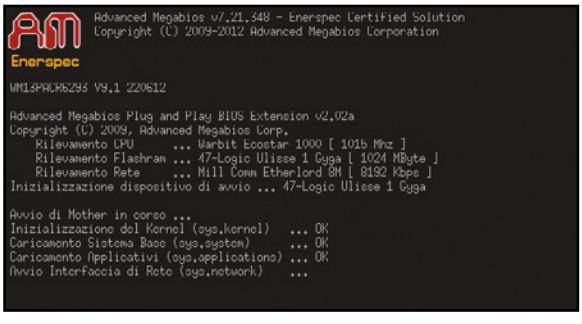
Per mettere alla prova le nostre capacità di hacker procediamo innanzitutto all'installazione del simulatore. Al termine, saremo pronti per tuffarci nel misterioso mondo dei pirati informatici!

1 Cartella di destinazione

Facciamo doppio clic sul file *mother-v1.0.exe* per avviare la procedura di installazione. Dopo aver cliccato su *Avanti* e accettato i termini di licenza ci ritroveremo nella scelta della cartella di installazione: il percorso predefinito è *C:\Programmi\Mother*.

2 Installazione in corso

Qualora volessimo cambiarla è sufficiente cliccare su *Sfoglia* e scegliere il nuovo percorso. Effettuata la scelta clicchiamo su *Avanti* anche nelle finestre successive, poi *Selezioni componenti* e *Selezione della cartella nel menu Avvio/Start*, quindi su *Installa*.

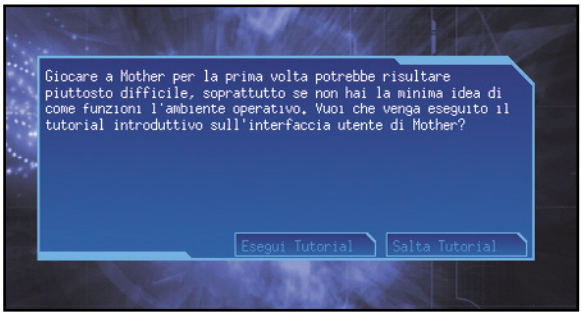


3 Avviamo l'emulatore

Al termine dell'installazione potremo avviare subito Mother mantenendo spuntata la casella *Avvia subito Mother* e cliccando su *Fine*. Verrà caricato il simulatore di gioco il quale si avvierà come un vero sistema operativo mostrando i messaggi del kernel.

4 Creiamo un account utente…

Se stiamo utilizzando Windows Vista non possiamo eseguire il gioco. Dobbiamo procedere dapprima all'aggiornamento seguendo quanto riportato nel box di fianco *Update necessari*. Per creare un nuovo account inseriamo username e password e clicchiamo su *Login*.



5 … e poi registriamolo

Poiché al primo avvio non sarà presente alcun utente registrato ci verrà ricordato che tale account non esiste e se vogliamo registrarne le credenziali riportate. Clicchiamo su *Conferma* per accedere al gioco dove verremo accolti dalla schermata di Mother.

6 Impostazioni del gioco

La registrazione dell'account fa parte della simulazione del gioco e non ha niente a che vedere con community Web ecc: tutto avviene in locale. Prima di creare l'account o effettuare il login impostiamo le proprietà del simulatore (sfondi, audio ecc) cliccando sull'icona "i" in basso a destra.

BUONI CONSIGLI

UPDATE NECESSARI

Nel tutorial sono stati illustrati due passi dell'installazione con riferimento all'eseguibile *mother-v1.0.exe*. Facciamo presente che, seguendo la stessa dinamica, possiamo, e se utilizziamo Windows Vista dobbiamo, procedere all'installazione di almeno due patch (presenti sul Win DVD-Rom): la 1.01, file *mother-v1.01-upgrade.exe*, e la 1.02 con il file *mother-v1.02-upgrade.exe*. Attenzione però, non possiamo installare direttamente la patch 1.02 ma dobbiamo assicurarci di avere già precedentemente aggiornato il gioco alla versione 1.01! Solo a questo punto possiamo procedere all'aggiornamento alla versione 1.02 la quale corregge problemi minori e, soprattutto, introduce il supporto a Windows Vista, diversamente non potremo lanciare il gioco se è in uso questa versione di Windows.

NUOVI SUONI

C'è un pacchetto che rientra negli aggiornamenti facoltativi ed è indipendente dalla versione di Windows in uso. Permette di avere temi sonori differenti da quelli presenti nella versione originale del gioco. La patch *mother-v1.02pcwed-music_patch.zip*, che pesa poco meno di 15 MB, è installabile decomprimendo il contenuto dell'archivio nella cartella radice di installazione del gioco (di default in *C:\Programmi\Mother*), confermando eventuali richieste di sovrascrittura di file. Nella pratica verrà sovrascritto il file *sounds.dat* presente nella cartella *data*.

BUONI CONSIGLI

UTENTI E SERVER

Durante il normale uso del simulatore potrebbe capitare di creare più di qualche account utente. Dove vengono registrati? Semplice, nella cartella *users* nel percorso di installazione: ad ogni nuovo account corrisponde una cartella dedicata con il medesimo nome dell'account. I server che compaiono negli screenshot di queste pagine sono invece presenti in *dataservers* nel percorso di installazione. Il numero è elevato pertanto non facciamoci ingannare dai pochi incontrati nei tutorial.**

MANUALE ON-LINE

Nel pacchetto di installazione è presente un manuale completo che può essere consultato utilizzando anche il browser. È possibile leggerlo in maniera indipendente dal gioco andando nel percorso di installazione di Mother e aprendo il file *manual.html*. Il gioco è localizzato interamente in italiano quindi non dovremo preoccuparci di installare alcun file di lingua oppure di procedere a traduzioni di voci/frasi non comprensibili.

LE RISORSE INIZIALI

Ricordiamo che il simulatore ha un comportamento "quasi reale": ad esempio le attese per la ricezione delle e-mail rispecchia con una certa fedeltà la realtà. Anche per il cracking delle password dovremo attendere che il software specifico porti a termine la sua procedura! Così come nei server di chat dovremo attendere l'arrivo di nuovi messaggi.

Tecniche hacker per tutti

Avviato Mother, dobbiamo apprendere l'ABC del simulatore. Per farlo è opportuno seguire il tutorial di base a cui farà seguito uno scambio di e-mail con il primo hacker!

1 Avviamo il tutorial

Al primo login come nuovo utente (la stessa finestra si presenterà, pertanto, anche se provassimo a registrare un secondo utente) verrà chiesto se vogliamo eseguire il tutorial di base. Clicchiamo su *Esegui Tutorial* per vedere apparire un riquadro in basso.

2 Colleghiamoci al Network!

Nel corso del tutorial verrà illustrato e descritto, passo dopo passo tramite l'ausilio del riquadro e accompagnati da un tema sonoro accattivante, il significato delle varie voci. Seguiamo con attenzione cercando di entrare subito nell'ottica di gioco.

3 Acquisti on-line

Per poter acquistare utility che possano aiutare a farci uscire dal pietoso stato di *Lamer*, dovremo collegarci con un nodo (server) e procedere agli acquisti di ciò che ci occorre, in funzione del *Credito*, la moneta della rete Network, a disposizione.

4 Vari tipi di nodi

Ogni nodo (server) ha la sua peculiarità, esattamente come accade in una reale connessione di rete. Troveremo quindi server di news, chat server, server per acquisti on-line e server da violare per poter migliorare la nostra posizione nella community.

5 Comunicazioni in corso

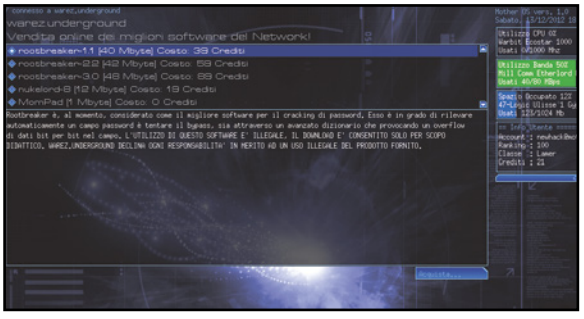
Al termine del tutorial di base ci arriverà una e-mail di aiuto dall'hacker *1ronch4ang* che provvederemo ad aprire e leggere attentamente. Risponderemo cliccando sul pulsante *Invia*: la scrittura avverrà automaticamente, quindi dovremo attendere qualche secondo.

6 Un attacco guidato

Il nostro "amico" hacker 1ronch4ang ci ha risposto (ce ne accorgiamo osservando il numero di e-mail in basso a sinistra) allegando il tutorial *tut_hack-1.0* che avvieremo cliccando sul pulsante *M* in basso a destra (l'equivalente del menu *Start* in Windows).

C Via con l'attacco guidato!

Nella e-mail il nostro amico ci dirà come procedere per effettuare un attacco. L'obiettivo è migliorare il proprio ranking nell'immediato e guadagnare Credito in un futuro prossimo!



1 Un tentativo inutile!

Il primo tentativo di collegamento al server *test1.valdenet* risulterà vano poiché l'accesso è protetto dall'usuale richiesta di username e password. Dobbiamo quindi superare il problema acquistando un software di cracking adatto allo scopo.

2 È tempo di shopping!

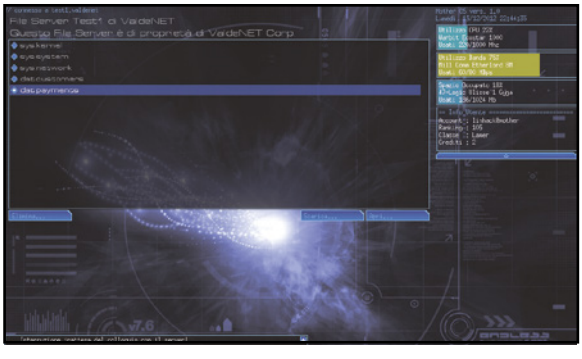
Per portare a termine il primo acquisto on-line colleghiamoci al server *werez.underground*: clicchiamo sul server nella *Network Map* e su *Connetti* in basso a destra. Quindi procediamo all'acquisto del software *rootbreaker* per il cracking delle password.

3 D'obbligo la maschera!

Al termine del download possiamo subito utilizzare il software, ma c'è un altro problema che dobbiamo risolvere: ci occorre un software che possa mascherare il nostro IP. Si chiama *Back Mirror* e dobbiamo procedere al suo acquisto.

4 Avviamo l'istallazione

A questo punto, dopo aver messo *Back Mirror* "in ascolto" e aiutandoci con *rootbreaker* per violare la password, proviamo ad eseguire nuovamente l'accesso al server *test1.valdenet* attendendo il tempo necessario al cracking.



5 Entrati nel server!

Una volta entrati nel server eseguiamo qualche operazione, ad esempio il download di un file presente e solo al termine rimuoviamo la connessione, non prima però di aver cancellato il file di log (*log.connections*) per non lasciare tracce.

6 Soli con le nostre incertezze!

Arrivati a questo punto dovremo proseguire tenendo bene a mente i due obiettivi: uscire dalla condizione di Lamer e guadagnare qualcosa. Iniziamo a connetterci al server di chat e attendiamo i messaggi degli utenti e una nuova e-mail!

BUONI CONSIGLI

SOLUZIONE ON-LINE

Alcuni siti specializzati, e anche diversi blog di utenti che hanno provato e portato a termine il gioco, forniscono la soluzione completa: una serie di istruzioni da seguire passo dopo passo ma a cui non vi rimandiamo altrimenti verrebbe meno il gusto di giocare. Ci si potrebbe far ricorso qualora ci si fosse arenati in una determinata situazione.

ANCHE CON LINUX!

Diversi utenti Windows hanno un dual boot sul proprio PC desktop e/o portatile con il sistema operativo del Pinguino. La versione di Mother che abbiamo qui presentato è disponibile solo per Windows. È possibile, però, giocare anche su GNU/Linux utilizzando il "ricostruttore" WINE (www.winehq.org) che dovrà essere installato utilizzando il gestore dei pacchetti della propria distribuzione. L'installazione avverrà da terminale utilizzando il comando wine *mother-v1.0.exe*.

IL FUTURO DEL GIOCO

Abbiamo accennato come giocare con Mother su GNU/Linux. La nuova versione del simulatore supporterà i tre sistemi operativi più comuni: Microsoft Windows, Mac OS X e GNU/Linux. Al momento, però, è ancora in una acerba versione "alpha" pertanto è soggetta a tutti i problemi tipici quali non completezza di alcune fasi di gioco e bassa stabilità.

Abbiamo scoperto il Web segreto

C'è una porta nascosta del Web dalla quale si accede ad un archivio di comunicazioni private

Cosa ci occorre

30 MIN.
FACILE

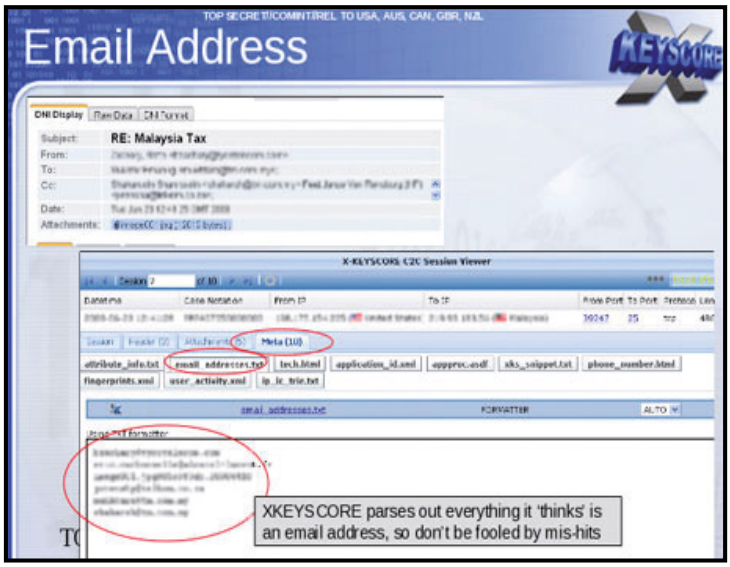
BROWSER DI NAVIGAZIONE ANONIMA
TOPSECRET EXPLORER
☑DVD
SOFTWARE COMPLETO
Note: Il software che ci permette di accedere agli archivi segreti del Web si chiama Tor Browser, che noi abbiamo ribattezzato come Top Secret Explorer

Negli ultimi mesi, i media di tutto il mondo hanno parlato dello scandalo NSA, la National Security Agency, ovvero l'organismo governativo degli Stati Uniti d'America che, insieme alla CIA e all'FBI, si occupa della sicurezza nazionale. A gridare allo scandalo è stato l'ex tecnico della CIA Edward Snowden, il quale ha dichiarato, con ingenti quantitativi di prove, che il sistema per la sicurezza nazionale è sempre andato ben oltre i limiti imposti all'interno degli accordi Internazionali e le attività di "controllo" si estendevano anche, senza permesso, ad intercettazioni di telefonate, fax e dati anche su altri paesi ed in particolar modo su politici esteri di un certo spessore (ultima saltata alla ribalta dello scandalo NSA è stata la Cancellieria dell Germania, Angela Merkel)

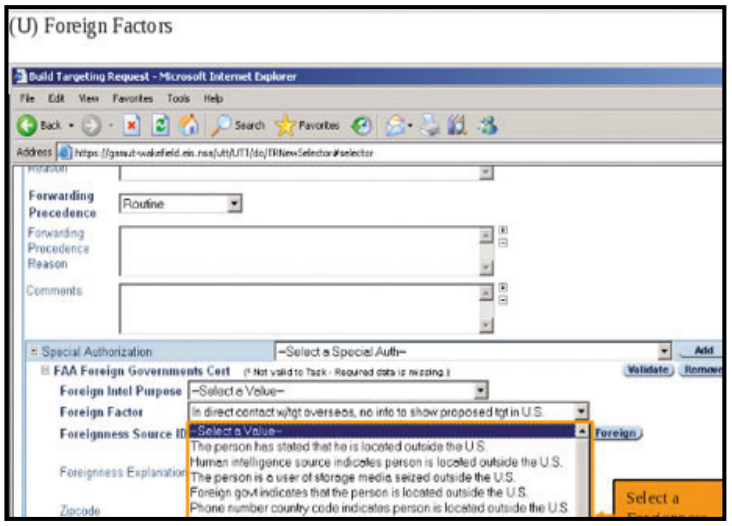
Xkeyscore: il software per le intercettazioni

Spesso può sembrare quasi impossibile che informazioni così riservate, come possono essere le telefonate di alti capi di Stato, siano intercettate così facilmente da enti esterni. Ma le prove rilasciate da Snowden, e pubblicate anche all'interno di archivi come WikiLeaks e Cryptome, non lasciano dubbi sull'invasione dei sistemi utilizzati principalmente dagli Stati Uniti per garantire una sicurezza nazionale quanto più possibile. **Il software utilizzato dall'agenzia NSA per le intercettazioni è saltato allo scoperto grazie ad un articolo apparso sul giornale "The Guardian" di alcuni mesi fa. Tale programma prende il nome di Xkeyscore e permette di accedere ai dati della cronologia di navigazione, di quella di ricerca, alle mail, alle telefonate ed alle conversazioni private su Facebook.**

I documenti messi on line dal Guardian e da altri quotidiani, tra cui Le Monde, mettono in luce il suo funzionamento. La NSA lo definisce come un strumento che permette di esaminare «quasi



Il software Xkeyscore in azione per il filtraggio delle e-mail.



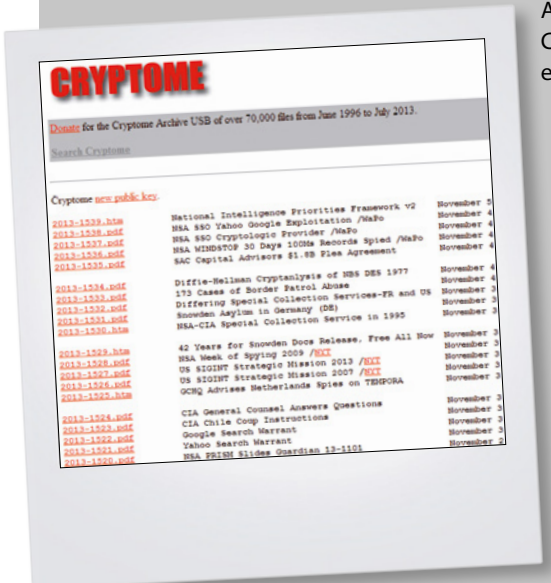
I filtri di Xkeyscore permettono di indicare la tipologia di persona da filtrare (è possibile selezionare se l'utente sta parlando "in codice", se si trova all'esterno o all'interno del territorio USA).

tutto quello che un individuo fa su Internet».
Secondo le rivelazioni diffuse da Snowden il software Xkeyscore è in grado di analizzare anche le conversazioni cifrate. Sulla base di alcuni screenshot rilasciati sembrerebbe possibile, infatti, poter risalire a tutte le informazioni che vengono trasmesse in forma nascosta per poi successivamente decifrare in maniera del tutto automatica. Secondo la documentazione ufficiale NSA i dati vengono memorizzati per un massimo di 5 giorni, tranne quelli ritenuti di estrema importanza. Dopo la divulgazione di queste molteplici informazioni la NSA ha pubblicato la seguente dichiarazione sul quotidiano "The Guardian": *«Le affermazioni secondo le quali ci sarebbe un accesso generalizzato e senza controllo alcuno dei nostri analisti ai dati raccolti dalla Nsa è falsa. L'accesso a Xkeyscore è limitato al personale che ne ha bisogno nello svolgimento del suo lavoro».*
Gli Stati Uniti D'America affermano che l'intercettazioni di ingenti quantità di dati sia effettivamente reale, ma che la loro analisi venga effettuata solamente verso individui che potrebbero mettere a rischio la sicurezza Nazionale e non.

Cryptome: l'antenato di wikileaks

Quando WikiLeaks, la creatura di Julian Assange su cui in questi giorni è uscito un film nelle sale cinematografiche di tutto il mondo dal titolo "Il Quinto Potere", saltò alla ribalta nel 2009 (in realtà il sito era online dal 2006) pochi sapevano che fin dal 1996 esisteva un portale, chiamato Cryptome, dove informazioni riservate ad analoghe, i cosidetti "leaks", venivano pubblicati alla portata di tutti senza alcun tipo di censura.Ancora oggi Cryptome è online e continua a riscuotere moltissimo successo pur non essendo mai balzato sui media come invece è successo su WikiLeaks. Grazie ad una serie di ricerche siamo riusciti a recuperare documenti inediti riguardanti l'Italia. In queste pagine vogliamo mostrarvi delle foto in esclusiva riguardanti la tragedia della Costa Concordia, foto mai divulgate pubblicamente e scattate direttamente dalle aziende che hanno avuto l'incarico di assicurare il relitto e procedere allo smaltimento di quest'ultimo. Accedere a Cryptome è un'operazione che non richiede alcun tipo di conoscenza tecnica ed il suo utilizzo è molto più intuitivo di WikiLeaks. Basterà infatti accedere con il proprio browser all'indirizzo http://cryptome.org/ per essere proiettati all'interno di migliaia di documenti strettamente riservati che mai avrebbero dovuto vedere la luce. **L'archivio di Cryptome al momento contiene oltre 70.000 documenti inviati in forma anonima da attivisti di tutto il mondo**. Le fonti rimangono sempre sconosciute grazie alla possibilità di inviare messaggi anonimi allo staff del portale grazie ad una chiave pubblica ed una chiave privata.

SU CRYPTOME DOCUMENTI INEDITI SUL NOSTRO PAESE

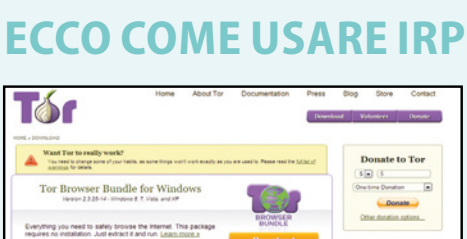


All'interno dell'archivio italiano disponibile su Cryptome sono state trovate anche delle foto esclusive e ad alta risoluzione sul naufragio della Concordia, scattate direttamente dai responsabili della messa in sicurezza del relitto e mai divulgate sui media.

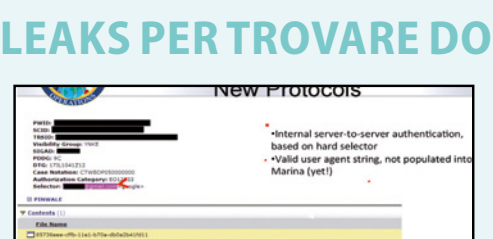
NASCE IRPILEAKS: IL "WIKILEAKS" ITALIANO

Dopo Cryptome e WikiLeaks sono nati in tutti gli stati dei portali che hanno come scopo quello di collezionare i documenti riservati della propria nazione. Anche in Italia abbiamo un progetto analogo ed il suo nome è "IrpiLeaks" (accessibile da: https://irpi.eu/irpileaks/?lang=it). Il progetto è stato realizzato ed è sostenuto dal Centro Studi Hermes per la Trasparenza e Diritti Umani Digitali (http://logioshermes.org/). L'intero sistema si basa sull'utilizzo di Tor, già integrato nella piattaforma, che risulta essere la miglior tecnologia di anonimato a disposizione degli utenti su Internet, ed è costantemente soggetto a revisioni da parte di esperti della sicurezza. Tor garantisce che nessuna traccia personale rimanga su IrpiLeaks. vIrpi suddivide le informazioni in diverse categorie al fine di renderle accessibili più facilmente sulla base dei propri interessi personali: Spesa pubblica, Frodi, Finanza, Criminalità organizzata ed Ambiente. Il portale pubblica materiale anche in lingua Inglese al fine di poter rendere internazionale la diffusione delle notizie sopra-riportate. Come per WikiLeaks e Cryptome anche Irpi permette di caricare, per chi lo desidera, qualsiasi tipo di materiale senza dover compromettere la propria identità. All'interno dello stesso portale è disponibile un'ampia guida per aiutare i "whistleblower", ovvero coloro che vogliono diffondere una notizia di cui sono a conoscenza e che è reputata "Top Secret", ad effettuare l'upload del materiale.

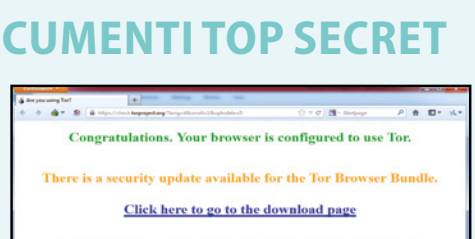
ECCO COME USARE IRPILEAKS PER TROVARE DOCUMENTI TOP SECRET



1 Il primo passo consiste nello scaricare dal nostro Win CD/DVD –Rom (sezione Indispensabili) il software TOR Browser.



2 Scompattiamo l'archivio sul Desktop o in qualsiasi altra cartella all'interno del computer. Non sono necessarie installazioni.



3 Per poter avviare il browser TOR basterà adesso fare doppio click sull'applicazione "Start Tor Browser" e al termine inserire l'indirizzo https://irpi.eu/irpileaks/?lang=it

Gli ultimi documenti che appaiono all'interno della Homepage del portale riguardano quasi esclusivamente lo scandalo NSA ed in particolar modo una serie di slide Powerpoint che mostra nei dettagli i sistemi utilizzati dall'ente governativo per mantenere sotto controllo le conversazioni di moltissimi Stati stranieri.

MafiaLeaks per combattere la mafia Italiana

Se CryptoMe, WikiLeaks e IRPILeaks sono portali in cui è possibile inviare o leggere documentazioni riservata a livello generale, MafiaLeaks (www.mafialeaks.org) è il primo portale al mondo verticale di questa tipologia. Il servizio, basato anch'esso sulla rete TOR, permette di divulgare in forma completamente anonima qualsiasi informazione inerente alla Mafia italiana. Lo scopo di MafiaLeaks è quello di funzionare da intermediario tra coloro che possiedono determinate informazioni riservate e le "persone fidate" in grado di combattere oppure aiutare le vittime di mafia. Sul portale MafiaLeaks si legge:
«Le persone fidate sono le persone che riceveranno la tua segnalazione. Le informazioni che tu deciderai di svelare attraverso la nostra piattaforma non verranno inviate indiscriminatamente a tutti ma sarai tu a scegliere a chi farle pervenire. Il nostro elenco di persone fidate è in aggiornamento e stiamo lavorando per aumentare il loro numero.»

La lista al momento comprende: Forze dell'ordine (per agire), giornalisti (per informare) e associazioni antimafia (per aiutare).

COSÌ I DOCUMENTI RISERVATI VIAGGIANO NELLA RETE

1 Scarica Tor

Scarica il browser Tor Bundle dal link che trovi sopra.

Salva la Cartella Tor sul tuo Desktop.

2 Apri Tor & IRPILEAKS

Apri la Cartella Tor e fai doppio click sul file Start Tor Browser.exe.

Copia l'indirizzo di IRPILEAKS che trovi sopra e incollalo nella barra di navigazione di Tor.

3 Invia una Segnalazione

Se vuoi inviare una Segnalazione clicca sul tasto Invia una Segnalazione.

Se invece hai già inviato una Segnalazione, digita il codice della Ricevuta per modificarla.

4 Argomento & Destinatario

Scegli l'Argomento più pertinente alla tua Segnalazione e indica il Destinatario della stessa.

5 Compila il form

Compila il form nel modo più dettagliato possibile.

Qualora desideraste venire contattati, aggiungete dei contatti di riferimento..

6 Carica i file

Clicca su Aggiungi File per condividere documenti a sostegno della tua Segnalazione.

Per noi è fondamentale poter provarne la genuinità.

7 Accetta & invia

Clicca su Accetto soltanto dopo aver letto attentamente le istruzioni.

Invia la tua Segnalazione.

8 Conserva la Ricevuta

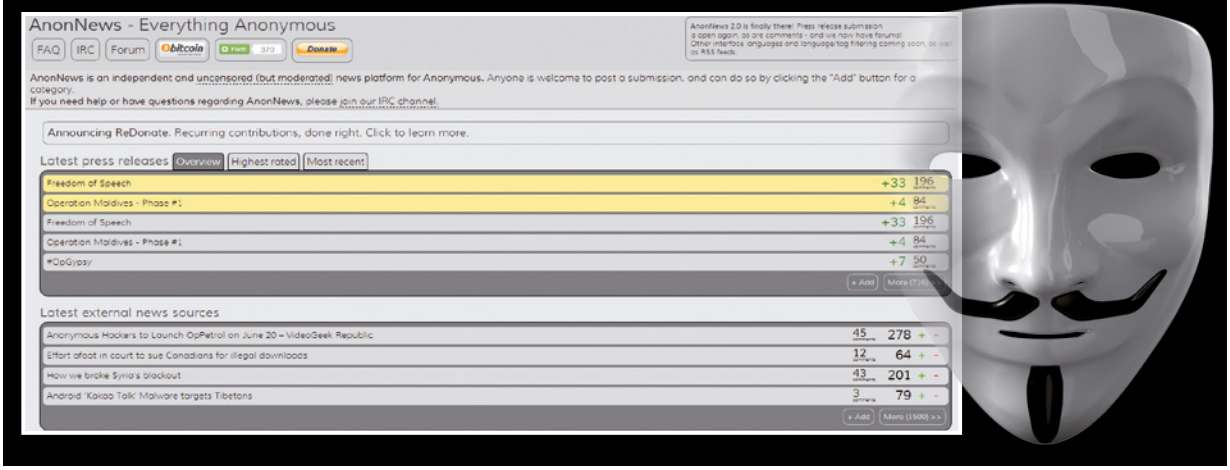
Conserva la Ricevuta che appare sullo schermo ma ***non salvarla sul tuo computer***!

La Ricevuta ti consentirà di accedere alla tua Segnalazione in futuro.

ANONNEWS: PER CHI RIMANE NEL SILENZIO

Molte fughe di notizie o di Hacktivism rimangono spesso nel silenzio: questo accade perchè spesso i Media non danno l'importanza di un attacco Hacktivism quanto ad una fuga di notizie come quanto avvenuto per l'NSA, ma in Rete il portale AnonNews (www.anonnews.org) ha lo scopo di raccogliere gli attacchi portati a termine da parte dei gruppi Anonymous.

All'interno di AnonNews sono riportate notizie che, a causa della censura, non vengono spesso pubblicate all'interno di molti quotidiani, principalmente legati alle questioni Siriane. AnonNews è, infatti, anche un canale di comunicazione che, grazie alla rete TOR su cui si basa come tutti i servizi visti in precedenza, permette di bypassare i filtri che i diversi stati abilitano per il controllo delle notizie.



COSA VUOL DIRE

NSA: National Security Agency, organismo degli USA che si occupa della sicurezza nazionale.

CIA: Central Intelligence Agency, l'agenzia di spionaggio degli USA, responsabile dell'ottenimento e dell'analisi delle informazioni sui governi stranieri, sulle società ed individui

FBI: Federal Bureau of Investigation, ente investigativo di polizia federale, principale braccio operativo del Dipartimento della Giustizia degli Stati Uniti

Edward Snowden: Ex tecnico della CIA ed ex collaboratore della Booz Allen Hamilton (azienda di tecnologia informatica consulente della NSA, la National Security Agency) noto per aver rivelato pubblicamente dettagli di diversi programmi di sorveglianza di massa del governo statunitense e britannico, fino ad allora tenuti segreti

Cryptome: Portale nato nel 1996 con lo scopo di raccogliere e pubblicare i documenti TopSecret

WikiLeaks: Portale nato nel 2006 da Julian Assange saltato alla ribalta dei media dopo la pubblicazione dei "War Log" americani e di video militari riservati

NoForn: Dicitur utilizzata all'interno dei documenti Americani per indicare il materiale che non deve essere condiviso con Stati stranieri, anche se amici.

TOR: Sistema che permette di navigare completamente anonimi sfruttando dei proxy

Whistleblower: Utenti che sono in possesso di materiale riservato e decidono di renderlo pubblico.

C'è chi ha trovato un modo per scroccare la connessione Wi-Fi altrui e navigare senza spendere un euro...

ADSL gratis su tablet e cellulari

Cosa ci occorre 30 MIN. DIFFICILE

TESTER PER RETI WI-FI
WPA TESTER
SOFTWARE COMPLETO
Sito Internet:
www.winmagazine.it/link/2196

SUITE DI PENETRATION TEST
DSPLOIT
SOFTWARE COMPLETO
Sito Internet:
www.dsploit.net

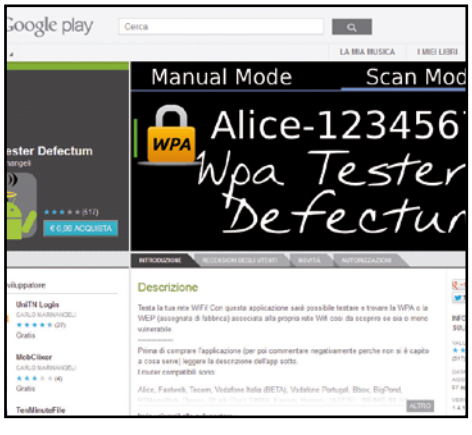
Come sanno bene tutti coloro che accedono a Internet usando una rete senza fili, al pirata bastano pochi secondi per intrufolarsi in una LAN e navigare a scrocco. Ma potrebbe anche accedere ai file e alle risorse condivise, invadendo la nostra privacy. La cosa più preoccupante è che per farlo gli basta un semplice smartphone: dimentichiamoci, quindi, il solito smanettone occhialuto seduto dietro un computer in una stanza buia tutto il giorno. Con un telefonino e le app giuste, chiunque abbia un minimo di conoscenze tecniche può andarsene in giro per la città a "bucare" reti wireless e scorrazzare liberamente tra cartelle, dati e risorse condivise. Il grimaldello preferito dai pirati è WPA Tester, un'applicazione scaricabile dal Play Store di Google nata col nobile intento di consentire a chiunque di testare la sicurezza della chiave di accesso alla propria rete Wi-Fi, ma che nelle mani sbagliate si trasforma in un pericoloso passpartout per le porte dei router!

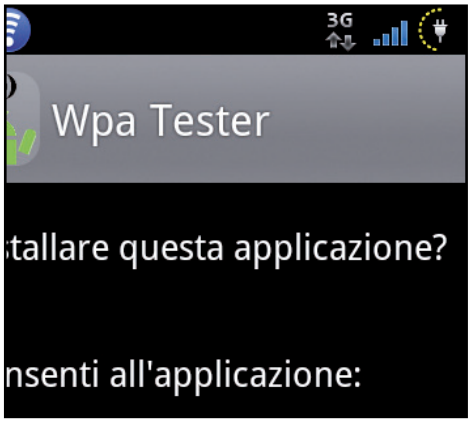
Una suite tuttofare

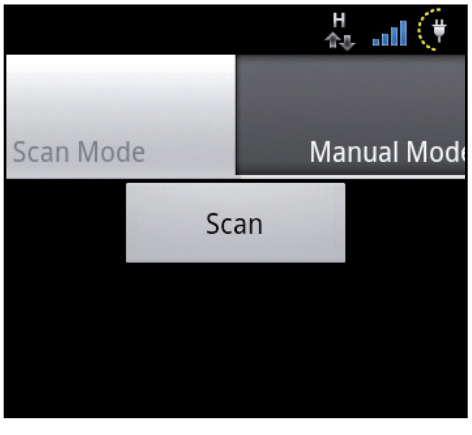
Il perfetto complemento di WPA Tester è poi un'altra applicazione sviluppata da un gruppo di hacker e che può essere definita senza problemi la BackTrack per smartphone, cioè la versione mobile della nota distribuzione Linux già configurata con tutti gli strumenti utili per testare la sicurezza delle reti (Wi-Fi e cablate). Gli strumenti messi a disposizione da dSploit, questo il nome dell'applicazione, sono veramente infiniti e la sua semplicità d'uso è disarmante. Anche gli utenti meno esperti possono analizzare le vulnerabilità riscontrate in tutti i dispositivi connessi alla stessa rete dello smartphone o sniffare password in chiaro. Resta sottinteso che l'utilizzo che ne faremo nel tutorial è solo a scopo didattico, per mettere alla prova la sicurezza della nostra rete WLAN e conoscere gli strumenti utilizzati dai pirati così da poterli contrastare sul loro stesso terreno.

A Reti Wi-Fi: pochissimi secondi e la

Prima di tutto, il pirata scopre la chiave per l'accesso alle reti wireless da attaccare. Usando un tool come WPA Tester o AircrackGUI gli bastano pochi secondi, perché spesso gli utenti non modificano la password predefinita!







Download dell'app

1 WPA Tester è presente a pagamento nel *Play Store* di Google, ma può essere comunque scaricata gratuitamente anche dall'indirizzo www.winmagazine.it/link/2197. Terminato il download del file *WpaTester.apk*, il pirata trasferisce il file nella memoria dello smartphone.

Installazione in corso

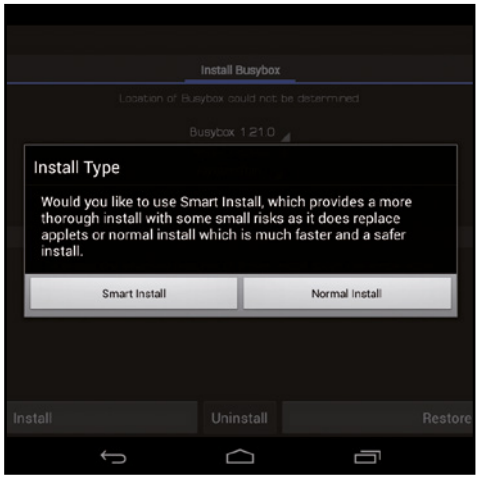
2 Utilizzando il file manager integrato nel nostro telefonino, raggiunge il percorso nel quale ha appena memorizzato il file APK scaricato al passo precedente e lo apre con un singolo tap. Conferma l'installazione di WPA Tester con *Installa* e successivamente con *Fine*.

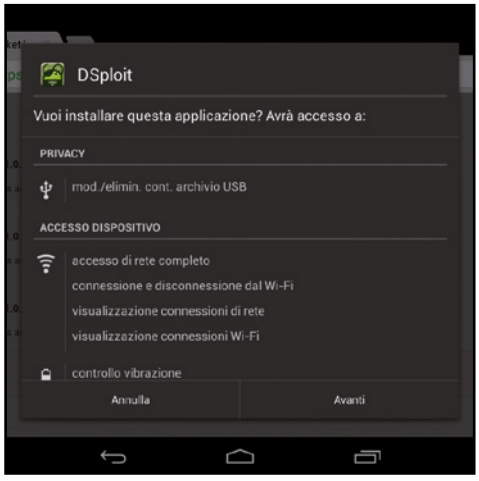
Scansione delle reti Wi-Fi

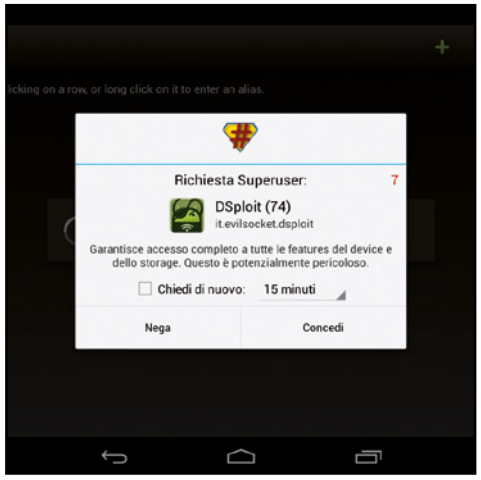
3 Non gli resta che ricercare nel *Menu* di Android l'applicazione appena installata e avviarla. Legge sommariamente le condizioni d'uso dell'app e conferma tappando su *Continua*. A questo punto l'interfaccia Wi-Fi viene attivata visualizzando le reti disponibili nei paraggi.

Lo smartphone degli hacker

Individuata la chiave di accesso alla rete Wi-Fi, il pirata può procedere con l'installazione di tutto il necessario per trasformare il proprio dispositivo mobile in un perfetto strumento di analisi e attacco!







Soddisfiamo i requisiti

1 Prima di installare dSploit, accede al *Play Store* e ricerca l'applicazione *BusyBox*. Tappa *Installa*, poi *Accetto* e attende la fine dell'operazione. Al termine avvia BusyBox tappando *Concedi* per fornire i permessi di root. Quindi tocca *Install* e poi *Normal Install*.

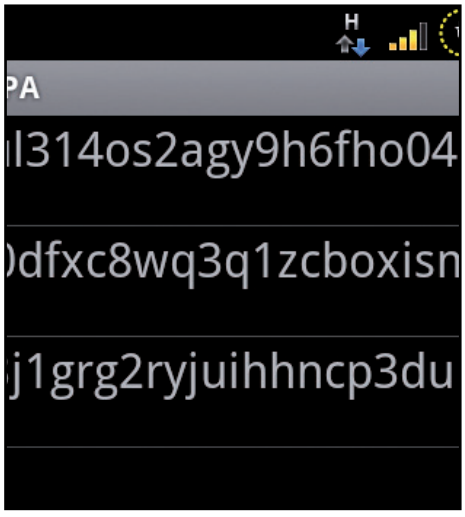
Download della suite

2 Direttamente dallo smartphone, avvia il browser Internet e raggiunge la pagina Web www.winmagazine.it/link/2198. Scarica quindi l'ultima versione disponibile dell'app dSploit (al momento in cui scriviamo la *1.0.31b*). Avvia poi l'installazione con un tap su *Avanti*.

I permessi necessari

3 Anche dSploit ha bisogno dei permessi di amministrazione. Ricerca quindi l'applicazione dal *Menu principale* di Android e la avvia. Non appena appare la finestra *Richiesta Superuser*, tocca il pulsante *Concendi*: dSploit è finalmente pronta per essere utilizzata.

WPA è bucata



Ecco la chiave di accesso!

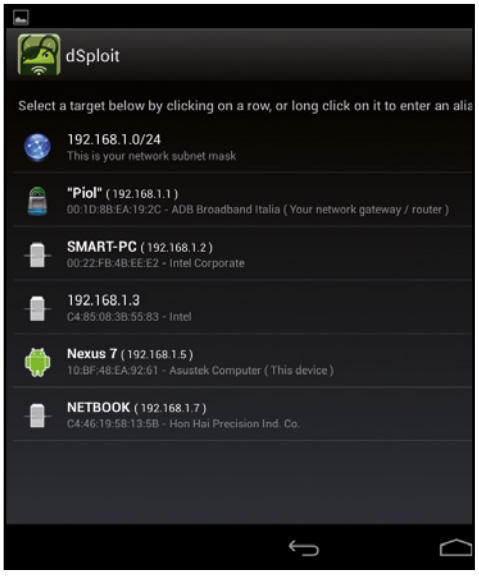
4 Seleziona la rete da "hackerare" e dopo qualche secondo visualizza le password associate. Non gli rimane quindi che provarle tutte nella speranza di trovare quella giusta. Volendo procedere in manuale, tappa *Manual Mode*, seleziona il produttore del router e tappa *Calcola*.

AIRCRACK SU SMARTPHONE ANDROID: IL PIRATA LO INSTALLA E LO USA COSÌ!

Il pirata informatico vuole togliere i lucchetti da una rete Wi-Fi non supportata da WPA Tester? Nessun problema, ci pensa AirCrack. Come molti di noi sapranno già, si tratta di uno dei software più apprezzati dagli hacker di tutto il mondo e che permette loro di "invadere" letteralmente qualsiasi rete senza fili maneggiando unicamente un PC. Ma un team di smanettoni è riuscito ad effettuare il porting di AirCrack anche su piattaforma Android includendo una comoda interfaccia grafica che rende tutto più semplice. Al momento in cui scriviamo, l'app può essere scaricata gratuitamente dal forum di XDA Developer, ma non è compatibile con tutti i modelli di smartphone: è possibile installare l'app unicamente sul Nexus One, sull'HTC Desire Z o sul Wildfire S, così come sul Samsung Galaxy SII. In definitiva, su tutti i device equipaggiati con una scheda Wi-Fi Broadcom BCM4329 o BCM4330. Affinché l'installazione possa essere portata a termine con successo è necessario che sul telefonino siano attivati i permessi di root e che vengano compilati dei nuovi e particolari driver di gestione per la scheda Wi-Fi. Di certo non una cosa semplice e alla portata di tutti. Proprio per andare incontro anche a quei pirati alle prime armi, gli sviluppatori hanno creato una "pappa pronta": due soli file .apk da trasferire sulla memoria interna dello smartphone, a patto di aver installato la cooked ROM CyanogenMod. Nel caso di un Samsung Galaxy S II, infatti, al pirata basta ricercare sul Web il file ***bcmon.apk*** e trasferirlo nella memoria del telefonino. Dopo averlo installato, gli basta tappare sul pulsante ***Yes*** per scaricare i nuovi driver della scheda di rete Wi-Fi. Una volta fatto questo, il pirata ricerca e scarica da Internet un altro pacchetto, ***AircrackGUI-1.0.4.apk***. Installa anche questo sul suo device ed è pronto a bucare ogni rete che gli capiti a tiro! Tutto quello che deve fare è infatti tappare sul pulsante ***Enable Monitor Mode*** per iniziare a catturare i pacchetti. Raggiunto un numero abbastanza elevato, può fermare la cattura e procedere alla decodifica della giusta chiave WPA o WEP che avviene grazie ad un dizionario integrato nell'app (il cosiddetto wordlist).

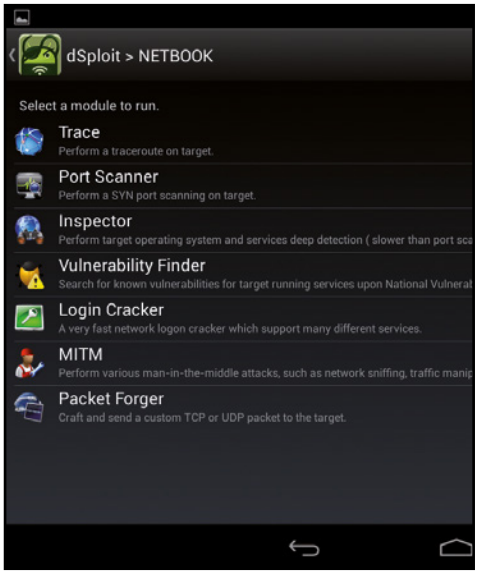
Ti sniffo dallo smartphone!

Dopo aver installato dSploit bastano pochi tap per analizzare tutte le vulnerabilità di una rete Wi-Fi e tentare un attacco di tipo hijacking, il preferito dai pirati per "spiare" le nostre attività.



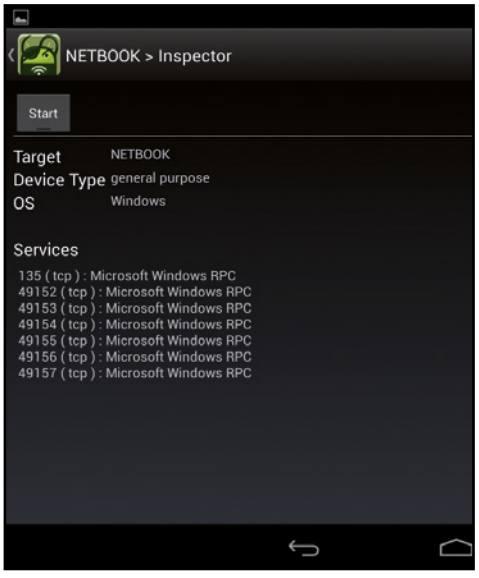
Scansione della rete

1 Innanzitutto il pirata si connette all'hotspot Wi-Fi di cui ha scoperto la chiave e avvia dSploit: l'app si mette alla ricerca di tutti i PC connessi alla rete locale. Seleziona uno fra quelli presenti in elenco. Se vuole agire sull'intera WLAN, seleziona la prima voce, *192.168.1.0/24*.



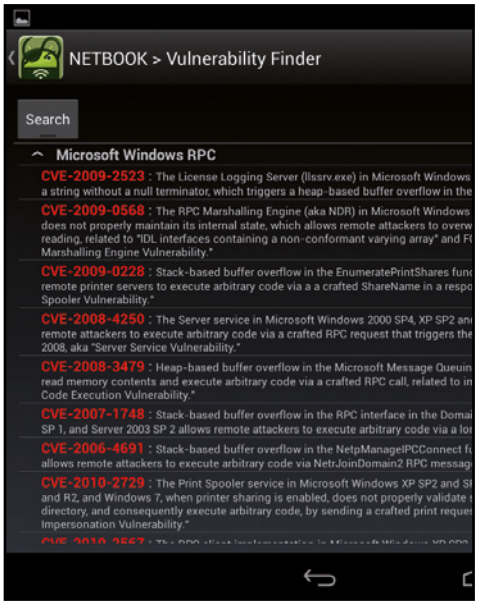
Cosa dobbiamo fare?

2 Si ritrova così in una nuova schermata in cui indicare quale tipologia di operazione effettuare. Può ad esempio scansionare l'host alla ricerca di eventuali porte aperte, servizi attivi o attuare un attacco "man in the middle" per intromettersi nelle comunicazioni di rete.



Ecco i servizi attivi

3 Seleziona *Inspector*: grazie a questo modulo potrà scoprire quali servizi sono attivi sull'host selezionato per analizzarne in seguito eventuali vulnerabilità. Per iniziare la scansione tappa sul pulsante *Start*. L'operazione può durare anche diversi minuti.

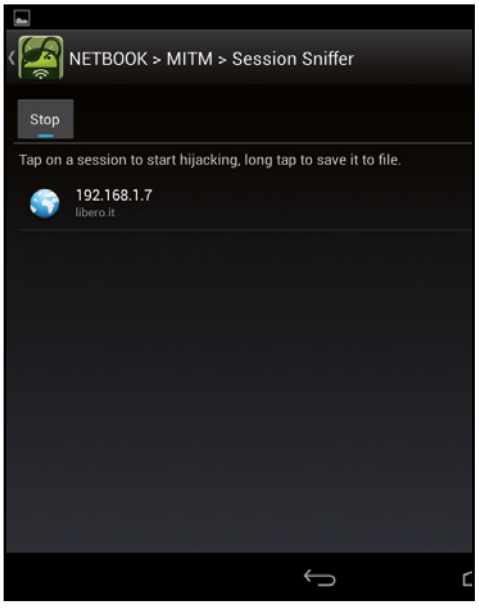


Ci sono vulnerabilità?

4 Quando la scansione sarà conclusa, preme il pulsante *Indietro* e si sposta sulla voce *Vulnerability Finder*. Sfruttando i dati raccolti nel passo precedente, può così analizzare le eventuali vulnerabilità trovate. Avvia quindi il processo con un tocco su *Search*.

Attacco in corso!

5 È arrivato il momento di testare seriamente la sicurezza della rete. Dai moduli di dSploit il pirata seleziona *MITM* (*Man In The Middle*): può eseguire uno sniffing di dati o cercare di loggarsi ai servizi Web attivi sull'host. In quest'ultimo caso, seleziona *Session Hijacker*.

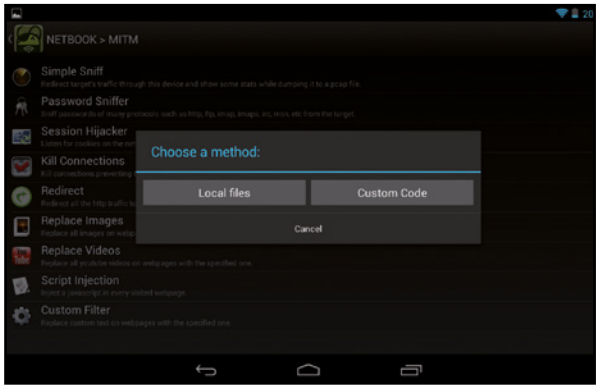


Hijacking effettuato

6 Tappa poi su *Start* e attende che dSploit trovi una sessione attiva su qualche servizio Web (come ad esempio la Webmail del portale Libero). Tappando sul risultato di ricerca, si apre una nuova finestra del browser nella quale si ritroverà loggato con i dati della vittima!

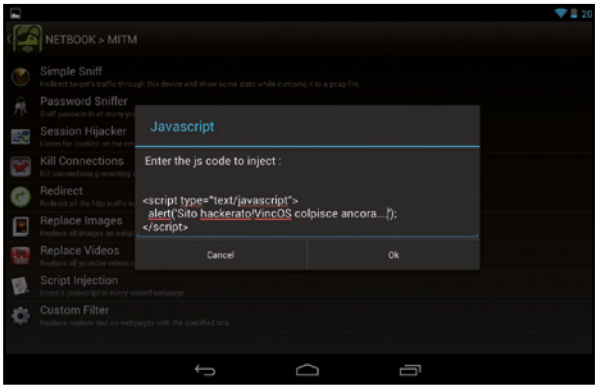
Password in pericolo!

Sfruttando gli strumenti integrati nella suite dSploit il pirata può intercettare la navigazione sul Web di un computer connesso in Wi-Fi per visualizzare in chiaro tutte le password digitate.



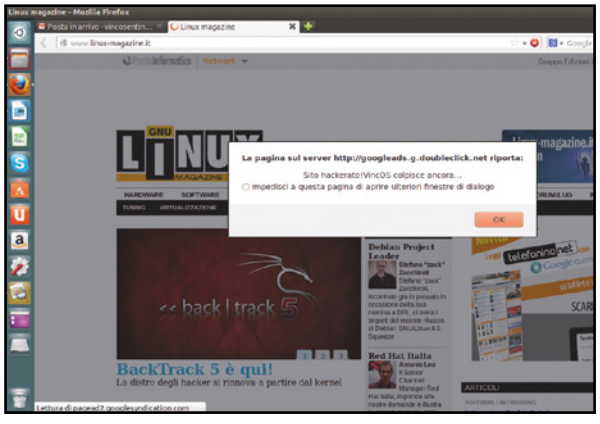
Un'iniezione di script

1 Dall'interfaccia grafica principale di dSploit, seleziona l'indirizzo IP dell'host sul quale vuole effettuare il suo "esperimento". Fatto ciò, tappa dapprima su *MITM* e successivamente su *Script Injection*. Nella nuova finestra che appare scegle quindi il comando *Custom Code*.



Serve un po' di codice Java

2 Compila il campo *Enter the js code to inject* con il codice Java dell'operazione che vuole far eseguire sulle pagine Web visualizzate dall'host. Per visualizzare un messaggio di testo, ad esempio, scrive *<script type="text/javascript"> alert('messaggio'); </script>*.



Attacco sferrato!

3 Conferma con *OK*: a questo punto lo script è in funzione. Ogniqualvolta l'host aprirà una nuova pagina Web, apparirà a schermo il messaggio che il pirata ha settato al passo precedente. Per terminare l'attacco, preme il pulsante *Indietro* dello smartphone.

password in chiaro!

4 Sempre dal modulo *MITM* di dSploit, tappa su *Password Sniffer*. Avvia il processo con *Start* e attende che l'host si logghi a qualche servizio Web (non usando il protocollo HTTPS). Gli username e le password digitate gli appariranno in chiaro sul display del suo dispositivo!

BUONI CONSIGLI

SICURI DI ESSERE AL SICURO?

Se quello che abbiamo scoperto fino ad ora ci ha lasciato a bocca aperta, lo saremo ancor più ora che vedremo come visualizzare in chiaro, direttamente sul display dello smartphone, tutte le password che circolano all'interno della nostra rete locale. Quest'avventura ci ha fatto aprire ancora una volta gli occhi sulla poca sicurezza che ruota attorno al mondo dell'informatica. E se un pirata riuscisse ad accedere al nostro hotspot? Gli basterà maneggiare solo il suo telefonino, ma anche il tablet, per mettere a repentaglio tutti i nostri dati.

UN TABLET, MILLE TOOL: L'HACKING A PORTATA DI DITA

Apparentemente è un normalissimo Nexus 7, ma non è così. All'interno del Pwn Pad, questo il nome di questo incredibile tablet, batte il cuore di una versione customizzata di Android appositamente studiata per ospitare tutti i tool dei veri hacker. E, poiché l'adattatore Wi-Fi integrato del tablet non è poi così potente, il Pwn Pad è dotato di un'antenna esterna. Decisamente nutrita la lista dei software integrati: Aircrack, Kismet e Metasploit sono solo alcuni dei circa 40 tool integrati. Il prezzo? Circa 900 dollari. Maggiori informazioni sono disponibili alla pagina www.winmagazine.it/link/2199.

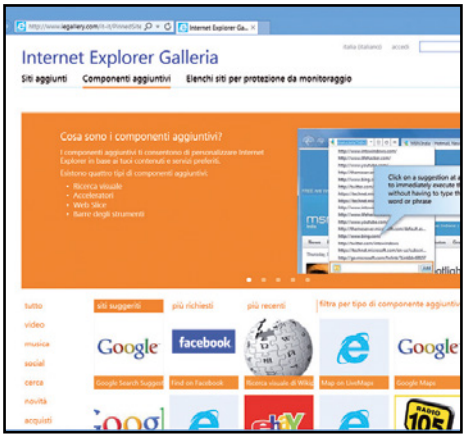
Il super browser di Win Magazine

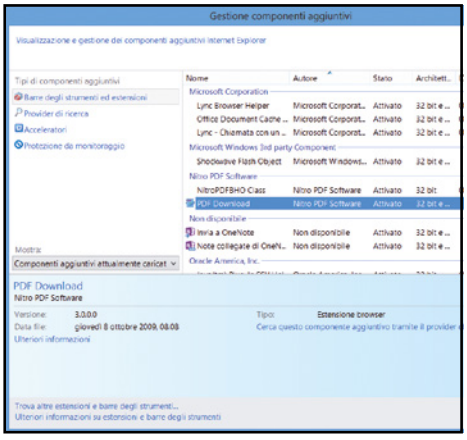
Supera i limiti del Web e trasforma il tuo software di navigazione in un sistema perfetto per fare di tutto e di più in Rete

Da semplici programmi per navigare tra i siti Web preferiti, i browser possono trasformarsi in completi strumenti per fare di tutto e di più. Esistono applicazioni e componenti aggiuntivi che, se installati, aggiungono tantissime altre funzioni trasformandoli in veri e propri "Super Browser". Con semplici add-on, ad esempio, possiamo bloccare tutti gli annunci pubblicitari, prelevare video da YouTube, convertire file e scaricare dalla rete BitTorrent senza dover installare altri programmi sul PC. Il computer rimarrà così più leggero e scattante, mentre tutte le attività potranno essere svolte direttamente nel browser... da un'unica, comoda finestra. È bene precisare che per Internet Explorer, il browser ufficiale Microsoft, esistono solo pochi componenti aggiuntivi e la stessa cosa vale per Safari di Apple; ma per Chrome, Firefox e Opera, invece, c'è davvero l'imbarazzo della scelta: veri e propri store con migliaia di contenuti, compresi giochi completi dalla grafica eccezionale. Quindi, se proprio vuoi il massimo, è il caso di migrare una volta per tutte a uno di questi software di navigazione. Inoltre, possono anche essere personalizzati con temi e colori, in grado di renderli più gradevoli e dal look moderno e giovanile. Insomma, per non deludere le aspettative di nessuno abbiamo raccolto le estensioni disponibili per i browser più famosi (Firefox, Internet Explorer, Safari, Opera e Chrome), selezionando dall'immenso calderone quelle che possono davvero dare una marcia in più al nostro browser. Tuffati in questo mondo fatto di add-on ed estensioni e fai col tuo browser ciò che non avevi mai immaginato di fare!

Estensioni per Internet Explorer

Da sempre il browser Microsoft non brilla per numero e qualità di add-on, ma qualcosa di buono c'è! Ecco come trovarle, installarle e rimuoverle: così la gestione è totale!





1 Dove trovare le add-on

Avviamo Internet Explorer e andiamo sul sito www.winmagazine.it/link/2240. Spostiamoci nella sezione *Componenti aggiuntivi* e scorriamo la pagina verso il basso. Troveremo una serie di add-on suddivisi per categorie: scorriamo, troviamo il componente da installare e clicchiamoci sopra.

2 L'installazione è rapida

Verrà mostrata una scheda con la descrizione dell'estensione. Per installarla clicchiamo *Aggiungi a Internet Explorer*. Seguiamo la procedura guidata e completiamo i passi dell'installazione. Una finestra ci informerà che il componente è pronto per essere utilizzato e ci chiederà se vogliamo abilitarlo.

3 Gestione a portata di clic

Per disabilitare un componente aggiuntivo in IE andiamo in *Strumenti* e clicchiamo *Gestione componenti aggiuntivi*. In *Mostra* selezioniamo *Tutti i componenti aggiuntivi*, tocchiamo sul componente e facciamo *Disabilita*. Per disinstallarlo basta andare nel *Pannello di controllo*.

TUTTA LA RAI A PORTATA DI CLIC

La televisione nazionale trasmette in streaming, direttamente sul suo portale, tutti i contenuti del palinsesto giornaliero. Ecco come accedervi direttamente dalla home page di Internet Explorer.

Con il componente Rai Tv Webslice possiamo aggiungere alla barra dei preferiti di Internet Explorer una Webslice che ci permette con un clic di visualizzare le dirette dei canali Rai. In altre parole, cliccandoci sopra si apre una piccola finestra. Qui possiamo selezionare il canale su cui vogliamo sintonizzarci. Dopo aver fatto clic, il canale viene visualizzato in una nuova finestra del browser.

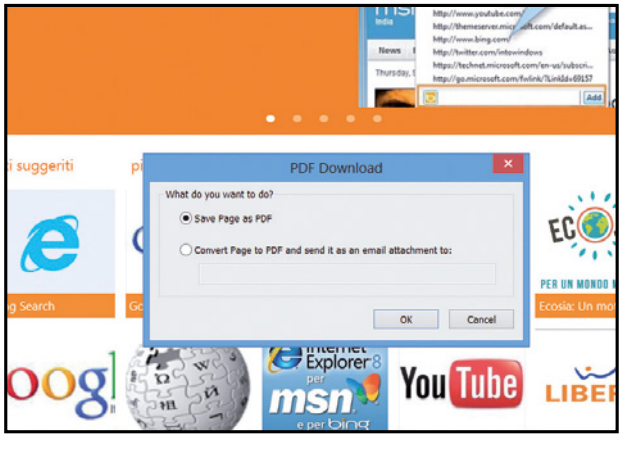
www.winmagazine.it/link/2241

CONVERTI I SITI WEB IN DOCUMENTI PDF

Vuoi leggere una pagina Web in modo più tranquillo, magari in un secondo momento e quando non sei collegato a Internet? Ti basta convertirla in formato PDF!

Con l'estensione *PDF Download for Internet Explorer* possiamo trasformare velocemente qualsiasi pagina Web in un documento PDF e inviarcela per e-mail. Per farlo, carichiamo la pagina nel browser e clicchiamo sull'icona del componente presente nella barra degli strumenti. Selezioniamo *Save Page as PDF* e diamo *OK*. Inseriamo nella pagina il nostro indirizzo e-mail e clicchiamo *Convert to PDF*. La pagina verrà convertita in PDF e ci sarà inviata come allegato di posta elettronica.

www.winmagazine.it/link/2242



SINCRONIZZA I PREFERITI

Capita spesso di usare più computer diversi e avere la necessità di accedere ai nostri siti preferiti. Con l'estensione giusta, possiamo sincronizzarli su tutti i browser con un clic.

Con Xmarks possiamo sincronizzare i nostri preferiti con più computer in modo semplice e veloce e questo componente può essere installato anche in altri browser. Avviata la procedura di installazione, dovremo innanzitutto creare un account necessario per la sincronizzazione on-line dei bookmark: basterà compilare i campi con i nostri dati e un indirizzo di posta valido. Completata la procedura, ci verrà inviata un'e-mail con il link per confermare l'account. Dopo averci cliccato, una finestra ci chiederà se sincronizzare o meno i *Preferiti*: non ci resta che confermare. Installando Xmarks anche in tutti gli altri browser che abbiamo, avremo i *Preferiti* sempre sincronizzati. Per gestirli possiamo anche andare sul sito https://my.xmarks.com. Dopo aver eseguito l'accesso col nostro account, in *Bookmarks* possiamo visualizzarli, cancellarli (*Delete*) ed eventualmente aggiungerne altri con *New*.

www.winmagazine.it/link/2243

SCARICARE IMMAGINI DAI SITI

Grazie ad un'estensione scaricabile dal sito PinnedSites possiamo aggiungere ad Internet Explorer una comoda barra strumenti che ci permetterà di gestire al meglio le immagini sul Web.

L'add-on si chiama *Pictures Toolbar For Microsoft Internet Explorer* e, grazie alla sua barra strumenti, permette di scaricare facilmente immagini dai siti Web visitati con Internet Explorer. Tutto quello che dobbiamo fare è andare col browser sulla pagina dove è presente la galleria e cliccare sul tasto con la freccia verso il basso mostrato alla fine della barra strumenti. Si apre quindi una piccola finestra che ci chiederà in quale galleria salvare le immagini. Selezionando *My Photo Albums* le immagini saranno accessibili nella cartella *Immagini* dell'*Esplora risorse* di Windows. Premiamo *OK* per avviare il download.

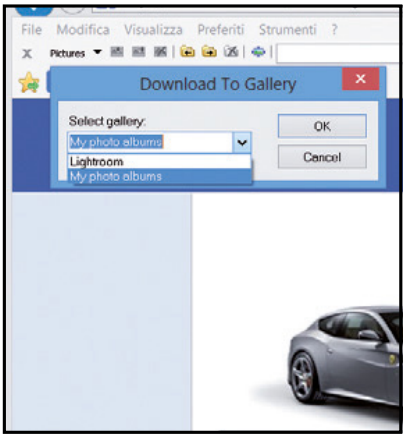
www.winmagazine.it/link/2244

RICERCHE VELOCI SU FACEBOOK

Con Find on Facebook possiamo installare in IE un acceleratore che consente di trovare qualsiasi cosa sul nostro social network preferito.

Per utilizzarlo basta evidenziare la parola da cercare e cliccare sul pulsante che viene mostrato per aprire il pannello con gli acceleratori disponibili. Andiamo in *Tutti gli acceleratori* e clicchiamo su *Find on Facebook*: si aprirà la pagina con i risultati sul social network.

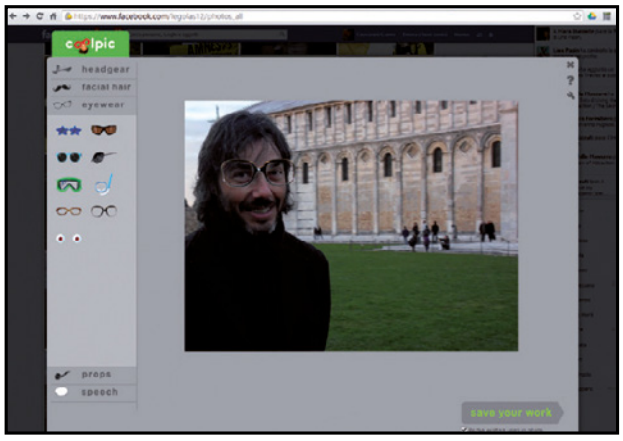
www.winmagazine.it/link/2245



RITOCCA LE FOTO DI FACEBOOK

Ci piacerebbe dare un tocco artistico alle foto dei nostri amici di Facebook, senza per questo interrompere la navigazione per passare ad un programma di fotoritocco? Basta installare l'estensione giusta su Chrome!

Con *Facebook and Flickr photos made fun*, quando si apre una foto sul social network clicchiamo sul piccolo pannello a sinistra per accedere all'editor di Coolpic.



Possiamo aggiungere occhiali finti (*eyewear*), baffi (*facial hair*) e molti altri elementi per rendere le foto davvero uniche e divertenti. Tutto quello che dobbiamo fare è trascinarli sulla foto. Al termine premiamo *Save your work*. L'estensione funziona anche con Picasa e Flickr.
www.winmagazine.it/link/2246

CONTROLLARE IL PC A DISTANZA

Con Chrome Remote Desktop possiamo controllare da remoto il nostro computer utilizzando Chrome. Ecco come fare.
Al primo avvio dell'applicazione bisognerà consentire le autorizzazioni necessarie all'uso del computer. Dopo aver accettato i permessi, un piccolo tutorial ci guiderà all'uso dell'applicazione. A questo punto si deve decidere se condividere il proprio desktop o accedere a quello di un altro utente. Nel primo caso clicchiamo *Condividi*: ci viene fornito un codice numerico che dovremo fornire all'utente che vuole accedere al nostro computer. L'altra persona dovrà a sua volta aver installato l'applicazione sul computer e avviarla. Dovrà quindi scegliere l'opzione *Accesso* e inserire il codice nel campo *Codice di accesso*. Dopo aver premuto *Connetti* sarà in grado di accedere da remoto al computer e usarlo proprio come se si trovasse seduto alla scrivania.
www.winmagazine.it/link/2247

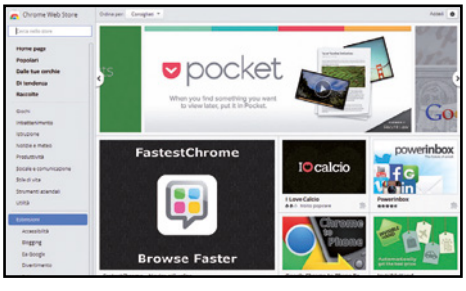
ACCESSO REMOTO SULLO SMARTPHONE

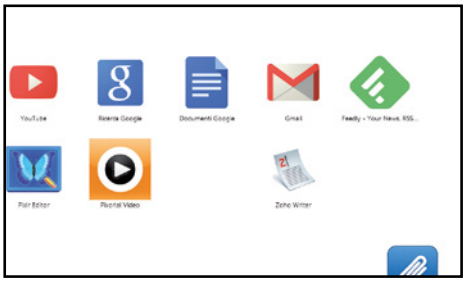
Con AirDroid potremo accedere al tuo dispositivo Android direttamente dal browser e gestirlo da remoto. Scopriamo come.

Per prima cosa si deve scaricare l'applicazione AirDroid dal dispositivo Android andando su Google Play. Al primo avvio, bisogna creare un nuovo account AirDroid fornendo un'e-mail e una password ed eseguire l'accesso. Spostarsi quindi sul PC, avviare AirDroid in Chrome ed eseguire l'accesso con lo stesso account del dispositivo. Dopo averlo fatto, visualizzeremo nel browser un desktop che ci permetterà di controllare le applicazioni, visualizzare i contatti e usarne anche le varie funzioni a distanza come la fotocamera.
www.winmagazine.it/link/2248

Chrome: oltre il browser!

Tante applicazioni da installare gratuitamente per scaricare video, guardare canali televisivi e molto altro ancora. Ecco come usare il Web store di Google dedicato al programma di navigazione di Mountain View.





1 Non solo estensioni

Per accedere al Web Store di Chrome apriamo una nuova scheda e clicchiamo sull'icona *Store* o in alternativa andiamo su https://chrome.google.com/webstore. A differenza di altri browser, quello di Big G consente di installare sia estensioni, sia vere e proprie applicazioni, oltre naturalmente a personalizzare l'interfaccia con i temi.

2 Tra app e add-on

Per installare un'estensione, clicchiamo sul pulsante *Aggiungi*: una finestra mostra i tipi di dati a cui potremo accedere con l'estensione. Clicchiamo *Aggiungi* per completare. Per le applicazioni la procedura è simile, solo che dovremo eseguire l'accesso con il nostro account Google. Le app sono accessibili nella sezione *Applicazioni* in *Nuova scheda*.

3 Questa non serve più

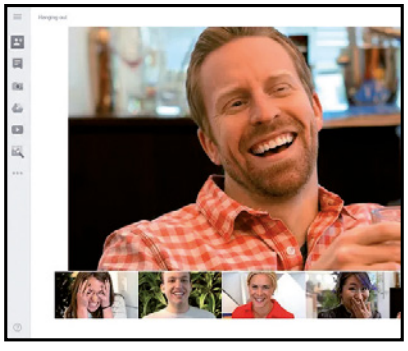
Per rimuovere un'estensione andiamo nel menu *Impostazioni/Estensioni* e clicchiamo sull'icona *Rimuovi da Chrome*. Per disinstallare le app, invece, andiamo nella pagina *Nuova scheda* dove saranno accessibili le app: trasciniamo quindi l'icona dell'app sul pulsante *Rimuovi da Chrome* nell'angolo in basso a destra.

LA VIDEOCHIAMATA SI FA IN GRUPPO

Con la nuova chat di Google possiamo chiamare e videochiamare i nostri amici direttamente dall'interfaccia di Chrome. Ecco in che modo.

Per prima cosa, dobbiamo installare l'estensione *Chiamata di Hangouts*: grazie ad essa possiamo videochiamare i nostri amici di Google+. Per iniziare velocemente una chat video di gruppo, avviamo l'applicazione ed effettuiamo l'accesso col nostro account Google. Ci viene mostrata la finestra *Aggiungi persone alla videochiamata*. Selezioniamo i contatti da aggiungere immettendoli nel campo sotto e clicchiamo su *Invia*. Cliccando su *Aggiungi telefono* possiamo anche chiamare un numero di telefono, ma in questo caso la chiamata non sarà gratuita e si dovrà disporre del credito necessario.

www.winmagazine.it/link/2249



CHIAMA GRATIS SEMPRE E OVUNQUE

Con ooVoo Video Chat abbiamo una piattaforma per realizzare videochiamate di gruppo via Web senza spendere un centesimo. Impariamo a sfruttarla al meglio.

Come altri programmi simili, ogni utente che partecipa dovrà aver installato l'apposita applicazione sul suo dispositivo. Avviata l'applicazione, dobbiamo eseguire l'accesso utilizzando il nostro account Facebook. Premiamo tre volte *OK* per consentire l'accesso ai nostri dati. Diamo il consenso per avviare l'applicazione nel browser. Premiamo sul pulsante *Start a call* per aprire la finestra da cui scegliere i contatti da chiamare. Cliccando su *Click here* possiamo configurare l'applicazione per accedere al nostro account di ooVoo e importare la lista dei nostri amici. Il bello di ooVoo è che è compatibile con PC, Mac, iPhone, Android, iPad ecc., così potremo contattare i nostri amici dal computer ovunque essi si trovino.

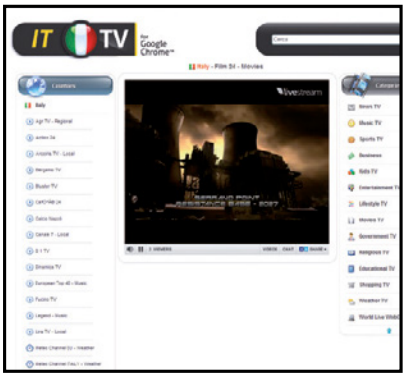
www.winmagazine.it/link/2250

GUARDA LA TV NEL BROWSER

Installando una semplice estensione, possiamo trasformare il browser Chrome in una vera TV digitale.

Dal *Chrome Store* scarichiamo e installiamo *Italia TV*. Basta quindi avviare l'estensione per accedere alle numerose emittenti televisive. A sinistra c'è l'elenco di quelle italiane mentre a destra possiamo scorrere quelle disponibili filtrandole per categorie. Se ad esempio cerchiamo qualche cartone animato per i nostri figli, basta cliccare su *Kid TV* dal pannello di destra per visualizzare i canali disponibili. Per ognuno sarà indicato il Paese attraverso la bandierina. Per avviare la visione basta fare clic sul nome del canale.

www.winmagazine.it/link/2251



CONVERTI TUTTI I TUOI FILE

Hai un file che non riesci ad aprire perché in un formato non compatibile con i tuoi programmi? Installa File Converter in Chrome e potrai convertirlo facilmente in qualsiasi altro formato.

Basta cliccare su *Scegli file* per selezionare il file da convertire, premere *Invia* e in *Select Output Format* selezionare il formato finale. Fatto ciò si deve premere *Convert* e attendere la conversione. Non resta che premere *Download* per scaricare il file zippato sul proprio PC.

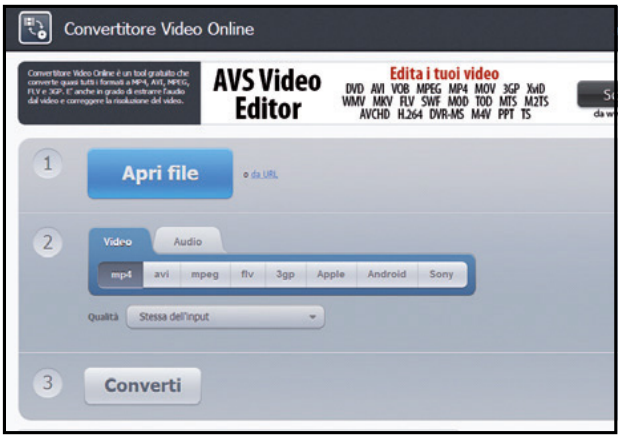
www.winmagazine.it/link/2252

VIDEO AL BACIO PER OGNI DISPOSITIVO

Anche per convertire i tuoi video ora puoi affidarti al browser. Bastano pochi clic e possiamo dire addio ai soliti problemi di compatibilità!

Con *Convertitore Video* potremo convertire ogni formato video come MP4, AVI, MPEG, FLV e 3GP. Possiamo anche estrarre l'audio da un filmato e modificare la risoluzione del file finale per adattarla al dispositivo dove andrà riprodotto. Supporta anche la conversione dei formati audio. Per procedere, clicchiamo su *Apri file*, selezioniamo il file e attendiamo che venga caricato nell'applicazione Web. In *Video* selezioniamo il formato, in *Qualità* scegliamo la risoluzione finale e premiamo *Converti*.

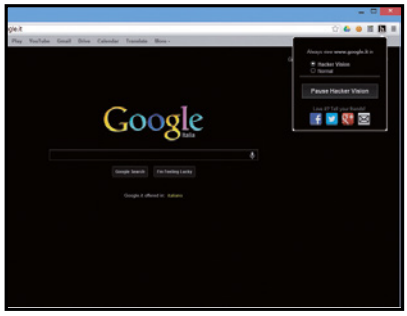
www.winmagazine.it/link/2253



PIÙ CONTRASTO ALLE PAGINE WEB

Lo sfondo bianco delle pagine Web ci da fastidio? Con Chrome possiamo modificarlo secondo i nostri gusti così da migliorare il contrasto col testo e renderlo più leggibile.

L'estensione *Hacker Vision* ci regala un nuovo modo per navigare il Web che ne migliorerà l'esperienza. L'estensione installa un piccolo pulsante con la lettera *h* a destra del



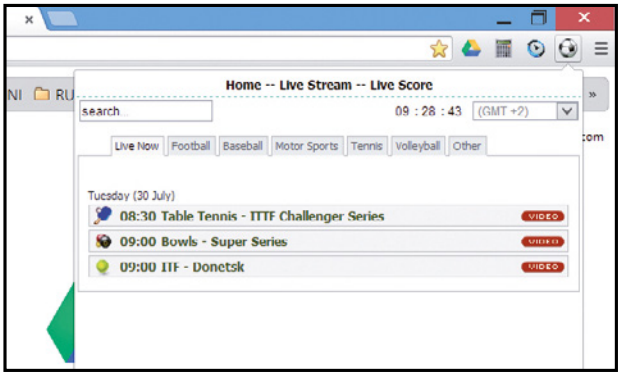
browser. Cliccandoci sopra potremo scegliere se applicare lo sfondo scuro (*Hacker Vision*) oppure se lasciare quello standard (*Normal*).
www.winmagazine.it/link/2255

VIDEOREGISTRA I CANALI DI YOUTUBE

Stiamo guardando un video in streaming su Internet come un film o una clip musicale? La soluzione c'è! Ecco come applicarla.
Con *Grab Any Media* possiamo scaricarlo per registralo sul computer e guardarlo anche off-line. Il suo uso è molto semplice. Basta portarsi sulla pagina in cui è presente lo streaming, come ad esempio quella di un video di YouTube, e cliccare sul pulsante che si installa a destra della barra degli URL. Grab Any Media effettuerà la scansione degli streaming presenti nella pagina e li mostrerà in una piccola finestra chiamata *Board*. Scegliamo quello che vogliamo scaricare e clicchiamo *Download*.
www.winmagazine.it/link/2256

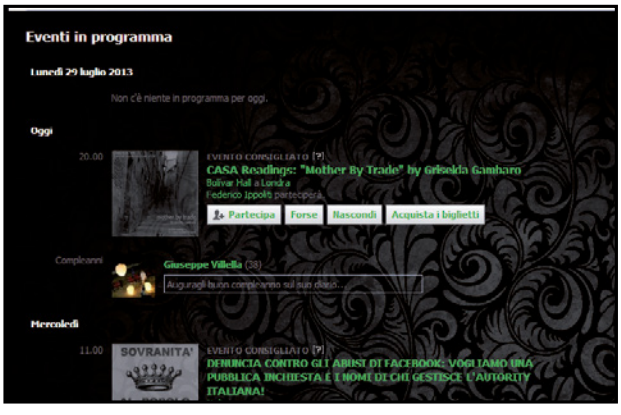
TUTTO LO SPORT IN DIRETTA

Vogliamo guardare un evento sportivo in diretta streaming? Allora Live Sports è l'estensione che ci serve!
Dopo averla installata, clicchiamo sul pulsante con la palla mostrata accanto al campo URL e attendiamo qualche secondo con pazienza. Si aprirà un piccolo riquadro da cui scegliere se cercare i *Live Streaming* o gli *Score*. Per le dirette video scegliamo il primo. Gli eventi sono suddivisi per tipologia di sport e cliccando su *Video* potremo visualizzare i link per avviare la diretta streaming.
www.winmagazine.it/link/2257



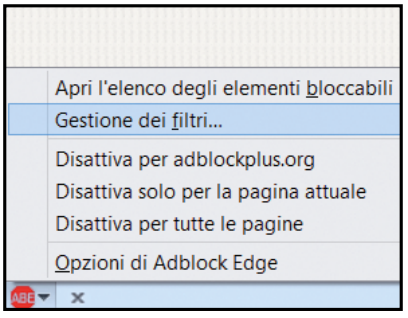
CAMBIA FACCIA A FACEBOOK

Grazie alle potenzialità di Chrome, possiamo decidere anche di dare un nuovo look alla nostra pagina Facebook? Vediamo in che modo.
Con *Facebook Themes* potremo utilizzare tantissimi temi per darle un tocco nuovo e più moderno. Per prima cosa dobbiamo installare l'estensione nel browser. Fatto ciò, rechiamoci su http://themecreator.funnerapps.com/facebook, scegliamo il tema che più ci piace e installiamolo premendo sul pulsante *Install*. La nostra pagina di Facebook avrà così un look tutto nuovo!
www.winmagazine.it/link/2258



STOP ALLA PUBBLICITÀ!

Molti siti Web sono pieni di banner pubblicitari, video, finestre che si aprono da sole e tanti contenuti inutili e ingannevoli. Possiamo rendere questi siti molto più leggeri e navigabili rimuovendo i componenti che non servono.
Basta installare *Adblock Edge* per ripulire le pagine non solo dalla pubblicità: i suoi filtri sono in grado di proteggere anche la nostra privacy e bloccare eventuali malware. I filtri sono intelligenti e bloccano solo gli annunci fastidiosi. Comunque, è possibile personalizzare il controllo sui siti in modo da scegliere come e cosa fermare. L'add-on funziona da subito senza dover fare nulla: basta installarlo e iniziare a navigare.
www.winmagazine.it/link/2260



IL TRADUTTORE PER IL WEB

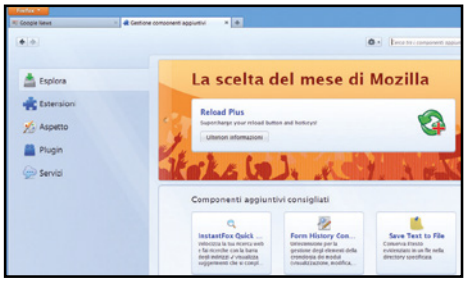
Stiamo navigando su un sito straniero e non riusciamo a raccapezzarci? Nessun problema, con gTranslate abbiamo un traduttore immediato sempre a portata di clic.
Dopo averlo installato, basta selezionare il testo da tradurre, cliccarci sopra col tasto destro e dal menu contestuale portarsi sulla linea *Tradurre*. La lingua viene riconosciuta automaticamente, ma è comunque possibile impostarla manualmente. Cliccando poi sulla traduzione, si viene reindirizzati automaticamente alla pagina del traduttore di Google.
www.winmagazine.it/link/2261

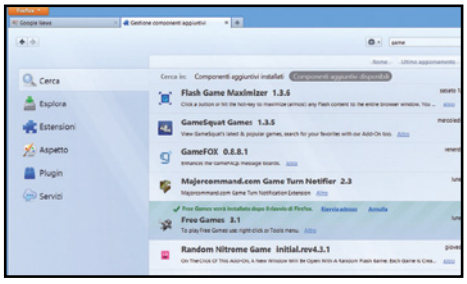
PROTEGGI LE NAVIGAZIONI

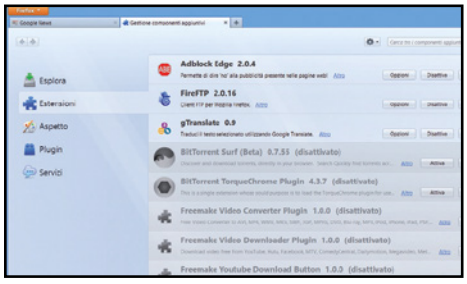
Molti siti nascondono al loro interno dei "trackers", ovvero dei piccoli strumenti che servono per tracciare le nostre attività e raccogliere informazioni a nostra insaputa. Con Ghostery la nostra privacy è al sicuro.
Questa particolare estensione per Firefox è in grado di rilevare questi trackers e bloccarli. Quelli fermati saranno notificati attraverso il componente che sarà visualizzato nella barra del browser in basso a destra.

Così Firefox mette le ali

Grazie alle estensioni, il browser Mozilla diventa un vero e proprio sistema operativo pronto a fare qualsiasi cosa. Ecco come fare incetta dei migliori add-on.







1 Un negozio integrato

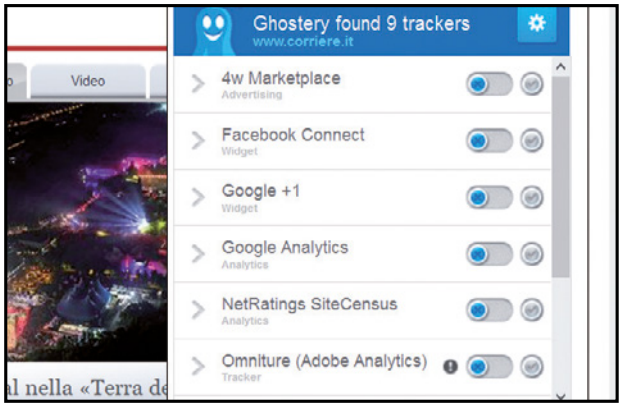
Per trovare i plug-in compatibili con Firefox, avviamo il browser, clicchiamo *Firefox* in alto a sinistra e selezioniamo *Componenti aggiuntivi*. Spostiamoci in *Esplora* e usiamo il campo di ricerca in alto a destra per trovare il componente da installare. Opzionalmente possiamo scorrere i contenuti navigando nella pagina.

2 Serve il riavvio

La ricerca mostra i primi risultati per pertinenza. Cliccando su *Visualizza tutti* si apre la pagina che mostra i risultati trovati. Per installare il componente aggiuntivo, basta cliccare sul tasto *Installa*. Il componente verrà scaricato e installato. Per completare il tutto, dobbiamo riavviare il browser cliccando su *Riavvia adesso*.

3 Un po' di pulizia

Per alleggerire Firefox dalle estensioni che non servono più, basta andare nel *Menu*, cliccare su *Componenti aggiuntivi* e spostarsi nella scheda *Estensioni*. Qui potremo visualizzare quelli presenti nel nostro browser, accedere alla finestra delle loro impostazioni, disattivarli ed eventualmente rimuoverli.



Cliccandoci sopra si apre la finestra con gli elementi bloccati. Per terminare il blocco, basta cliccare su *Pause Blocking*.
www.winmagazine.it/link/2262

AGGIRA LA CENSURA SUL WEB

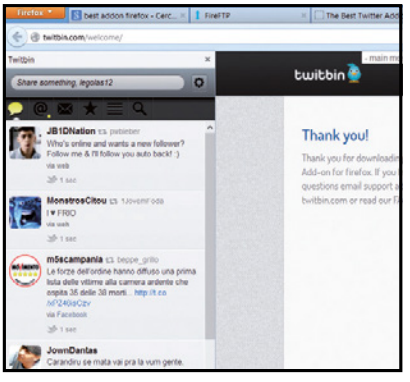
Sovente i provider bloccano alcuni siti Web. Succede, ad esempio, in Paesi dove i governi non voglio che i cittadini riescano ad accedere a siti stranieri oppure per impedire l'accesso a materiale protetto da copyright. Grazie a Firefox, questi blocchi diventano inutili!

Con *Hide My Ass! Web Proxy* si possono aggirare questi blocchi ed è utile anche per non lasciare tracce sui siti visitati. Utilizzarlo è semplicissimo: basta fare clic sul pulsante accanto la barra degli indirizzi, digitare il sito da visitare e premere *Proxy*.
www.winmagazine.it/link/2263

TWITTER SEMPRE CON TE

Con Twitbin possiamo aggiungere una barra laterale a sinistra del browser per tenere sempre sotto controllo il nostro account Twitter.

Dopo avere installato il plug-in, dovremo configurarlo. Ci verrà chiesto di eseguire l'accesso al nostro account della piattaforma di microblogging per autorizzare l'applicazione. Inseriamo i nostri dati e clicchiamo su *Authorize app*: otterremo un codice da inserire in *Twitbin*. Dopo averlo fatto, clicchiamo *Add User* per avere accesso al nostro account. Potremo leggere i tweet dalla nostra cronologia, vedere chi seguiamo, aggiornare il profilo, inviare messaggi e tanto altro ancora.
www.winmagazine.it/link/2264



MANO DI PENNELLO AI SITI WEB

Vogliamo dare un nuovo look ai nostri siti preferiti come Facebook? Color That Site! è quel che cerchiamo.

Dopo averlo installato, portiamoci sulla pagina da modificare e clicchiamo sul piccolo pulsante presente nella barra in basso a destra. Sulla sinistra si aprirà un pannello dal quale potremo modificare i colori del sito e trasformarlo come desideriamo. Con *Background colors*, ad esempio, possiamo modificare il colore di sfondo della pagina. Per salvare clicchiamo su *Save* e godiamoci

il nostro nuovo look. Come veri pittori, saremo noi a scegliere i colori dei siti Internet.
www.winmagazine.it/link/2266

RIPULIRE LA PAGINA DI FACEBOOK

Disponibile anche per Chrome, Opera e altri browser, Social Fixer consente di personalizzare la pagina Facebook per eliminare tutte le cose che non ci piacciono.

L'installazione è molto semplice: basta andare su www.socialfixer.com e installare la versione compatibile col proprio browser. Dopo averlo fatto, sarà sufficiente recarsi su Facebook e seguire il piccolo Wizard per scegliere le preferenze iniziali. Dopo, per personalizzare l'interfaccia, clicchiamo sul pulsante con la chiave inglese e scegliamo *Social Fixer Options*. Spuntando, invece, *Single column* possiamo personalizzare la timeline con un'unica colonna. In *Hide*, invece, possiamo selezionare i box da nascondere nella pagina come ad esempio quello degli amici (*Friends Box*).
www.winmagazine.it/link/2267

IL BUIO IN SALA

Proprio come facciamo quando guardiamo la TV a casa, con Turn Off the Lights possiamo spegnere la "luce" nel browser per concentrarci sulla visione del video di YouTube.

Basterà andare alla pagina del video e cliccare sul pulsante con la lampadina mostrato nella barra URL. La pagina si oscurerà ad eccezione del riquadro del video. Con un nuovo clic tornerà a illuminarsi.
www.winmagazine.it/link/2268

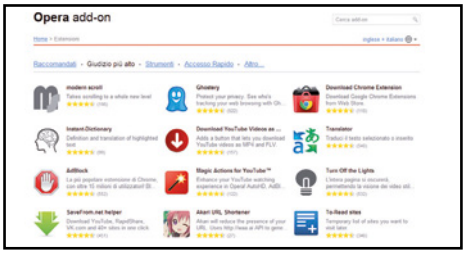
IL PIENO DI MUSICA E VIDEO

SaveFrom.net helper è il modo più semplice per scaricare video e musica da Internet. Impariamo ad usare al meglio questo ottimo plug-in per Opera.

L'estensione supporta i siti più importanti come YouTube.com, RapidShare.com, Vimeo.com, Dailymotion.com, VK.com, Soundcloud.com e altri ancora. Usarlo è semplicissimo. Dopo averla installata, rechiamoci sulla pagina di uno dei servizi supportati, ad esempio YouTube: troveremo il tasto *Download*. Premendolo ci verranno mostrate le opzioni per i formati in cui scaricare il contenuto. Non resta che scegliere quello che si vuole cliccandoci sopra e completare il download.
www.winmagazine.it/link/2269

Un'Opera d'arte di browser

Sebbene poco conosciuto, questo software di navigazione offre tantissime funzioni interessanti… da non perdere! Ecco come installare le estensioni e i nuovi temi grafici.



1 Lo store delle estensioni

Avviamo Opera e colleghiamoci alla pagina https://addons.opera.com/it/extensions. Qui è possibile trovare tantissime estensioni, suddivise per categoria. Possiamo modificare la lingua selezionandone un'altra se preferiamo. Per ogni estensione abbiamo una piccola descrizione con il giudizio degli utenti.

2 Installare in un clic

Dopo aver scelto l'add-on da installare, tocchiamo il tasto *Aggiungi a Opera*. Il tasto in un primo momento diventerà *Installazione* e al termine mostrerà la dicitura *Installata* che ci conferma che l'installazione dell'estensione è andata a buon fine. Non ci resta che provarla per verificarlo.

3 Rimozione in corso

Quando vogliamo rimuovere un'estensione, clicchiamo sul pulsante *Opera* in alto a sinistra e selezioniamo *Estensioni*. Nel tab *Attivata* possiamo visualizzare gli add-on attivi ed eventualmente disattivarli. Con *Opzioni* possiamo accedere alla scheda di configurazione dell'add-on.

La cronologia del Web anonimo

✓ È possibile risalire ai siti visitati durante una sessione di navigazione in incognito?

✓ Posso consultare Internet senza lasciare tracce?

SERVE A CHI...
... vuole navigare sicuro su Internet senza lasciare tracce sui siti visitati

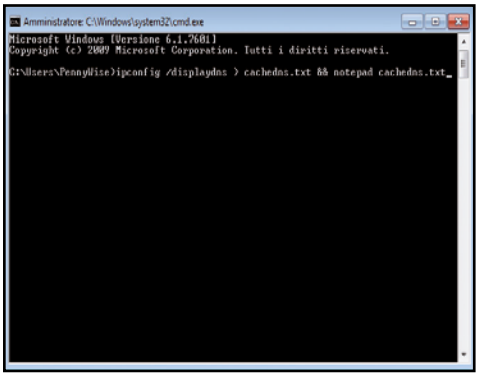
Ogni volta che apriamo il browser per collegarci ad un sito Internet, questo memorizza sul PC informazioni sulle pagine che andiamo a visitare. Questi dati, salvati sul disco rigido, compongono le vere e proprie "tracce" della nostra sessione di navigazione e vengono suddivise in cache, cookie e cronologia dei siti aperti. La cache è formata da tutti gli elementi che compongono una pagina Web visitata in modo da permettere un caricamento più veloce in caso di ulteriori visite della stessa pagina. Gli altri elementi che permettono di monitorare le nostre scorribande on-line sono i cookie. Nonostante le varie diatribe riguardo il loro corretto utilizzo nel rispetto della privacy, essi vengono sempre più utilizzati, oltre che per memorizzare i nostri dati di accesso ai vari siti Internet, anche in ambito dell'advertising on-line per personalizzare i banner pubblicitari in base alle preferenze di navigazione di ogni singolo utente.

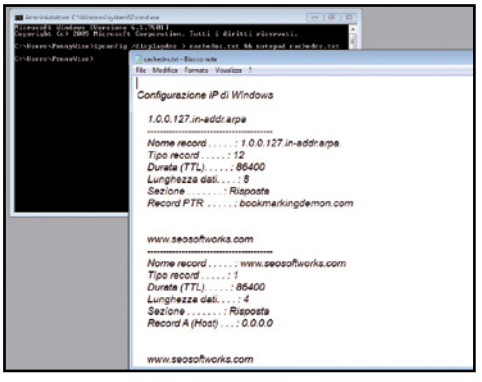
Non basta essere anonimi

Per fortuna le recenti versioni di tutti i browser permettono l'utilizzo della navigazione in incognito, una particolare funzione che consente all'utente di navigare su Internet evitando la memorizzazione e il salvataggio di cookie e cronologia di navigazione. Alcuni browser, come Google Chrome, hanno addirittura introdotto una modalità chiamata "Modalità ospite" che permette di utilizzare un qualsiasi PC senza il rischio di lasciare in memoria alcun dato personale che potrebbe far risalire alle nostre abitudini in Rete. Quello che in pochi sanno, però, è che nonostante l'utilizzo di queste speciali modalità è possibile risalire ai siti Web visitati dall'utente anche senza il salvataggio della cronologia da parte del browser. È sufficiente sfruttare il modulo Resolver DNS di Windows, ovvero la parte del sistema operativo che si occupa di tradurre i siti dal loro indirizzo IP alla classica visualizzazione che utilizziamo solitamente per la navigazione. Questo sistema, infatti, mantiene nella propria cache tutte le associazioni tra indirizzo IP e sito Web visitato rendendo possibile a chiunque, se opportunamente consultata, di risalire a tutti gli indirizzi visitati anche se abbiamo utilizzato la modalità di navigazione in incognito. Vediamo insieme come controllare la cache del Resolver DNS e come, eventualmente, ripulirla in modo da cancellare al 100 % la nostra cronologia di navigazione.

CANCELLIAMO LA MEMORIA
Come abbiamo visto, il Resolver DNS di Windows tiene traccia nella propria cache di tutti i siti Web visitati. Ma è possibile cancellare questa cache ed essere così sicuri di non lasciare traccia della nostra cronologia di navigazione? La risposta è sì! Per farlo è sufficiente aprire il *Prompt dei comandi* digitando cmd dalla barra di ricerca nel menu *Start*, digitare al suo interno il comando *ipconfig /flushdns* e confermare con *Invio*. Il prompt ci restituirà un messaggio di conferma della cancellazione della cache.

Ecco come scoprire i siti Web visitati durante la navigazione anonima





1 Apriamo innanzitutto il ***Prompt dei comandi*** di Windows: possiamo farlo dal menu ***Start/Tutti i programmi/Accessori/Prompt dei comandi*** oppure digitando cmd nella barra di ricerca del menu ***Start*** e premendo ***Invio***.

2 Verrà così caricata la classica schermata nera dell'ambiente di emulazione del DOS. Dal prompt digitiamo il comando ***ipconfig /displaydns > cachedns.txt && notepad cachedns***.txt, quindi premiamo ***Invio*** per confermare.

3 All sistema genererà automaticamente un file di testo TXT con i siti Web visitati dall'utente, mostrandone il contenuto a video. Basterà scorrere il contenuto per leggere sia il nome del sito che il suo indirizzo IP.

Maledette toolbar!

Rallentano la navigazione, consumano memoria e rubano dati personali. Rimuovile per sempre

Cosa ci occorre

15 MIN.
FACILE

SOFTWARE ANTIMALWARE
JUNKWARE REMOVAL TOOL
SOFTWARE COMPLETO
Lo trovi su: ☑DVD
Sito Internet: www.bleepingcomputer.com

TOOL DI RIMOZIONE
TOOLBAR CLEANER
SOFTWARE COMPLETO
Lo trovi su: ☑DVD
Sito Internet: http://toolbarcleaner.com

TOOL DI PULIZIA
CCLEANER
SOFTWARE COMPLETO
Lo trovi su: ☑DVD
Sito Internet: www.piriform.com

SOFTWARE ANTIVIRUS
MALWAREBYTES ANTI-MALWARE
SOFTWARE COMPLETO
Lo trovi su: ☑DVD
Sito Internet: http://it.malwarebytes.org

L'avvio di Firefox, Chrome e Internet Explorer è diventato lentissimo, così come la navigazione sul Web: da cosa può dipendere? In alcuni casi la colpa è delle troppe estensioni installate nel browser, ma il più delle volte la causa è ben più grave e ha un nome preciso: toolbar! Sempre più spesso, infatti, ci ritroviamo queste fastidiose e pericolose barre degli strumenti installate nei nostri browser apparentemente senza alcuna azione da parte nostra. In realtà, nella maggior parte dei casi vengono aggiunte al sistema contestualmente all'installazione di software freeware ed eliminarle, una volta insidiatesi nel browser, diventa una vera impresa. Molto spesso trasformano le pagine che visitiamo in un insieme di banner pubblicitari e alcune, addirittura, dirottano il nostro traffico su siti specifici modificando i risultati di ricerca di Google.

Navigazioni a rischio

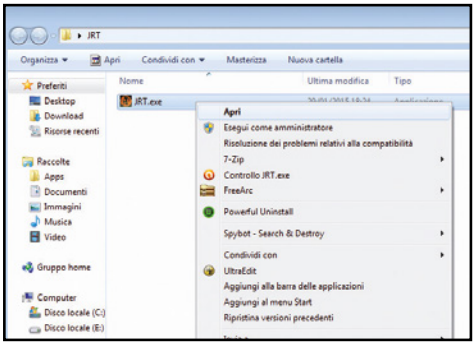
Non tutte le toolbar, comunque, sono pericolose. Quelle integrate nel browser contengono spesso strumenti utili all'utente e permettono di richiamare velocemente i nostri siti preferiti, gestire i download con un clic o attivare e disattivare i plug-in e le estensioni. Quelle delle quali ci dobbiamo preoccupare sono le toolbar di terze parti, ovvero sviluppate da aziende che nulla hanno a che fare con Google, Mozilla e Microsoft e il cui fine è soltanto quello di riempire il nostro browser di banner indesiderati e spyware pronti a rubare i nostri dati personali. Fortunatamente, gli strumenti per difenderci non mancano. In questo articolo vedremo come sfruttare al meglio tutti questi software di sicurezza progettati proprio per rimuovere questa inutile zavorra che rallenta il browser e la navigazione su Internet e ripulire il sistema da eventuali tracce di malware.

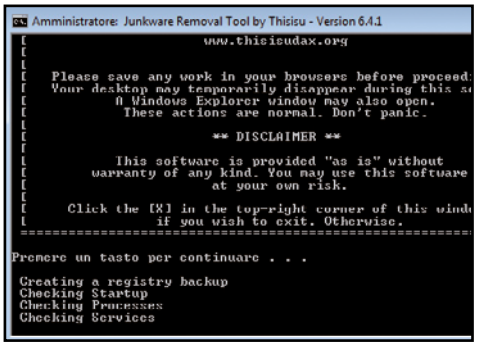
LE TOOLBAR PIÙ "PERICOLOSE" CHE BISOGNA TENERE ALLA LARGA DAL PC

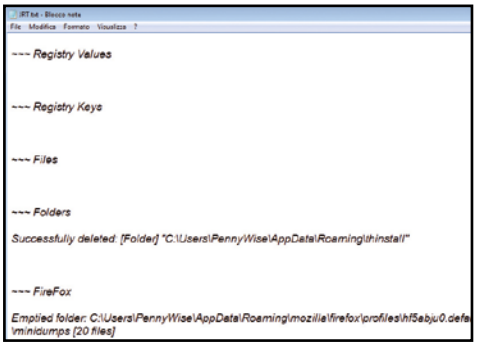
conduit · incredibar By Perion · OFFERBOX
dealply · @mail.ru · PRICEGONG we compare, you save
Delta Search · MyStart By IncrediMail.com · Snap.do
FunmoOds · mywebsearch · SOMOTO software monetization
iminent · YONTOO · sweet im

A Rimuoviamole in pochi clic

Prima di cancellare le toolbar che infettano il nostro browser conviene eliminare i file e i software che ne hanno consentito l'installazione. Per farlo useremo due software che faranno il lavoro sporco in automatico.







1 Un tool specializzato

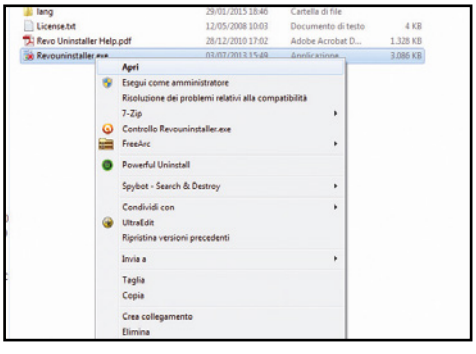
Scompattiamo l'archivio compresso *JRT.zip* che troviamo sul nostro Win DVD-Rom. Assicuriamoci di aver prima chiuso il nostro browser e clicchiamo due volte sul file *JRT.exe* contenuto al suo interno per avviare il tool di pulizia Junkware Removal Tool.

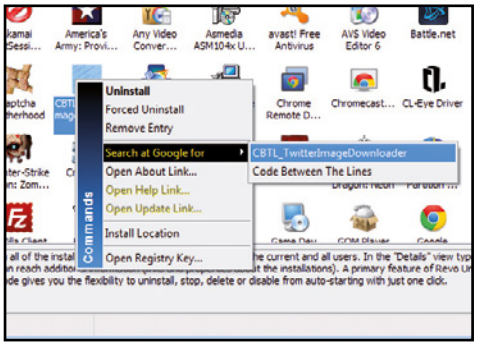
2 Il sistema viene analizzato

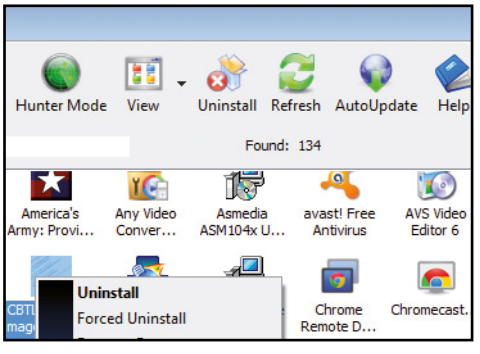
Il programma non richiede alcuna installazione. Una volta avviato, caricherà automaticamente una schermata del Prompt dei comandi di Windows. A questo punto, non dovremo fare altro che premere un tasto qualsiasi per avviare la scansione completa del sistema.

3 Eliminiamo la spazzatura

Attendiamo pazienti che il programma faccia il suo dovere analizzando file, voci del registro e add-on del browser. Terminata la scansione, si aprirà automaticamente un file testuale di log contenente gli eventuali file malevoli eliminati con successo dal PC.







4 Individuiamo il superfluo

Per completare la pulizia del browser dobbiamo utilizzare il programma gratuito Revouninstaller. Scompattiamo l'archivio compresso *Revouninstaller.zip* che troviamo all'interno del nostro Win DVD-Rom e avviamolo eseguendo il file *Revouninstaller.exe*.

5 Quale programma rimuovere?

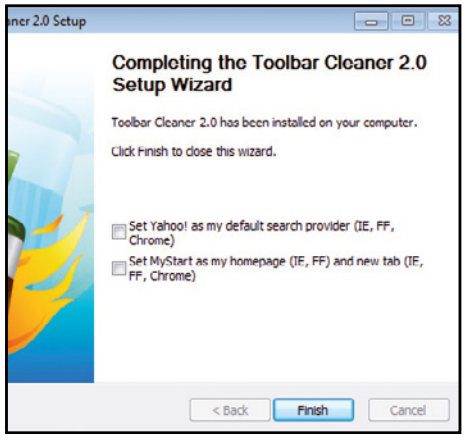
Dopo una veloce analisi del sistema, Revouninstaller ci fornirà la lista con tutti i software già installati nel PC. Cliccando sopra con il tasto sinistro del mouse e selezionando *Search at Google for* ci consentirà di verificare se si tratta di malware o meno.

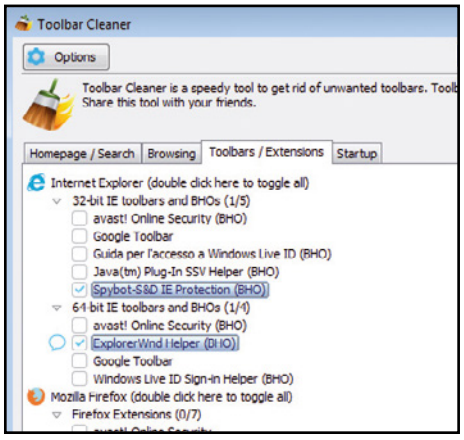
6 Pulizia ultimata!

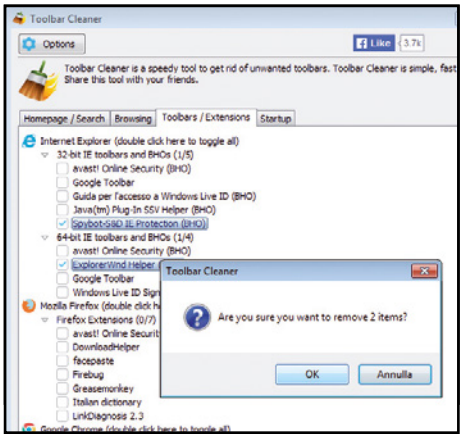
Una volta identificato un software potenzialmente dannoso possiamo procedere direttamente alla rimozione dello stesso cliccando con il tasto destro del mouse sul nome e selezionando *Uninstall* oppure cliccando sullo stesso pulsante nella barra strumenti in alto.

B Per una pulizia più approfondita

Effettuate le operazioni preliminari, possiamo proseguire con l'eliminazione delle toolbar tramite Toolbar Cleaner, software che permette la rimozione di questi add-on indesiderati dai nostri browser.







1 Installiamo il programma

Per prima cosa installiamo il programma tramite il suo eseguibile che troviamo sul Win CD/DVD-Rom, all'interno dell'archivio *ToolbarCleaner.zip*. Nell'ultima schermata dell'installazione togliamo la spunta dalle due voci indicate e clicchiamo *Finish*.

2 Troviamo le toolbar…

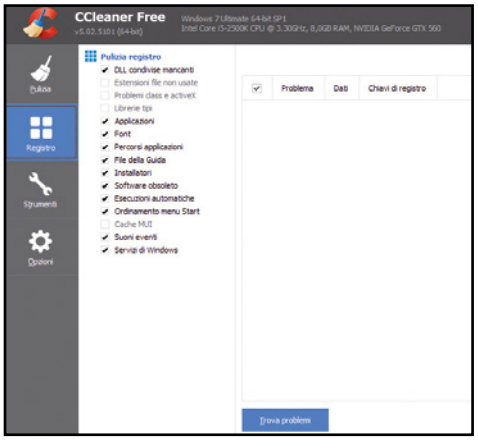
Una volta avviato il programma, spostiamoci nella scheda *Toolbars / Extensions*. In questa sezione vengono indicati tutti i browser installati nel nostro computer e le relative toolbar. Indichiamo quali sono quelle indesiderate selezionandole con un segno di spunta.

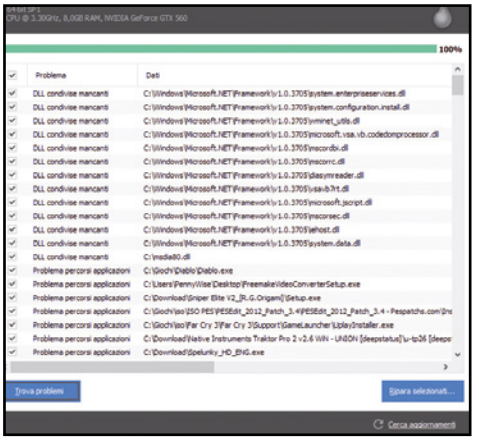
3 … ed eliminialole!

A questo punto, per eliminare le toolbar selezionate sarà sufficiente premere il pulsante *Remove Selected Toolbar(s)/BHO(s)* in basso. Il programma ci chiederà conferma dell'eliminazione: clicchiamo sul pulsante *OK* e attendiamo la fine del processo di cancellazione.

C Ora tocca al registro di sistema

Per ripulire completamente il nostro browser è necessario eliminare eventuali tracce di malware rimaste nel sistema dopo la rimozione delle toolbar. Per fare ciò ci viene in soccorso CCleaner.





1 Lo spazzino virtuale

Scompattiamo l'archivio compresso *CCleaner.zip* che troviamo sul nostro Win DVD-Rom ed eseguiamo il file contenuto al suo interno per avviare l'installazione di CCleaner. Al termine, spuntiamo *Esegui CCleaner* e premiamo sul tasto *Fine* per avviare il programma.

2 Un registro senza errori

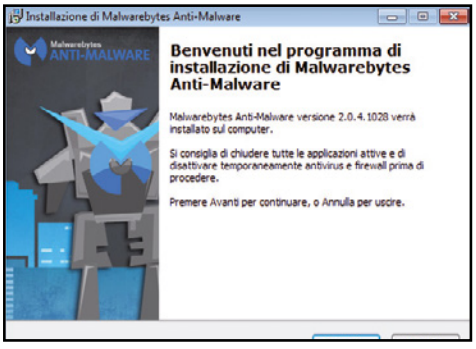
Spostiamoci nella sezione *Registro* e in *Pulizia registro* lasciamo selezionate le voci predefinite, quindi clicchiamo sul pulsante *Trova problemi*. Il programma analizzerà il registro di configurazione alla ricerca di eventuali tracce dei programmi rimossi precedentemente.

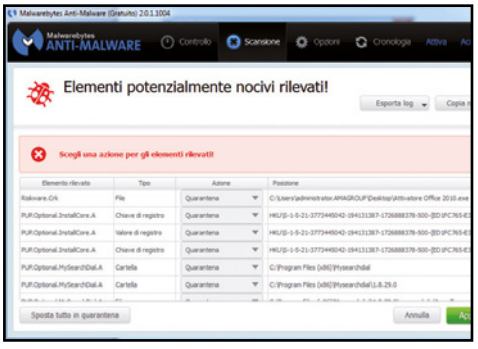
3 Cancelliamo le chiavi inutili

Terminata l'analisi del registro (la procedura potrebbe durare diversi minuti) CCleaner ci restituirà una lista con tutti gli errori rilevati. Per procedere alla pulizia ci basterà cliccare sul pulsante *Ripara selezionati (pulsante in basso a destra)* e attendere che il programma faccia il suo dovere.

Ripristiniamo il browser

Molte delle toolbar di terze parti nascondono malware pericolosi per il nostro computer. Per rimuoverli, però, non sempre è sufficiente il nostro antivirus. Vediamo come riconoscerli e rimuoverli.





1 Il cacciatore di malware

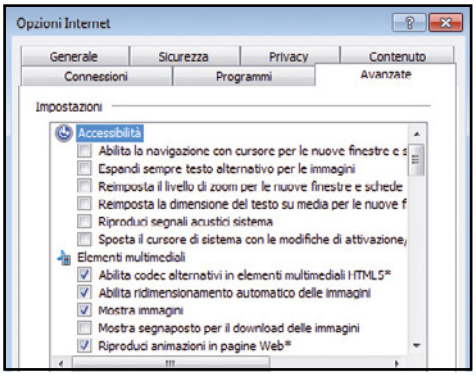
Per prima cosa installiamo il programma MalwareBytes Anti-Malware (presente sul Win DVD-ROM) seguendo le istruzioni riportate a schermo e facendo attenzione a togliere la spunta dalla voce *Attiva la prova gratuita* per non installare la versione commerciale.

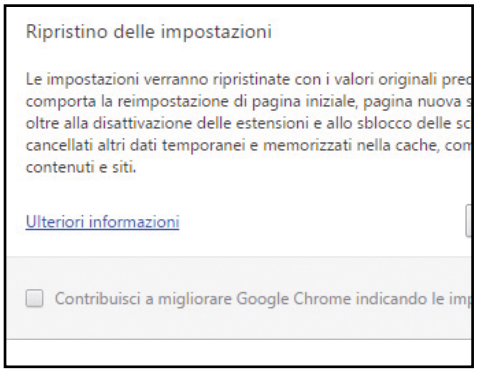
2 Avviamo la scansione

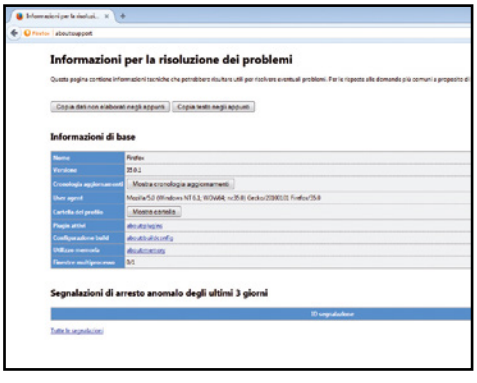
Una volta avviato il programma, spostiamoci nella sezione *Scansione*, selezioniamo e, successivamente, clicchiamo sul pulsante *Scansione*. Il programma avvierà l'analisi del sistema alla ricerca di eventuali malware e software malevoli presenti nel nostro PC.

3 Mettiamo i file in quarantena

Terminata la scansione (che potrebbe durare diversi minuti), il programma ci restituirà la lista di tutti gli elementi pericolosi rilevati. Assicuriamoci che la voce *Azione* sia impostata su *Quarantena* per le voci rilevate e clicchiamo sul pulsante *Applica azioni*.







4 Ripristiniamo IE

Vediamo ora come ripristinare i nostri browser e farli tornare al loro stato originario. Nel caso di Internet Explorer clicchiamo su *Strumenti/Opzioni Internet/Avanzate/Reimposta*. Tutte le impostazioni saranno ripristinate a quelle predefinite.

5 Chrome come nuovo!

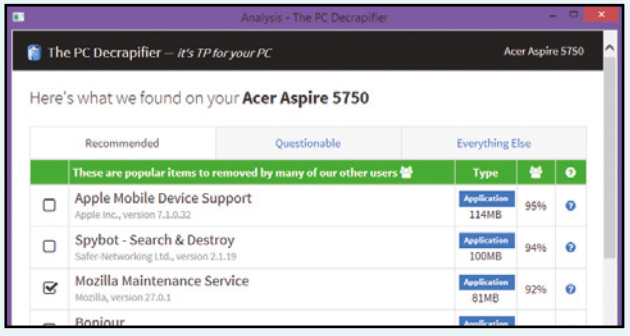
Nel caso di Google Chrome, invece, clicchiamo su *Impostazioni/Mostra Impostazioni avanzate* e selezioniamo la voce *Ripristino delle impostazioni*. A questo punto si aprirà un popup all'interno del quale dovremmo selezionare la voce *Ripristina*.

6 Il menu segreto di Firefox

Per ripristinare il browser alle impostazioni predefinite è necessario accedere ad un menu nascosto digitando *about:support* nella barra degli indirizzi e premendo *Invio*. Basterà selezionare la voce *Ripristina Firefox* per ripulire il browser.

RIPULIAMO IL NOSTRO COMPUTER APPENA ACQUISTATO

Quando acquistiamo un nuovo PC molto spesso troviamo al suo interno programmi preinstallati dalla dubbia utilità che non fanno altro che rallentare il funzionamento del sistema. Potremmo rimuoverli manualmente, ma richiederebbe troppo tempo. Meglio usare un programma gratuito come The PC Decrapifier che ricerca automaticamente i programmi superflui e ci consiglia quelli da disinstallare. Il programma non necessita di installazione: avviamolo e clicchiamo ***Analyze*** per analizzare automaticamente il sistema. Al termine ci verrà restituita una schermata con tutti i programmi generalmente preinstallati e che PC Decrapifier ritiene superflui. Selezioniamo con una spunta quelli che desideriamo rimuovere, clicchiamo ***Remove Selected*** e confermiamo con ***Begin Removal now***. Attendiamo la schermata di conferma, chiudiamo il programma e riavviamo il PC.



Scarica tutto dalle reti segrete

Software e abbonamento Premium per avere libero accesso ai canali underground del file sharing

Cosa ci occorre

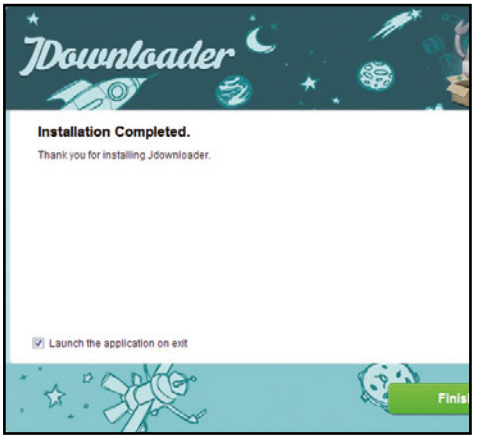
15 MIN.
FACILE

DOWNLOAD MANAGER
JDOWNLOADER
Lo trovi su: ☑DVD
SOFTWARE COMPLETO
Sito Internet:
http://jdownloader.org

Uno degli aspetti sicuramente più interessanti di Internet è la possibilità di condividere con altri utenti e scaricare sul proprio computer file di ogni genere, come ad esempio software o contenuti multimediali. Fino a qualche tempo per lo scambio e il download dei file gli Internauti utilizzavano per lo più le reti di file sharing, ma essendo queste divenute sempre più lente e piene di fake, hanno deciso man mano di passare ai più efficienti servizi di file hosting. Questi, generalmente, forniscono due tipi di accesso: gratuito e premium. Il primo con-

I download dal file

Vediamo come installare e configuranre JDownloader per scaricare dai siti di file hosting in modo facile e veloce.



1 Procediamo con il setup

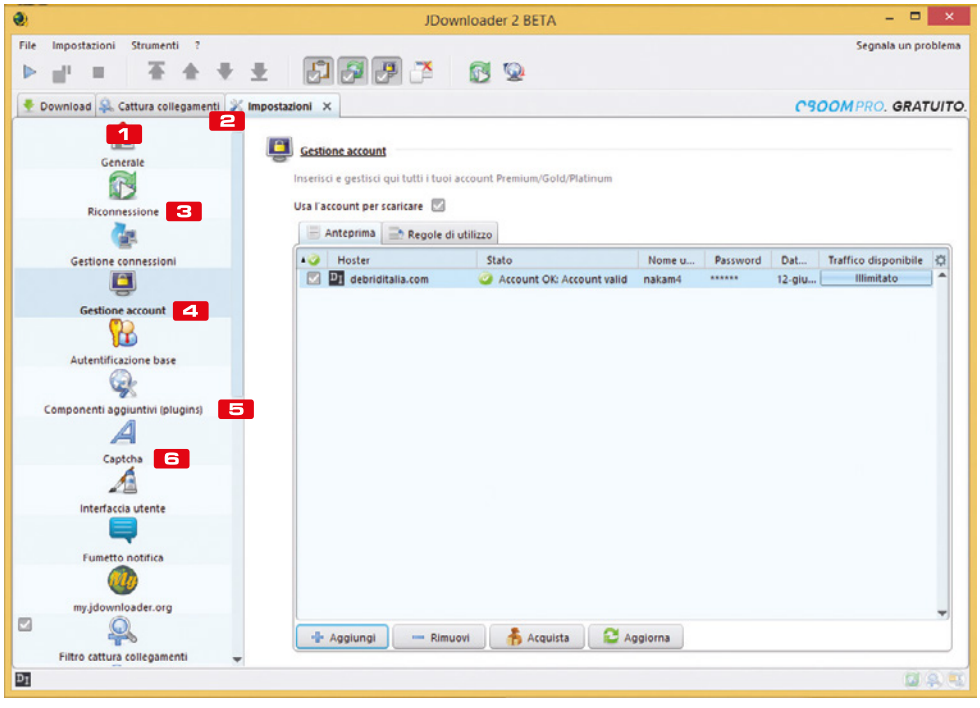
Estraiamo l'archivio compresso *WinDownloader2015.zip* lo trovi sul Win DVD-Rom), avviamo l'eseguibile di JDownloader e procediamo con l'installazione seguendo i passi della procedura guidata. Saremo così subito operativi per scaricare senza limiti dai siti di file hosting.

sente di scaricare file senza pagare nulla, ma occorre inserire un codice CAPTCHA di verifica per ogni download, non si possono scaricare contemporaneamente più file dallo stesso servizio e tra un download e il successivo deve trascorrere un certo tempo. L'account premium, invece non ha questi limiti ma comporta il pagamento di un canone.

Download senza limiti dal file sharing

Come fare allora per sfruttare al massimo la nostra banda ADSL e scaricare a tutta velocità dalla Rete? La soluzione si chiama Win Downloader, un pacchetto che comprende un download manager molto efficiente come JDownloader che permette di gestire automaticamente gli scaricamenti dalla Rete, senza preoccuparci di nulla. Questo software infatti dispone di numerose funzioni specifiche per i siti di file hosting, come ad esempio il riconoscimento degli URL e dei codici CAPTCHA. Vediamo subito come scaricare al massimo dalla Rete con Win Downloader 2015 e i trucchi avanzati che troviamo nelle prossime pagine.

LE FUNZIONI DI WIN DOWNLOADER 2015



1 DOWNLOAD
Da questa scheda è possibile tenere sotto controllo i download attivi

2 CATTURA COLLEGAMENTI
JDownloader cattura automaticamente i collegamenti ai contenuti scaricabili dai vari servizi di file hosting

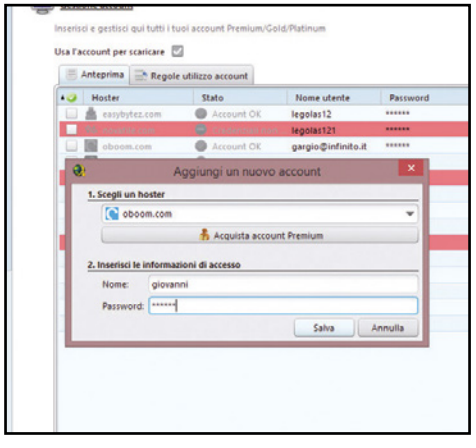
3 RICONNESSIONE
Una funzione utile che permette di riprendere in automatico il download dei file in coda

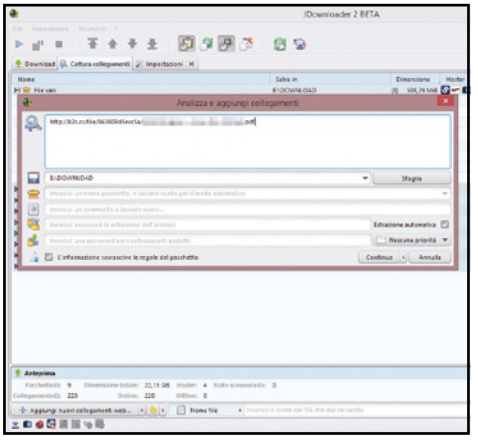
4 GESTIONE ACCOUNT
Da questa sezione è possibile configurare il nostro account premium con Debrid Italia

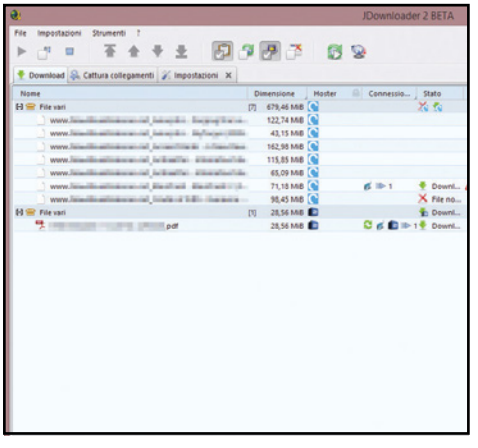
5 COMPONENTI AGGIUNTIVI
JDownloader può essere potenziato grazie a plugin che aggiungono nuove funzioni al programma

6 CAPTCHA
Possiamo configurare il programma per risolvere automaticamente i captcha usati da alcuni file hosting

hosting sono automatici!







2 Un account senza limiti

Se abbiamo sottoscritto un account Premium ad esempio a Debrid Italia, configuriamolo in JDownloader per avviare i download senza limiti. Da *Impostazioni/Gestione account* clicchiamo *Aggiungi*. Selezioniamo il servizio e inseriamo le informazioni di accesso (Username e Password) e cliccare *Salva*.

3 Alla ricerca di link

Configurato JDownloader, aggiungiamo i file da scaricare. Clicchiamo *Aggiungi nuovi collegamenti Web*, inseriamo l'URL del file trovato su Internet e clicchiamo *Continua*. Possiamo anche importare automaticamente i collegamenti cliccando col destro su un link e selezionando *Copia indirizzo*.

4 Avviamo il download

Nella finestra *Cattura collegamenti* troveremo tutti i file aggiunti a JDownloader e potremo verificarne la disponibilità. Per scaricarli selezioniamoli e clicchiamo *Avvia download*. Dalla finestra *Download* potremo controllarne lo stato e impostare il limite massimo di banda utilizzabile.

SCARICA A MILLE CON LE FUNZIONI AVANZATE DI JDOWNLOADER

1 IMPORTARE I FILE CON UN CLIC

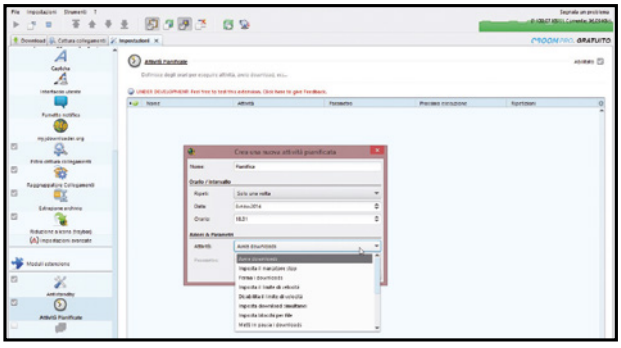
Per scaricare un file con JDownloader ci sono diversi modi. Oltre a cliccare sul tasto *Aggiungi nuovi collegamenti web*, possiamo anche trascinare un file testo contenente i vari link. In alternativa possiamo importare contenitori di file nei formati *DLC* (*Download Link Container*), *CCF* (*Cryptload Container Format*) o *RSDF* (*Rapidshare Downloader Format*). Questi contenitori si trovano solitamente sui portali dove si recuperano i link. C'è però un altro sistema ancora più veloce ed è quello della funzione *Click'n'Load*. Per usarla il programma deve essere attivo sul PC. Se lo è, il sito hoster in cui sono presenti i link attiva il pulsante *Click'n'Load*. Basterà cliccarci sopra per aggiungere i link nella finestra *Cattura collegamenti*.

2 UN NUOVO LOOK PER L'INTERFACCIA

Se i colori predefiniti dell'interfaccia di JDownloader non dovessero piacerci, possiamo modificarli per renderlo più vicino ai nostri gusti. Per farlo andiamo in *Impostazioni/Impostazioni avanzate*. Qui troveremo una finestra con una serie di voci. Tutte quelle che iniziano con *LAFSettings* ci permettono di personalizzare manualmente i colori dei vari componenti del programma. La voce *GraphicalUserInterfaceSettings: Look And Feel Theme* invece ci consente di cambiare velocemente il tema del programma. Per impostazione predefinita è selezionato quello DEFAULT. Possiamo però sceglierne un altro tra quelli disponibili. Una volta selezionato il nuovo tema, il programma ci chiederà se vogliamo installarlo. Confermiamo, portiamo a termine l'installazione e riavviamo JDownloader per applicare le modifiche.

3 DOWNLOAD PIANIFICATI

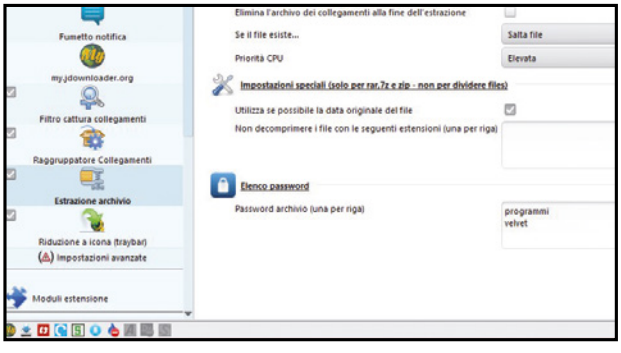
Può capitare di voler scaricare i file solo in un secondo momento, magari ad un'ora in cui tutti dormono e non ci sono quindi problemi ad utilizzare tutta la banda. In questo caso è possibile pianificare lo scaricamento dei file. Per farlo andiamo in *Impostazioni* e in *Moduli di estensione* abilitiamo la funzione *Attività Pianificate*. Clicchiamo su *Aggiungi* per configurare la prima attività. Diamo un nome, impostiamo l'orario o l'intervallo e scegliamo l'attività che vogliamo eseguire automaticamente.



Possiamo scegliere tra avviare i download, metterli in pausa o anche impostare dei parametri sulla velocità. Ciò può rivelarsi utile se non vogliamo arrestare lo scaricamento ma solo limitare la velocità di download perché ad un determinato orario la connessione serve anche ad altre persone).

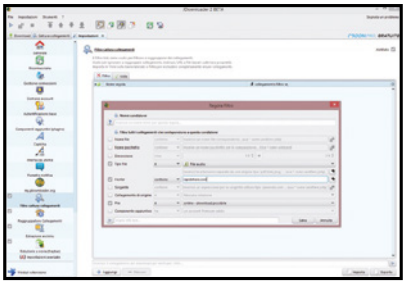
4 PASSWORD ACQUISITE AUTOMATICAMENTE

Molti file vengono scaricati in archivi compressi protetti con una password. Se il download viene fatto da fonti che utilizzano sempre le stesse password, possiamo creare un elenco in modo che il programma le prenda automaticamente e le utilizzi per scompattare i vari archivi senza doverle immettere manualmente ogni volta. Per farlo andiamo in *Impostazioni/Estrazione archivio* e nel campo *Elenco password* digitiamo le password una per riga. JDownloader, quando scaricherà un file compresso protetto da password, proverà ad aprirlo con quelle inserite. Nel caso in cui nessuna fosse corretta, una finestra ci chiederà di inserirla. Dopo averlo fatto, anche quest'ultima verrà aggiunta automaticamente alle altre.



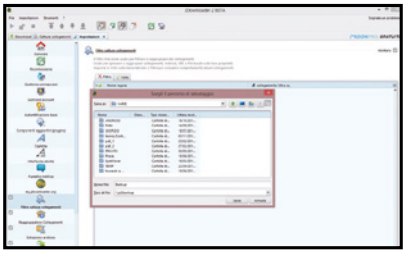
5 EVITARE SITI E TIPI DI FILE INDESIDERATI

JDownloader ha la funzione di cattura automatica dei link. In altre parole, quando clicchiamo su un collegamento col tasto destro e selezioniamo *Copia*, se il programma è aperto l'URL verrà automaticamente aggiunto alla finestra *Cattura collegamenti*. Se però vogliamo bloccare alcuni tipi di file o siti per evitare download accidentali, andiamo in Impostazioni/Filtro cattura collegamenti e clicchiamo su *Aggiungi* per inserire il primo filtro. Dalla finestra che si apre diamo un nome alla regola e specifichiamo le condizioni per applicarlo. Se ad esempio vogliamo bloccare il download dei file video, spuntiamo la casella *Tipo file* e scegliamo la tipologia dal menu a tendina. Se vogliamo bloccare solo determinate estensioni, non dobbiamo far altro che digitarle nel campo sottostante separate da una virgola. Per bloccare i download da un sito specifico, spuntiamo la voce *Hoster*, dal menu a tendina scegliamo l'opzione contiene e nel campo accanto digitiamo l'URL del sito (ad esempio rapidshare.com).



6 RIPRISTINIAMO I DOWNLOAD SU UN ALTRO PC

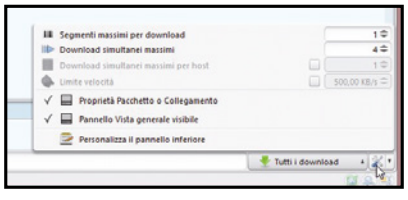
Possiamo trovarci nella situazione di dover reinstallare JDownloader o perché stiamo cambiando il computer o perché magari siamo costretti a formattarlo perché è stato infettato da un virus. Per non perdere tutti i link fortunatamente il nostro download manager ci permette di effettuarne un backup. Per farlo andiamo in *File/Backup/Backup di tutte le impostazioni*. Per eseguire il backup ci verrà chiesto di riavviare JDownloader. Confermiamo con *Continua*, selezioniamo la cartella in cui eseguire il backup e clicchiamo su *Salva*. Il file di backup avrà estensione *jd2backup*. Per ripristinarlo, dopo aver reinstallato JDownloader,



basterà andare in *File/Backup/Ripristina impostazioni*. Ricordiamo che facendo il ripristino JDownloader sovrascriverà tutte le impostazioni e la lista dei link.

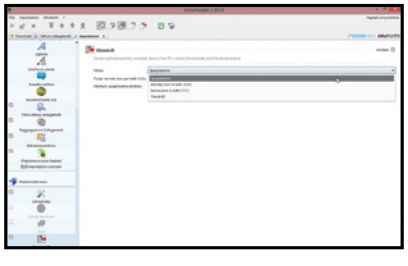
7 SFRUTTARE AL MASSIMO LA BANDA

Molti siti di file hosting impongono dei limiti nella velocità massima del download. A volte è possibile scaricare al massimo a 50-100 Kbps, molto meno rispetto alla connessione offerta dalla nostra ADSL. In questo caso, per sfruttare al massimo la banda conviene mettere a scaricare più file contemporaneamente. Per farlo andiamo nella finestra *Impostazioni/Generali*. La sezione *Gestione download* ci permette appunto di impostare i *Download simultanei massimi*. Per velocizzare lo scaricamento di un singolo file, invece, possiamo agire su *Segmenti massimi per download* (se l'hoster lo supporta): possiamo iniziare impostando 2 segmenti e poi provare ad aumentare con step successivi per vedere se la velocità di scaricamento aumenta. Possiamo modificare velocemente queste impostazioni in qualsiasi momento anche cliccando sull'icona in basso a destra mostrata nella finestra *Download*.



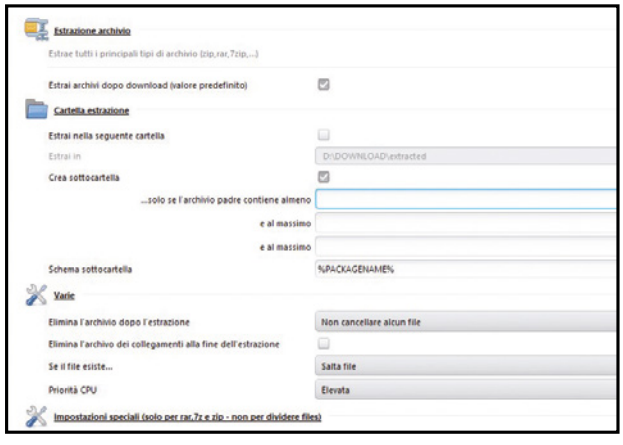
8 SPEGNIMENTO AUTOMATICO

Per terminare i download messi in coda capita di lasciare il computer acceso. Possiamo però impostare JDownloader in modo tale che spenga automaticamente il PC quando tutti i processi vengono terminati. Per farlo andiamo in *Impostazioni* e nella sezione *Moduli estensione* presente in basso a sinistra abilitiamo l'opzione *Chiusura JD*. Attraverso il menu a tendina visualizzato in *Modo* selezioniamo cosa vogliamo che il programma faccia al termine dei download. Possiamo scegliere tra spegnere il computer, metterlo in standby, passare alla modalità ibernazione o semplicemente chiudere solo JDownloader.



9 ESTRARRE GLI ARCHIVI IN CARTELLE SEPARATE

Per impostazione predefinita JDownloader scompatta i file compressi nella cartella scelta per il download. Spesso, però, questi archivi contengono più file e, per evitare che si crei confusione, conviene che ogni archivio venga scompattato in una cartella separata. Per farlo andiamo in *Impostazioni/Estrazione archivio* e spuntiamo la voce *Crea sottocartella*. Teniamo presente che se l'archivio contiene solo un file, possiamo tranquillamente lasciare che venga scompattato nella cartella principale e ricorrere alle cartelle separate solo con archivi che contengono più file. In questo caso basterà impostare il valore *2* alla voce solo se l'archivio padre contiene almeno. Possiamo inoltre fare il modo che gli archivi vengano cancellati automaticamente dopo la loro estrazione per non occupare inutilmente spazio sull'hard disk.



10 CONFIGURIAMO LA RICONNESSIONE

Molti hoster impongono un limite al numero di download al giorno. Possiamo aggirare tale limite riavviando il router in modo che venga assegnato dal provider un nuovo IP così da iniziare a scaricare di nuovo. Per evitare di dover riavviare ogni volta manualmente il modem/router, possiamo configurare JDownloader perché lo faccia automaticamente e quindi anche in nostra assenza. Per configurare tale opzione andiamo in *Impostazioni/Riconnessione*. In *Modo riconnessione* selezioniamo *LiveHeader*, inseriamo l'indirizzo IP del router, clicchiamo su *Crea nuovo script* e poi su *Avvia*. Verrà quindi aperta una pagina del browser per effettuare l'accesso al pannello di controllo del router. Spostiamoci nella pagina in cui è presente il pulsante per il riavvio o la riconnessione e premiamolo. Quando il router si sarà riavviato, salviamo lo script in JDownloader e abilitiamo la riconnessione automatica cliccando sul pulsante presente al centro della barra degli strumenti.

11 CONTROLLO REMOTO DEI DOWNLOAD

Una funzione sconosciuta della nuova versione di JDownloader è la possibilità di controllare i download da remoto. Per abilitarla andiamo su http://my.jdownloader.org e clicchiamo su *Register* per registrare un account gratuito al servizio. Inseriamo il nostro indirizzo e-mail, il codice captcha e premiamo *Register*. Completiamo la registrazione cliccando sul link inviatici per e-mail e scegliamo una password per utilizzare il servizio. Andiamo quindi su JDownloader, spostiamoci in *Impostazioni/my.jdownloader.org* e digitiamo l'indirizzo di posta elettronica e la password scelti per il servizio. Dopo aver cliccato su *Connetti* potremo controllare da remoto JDownloader da qualsiasi computer o dispositivo connesso a Internet andando sul sito http://my.jdownloader.org. Inoltre, dato che molti hoster richiedono l'inserimento di un codice captcha per avviare il download, installando l'applicazione MyJDownloader per Android, scaricabile da www.winmagazine.it/link/2856, potremo inserirli quando serve direttamente dallo smartphone o il tablet senza essere per forza davanti al PC.

12 VIDEO DI YOUTUBE NEL GIUSTO FORMATO

JDownloader integra tantissimi plug-in per scaricare non solo i file dai siti di hosting, ma anche filmati dai siti di condivisione video come YouTube. Non dobbiamo far altro che aggiungere l'URL del video alla finestra *Cattura collegamenti*. Quando carichiamo ad esempio un video di YouTube, JDownloader automaticamente seleziona la qualità migliore e ci dà anche la possibilità di scaricare solo l'audio, opzione utile ad esempio per estrarre un brano musicale da un videoclip. Cliccando sulla piccola freccia verso il basso possiamo però scegliere di scaricare il file in uno degli altri formati disponibili in modo da selezionare quello più adatto al dispositivo sul quale vogliamo scaricarlo. Possiamo modificare le impostazioni predefinite di questi plug-in andando in *Impostazioni/Componenti aggiuntivi*. Selezionando, ad esempio, il plug-in di YouTube possiamo scegliere i formati consentiti e un nome personalizzato per i download.

Il telefono invisibile!

Configura un dispositivo VOIP "inesistente" per dire e scrivere di tutto senza essere intercettati!

Cosa ci occorre

30 MIN. FACILE

CLIENT DI CHAT
JITSI
SOFTWARE COMPLETO
☑DVD
Sito Internet:
https://jitsi.org

CLIENT DI CHAT
TORCHAT
SOFTWARE COMPLETO
☑DVD
Sito Internet:
https://github.com/prof7bit/TorChat

ADD-ON PER CHROME
MUMAIL-CRYPT
SOFTWARE COMPLETO
☑DVD
Sito Internet:
https://chrome.google.com/webstore

BROWSER WEB
COMODO ICEDRAGON
SOFTWARE COMPLETO
☑DVD
Sito Internet:
www.comodo.com

Note: Il pacchetto Cryptophone può essere scaricato dall'indirizzo www.winmagazine.it/link/2385

La riservatezza è un diritto inalienabile di ogni individuo. In un mondo dominato dai social network, dove la parola d'ordine è comunicare e condividere rapidamente, nessuno si preoccupa più di salvaguardare la segretezza delle proprie conversazioni, salvo poi piangere lacrime amare quando foto e "pensieri" privati vengono rubati e resi pubblici! La colpa è della cattiva educazione del nuovo "homo informaticus", il quale spesso non comprende che la propria identità digitale può avere un impatto non trascurabile anche sulla vita reale. In tutto questo, la notizia positiva è che, con un po' di impegno e buona volontà, è ancora possibile garantire il proprio diritto alla privacy e con Windows può essere molto semplice farlo. Scopriamo subito come e perché.

Diritto alla riservatezza

Ogni persona ha il diritto di poter comunicare in totale segretezza. Non ci soffermeremo sugli aspetti oscuri legati al favoreggiamento di potenziali reati, perché la necessità di difendere un individuo soggetto a violazioni della libertà di opinione è indubbiamente più importante (i blogger cinesi ne sanno qualcosa). Ovviamente, non bisogna per forza essere un martire o un delinquente: quanto faremo può essere utile per tenere al sicuro gli aspetti della nostra vita che non vogliamo vengano divulgati. La sola criptazione del messaggio non basta per garantire la riservatezza di una comunicazione, che si può ottenere solo assicurandoci dell'identità dell'interlocutore e usando canali di comunicazione sicuri che garantiscono l'anonimato. E anche se nella maggior parte dei casi bastano semplici messaggi cifrati, acquisire la mentalità di chi per necessità deve "muoversi nell'ombra" può essere sempre utile.

Identifichiamo l'interlocutore

Gli appassionati di crittografia e i "paranoici"

A Installiamo il Cryptophone

Vediamo subito come impostare il client di chat multiprotocollo Jitsi, configurando la criptazione automatica e il login ai più famosi servizi di messaggistica come Hangouts, Facebook e XMPP.

1 Prima installiamo

Avviamo l'installazione del programma Jitsi eseguendo il file *jitsi-2.4-latest-x86.exe* (che troviamo sul Win DVD-Rom). Clicchiamo sul pulsante *Next* nella prima schermata, accettiamo la licenza l'uso con *Accept* e terminiamo cliccando di nuovo *Next*.

2 Uno sguardo d'insieme

Una volta installato, Jitsi si presenta con un'interfaccia utente molto semplice e comprensibile, sebbene sia disponibile solo in lingua inglese. Sulla destra abbiamo la lista dei servizi di chat ai quali possiamo loggarci mentre sulla destra vedremo poi apparire la lista dei contatti.

3 Anche il VoIP

Spostiamoci nella scheda SIP: da qui possiamo addirittura autenticarci ad un servizio VoIP di cui siamo magari abbonati. La funzione è utile nel caso volessimo criptare le nostre conversazioni: ricordiamo infatti lo scandalo NSA in cui i servizi segreti ascoltarono milioni di telefonate.

trovano piacevole approfondire gli aspetti storici e matematici legati ai diversi algoritmi crittografici utilizzati per le comunicazioni. A questo proposito, la lettura del libro The code book di Simon Singh potrà soddisfare le curiosità di molti. Nel nostro caso, invece, ci concentreremo sugli aspetti pratici. Il solo uso di algoritmi di criptazione ci rende capaci di cifrare e decodificare un messaggio che può essere scambiato via e-mail o altro, ma non di identificare l'interlocutore. ***PGP*** (***Pretty Good Privacy***, www.openpgp.org), la cui versione Open Source prende il nome di ***GPG*** (***Gnu Privacy Guard***, www.gnupg.org) nasce proprio per mettere insieme uno strumento basato su chiave pubblica/privata con un sistema capace di verificare l'identità del mittente. Affinché tutto funzioni correttamente, i due interlocutori devono scambiarsi le proprie chiavi pubbliche. Per essere sicuri che la chiave appartenga realmente al nostro interlocutore, essa deve essere ottenuta "vis-à-vis". Anche se ora sono rari, in passato venivano indetti periodicamente alcuni eventi chiamati PGP Party, dove i convenuti partecipavano all'evento con il solo scopo di acquisire e firmare le chiavi pubbliche delle persone conosciute, creando così una rete di fiducia. Infine, le chiavi firmate vengono inviate (opzionalmente) su alcuni key server pubblici.

Firma dei contenuti

Utilizzando uno dei tanti programmi per GPG possiamo gestire il portachiavi e svolgere le più comuni operazioni per le quali questo strumento è stato ideato. Supponiamo di avere già una coppia di chiavi e di possedere la chiave pubblica del nostro interlocutore. Ancora prima di pensare a criptare, facciamo queste ipotesi: vogliamo che il messaggio sia in chiaro, ma vogliamo impedire che qualcuno possa alterarlo; oppure vogliamo semplicemente evitare che qualcuno possa rubarci l'identità inviando messaggi con il nostro nome e indirizzo. I contenuti, siano essi testi o file, possono essere "firmati". Chi possiede la nostra chiave pubblica potrà verificare la firma: se il contenuto è stato alterato la verifica fallirà miseramente. Probabilmente facciamo uso di questa funzionalità ogni giorno: i gestori dei software delle distribuzioni utilizzano le firme PGP/GPG per evitare che qualcuno possa interporsi tra noi e i server degli aggiornamenti e iniettare nel nostro computer pacchetti compromessi con virus e rootkit.

Cifriamo i nostri messaggi

La cifratura con PGP/GPG utilizza un approccio inverso rispetto al normale pensiero logico: il cifrario è calibrato sulla chiave pubblica del destinatario. Il processo di cifratura, infatti, non necessita di una password aggiuntiva. Chi riceverà il contenuto criptato potrà sempre verificare l'identità del mittente verificando la nostra chiave pubblica, ma utilizzerà la password della sua chiave privata per decriptare il messaggio o il file. Quando dobbiamo inviare lo stesso contenuto a più persone, possiamo creare un unico messaggio selezionando più chiavi pubbliche durante la fase di cifratura. Ogni destinatario sarà ignaro delle altre persone che riceveranno il messaggio. Altrimenti, è sempre possibile utilizzare la criptazione simmetrica, che non utilizzerà alcuna chiave pubblica e sarà decifrabile da chiunque sarà in possesso della password utilizzata durante la sua creazione. Non è una soluzione realmente sicura, perché si perde la protezione aggiuntiva derivata dalla identificazione degli interlocutori e aumenta la possibilità di violare la criptazione a patto di scoprire la password, ma a volte è sempre meglio di niente.

E-mail e chat sono al sicuro

PGP è stato realizzato tenendo a cuore la comunicazione "asincrona" delle e-mail. Ora qui si pone un problema: i server che veicolano la posta elettronica registrano tutte le informazioni necessarie per tracciare mittenti e destinatari. Le

BUONI CONSIGLI

LA CHAT BLINDATA

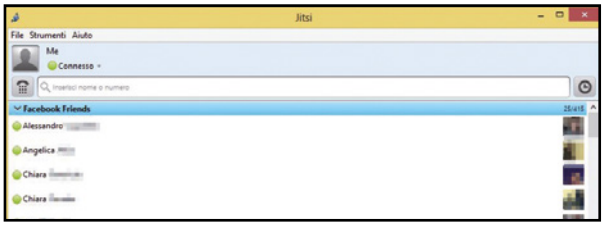
Per chi lo non lo sapesse, il protocollo XMPP è stato fin dal 1999 uno dei più usati nei programmi di chat. Presenta diverse caratteristiche che lo rendono alquanto blindato in Rete, come l'implementazione del protocollo TLS e la decentralizzazione dei server utilizzati, così da rendere di fatto impossibile l'intercettazione delle comunicazioni.

GOOGLE E FACEBOOK ALL'APPELLO

Qualora volessimo usare Jitsi anche per chattare con i nostri amici di Facebook possiamo farlo vantando una certa privacy. Non servirà infatti tenere aperto il browser per interagire con i nostri contatti, evitando così che Facebook tracci le nostre sessioni durante la navigazione Web. Basterà avviare Jitsi e loggarci al social network usando l'apposito modulo integrato. La procedura è analoga anche se usiamo il client di chat Google Talk, ora assorbito nel servizio Hangouts. Basterà infatti inserire il nostro indirizzo Gmail e la relativa password per rimanere in contatto con colleghi e amici senza rinunciare alla privacy.

B Facebook è sotto chiave

Il social network traccia ogni nostra attività on-line? Usare la chat senza browser e con un solido algoritmo di criptazione diventa allora la scelta migliore per comunicare con gli amici.



1 Effettuiamo prima il login

Per loggarci alla chat di Facebook direttamente da Jitsi dobbiamo prima andare a leggere il nostro username: per farlo, clicchiamo su *Impostazioni* (l'icona a forma di ingranaggio in alto a destra), poi su *Impostazioni account* e leggiamolo nel campo *Nome utente*.

2 Possiamo chattare in sicurezza

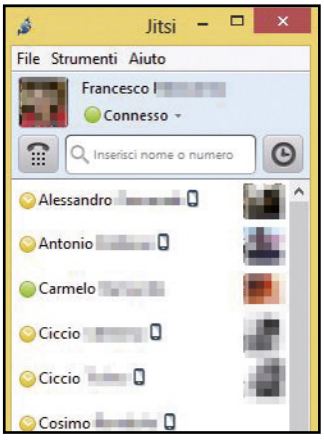
Una volta ottenuta questa informazione, inseriamolo in Jitsi insieme alla password del nostro contatto Facebook e clicchiamo *Effettua il login*. Pochi instanti e comparirà la lista di tutti i nostri amici! Potremo chattare, impostare lo stato della chat e altro ancora!

C Chat sicura con Google

Amiamo le chat ma usiamo solamente quella di Big G? Grazie a Jitsi bastano soltanto le nostre credenziali per iniziare a chattare subito con la massima sicurezza.

1 Prima i dati

Nello sezione dedicata alla chat di Google, inseriamo la nostra e-mail e la password in *Nome utente Google Talk* e *Password*. Se non abbiamo un account Google, registriamone uno con *Registrazione nuovo account Google Talk*.



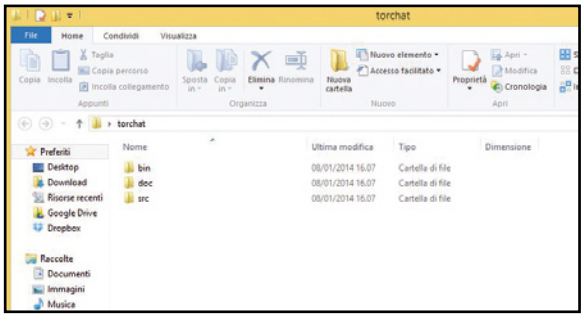
2 E adesso chattiamo!

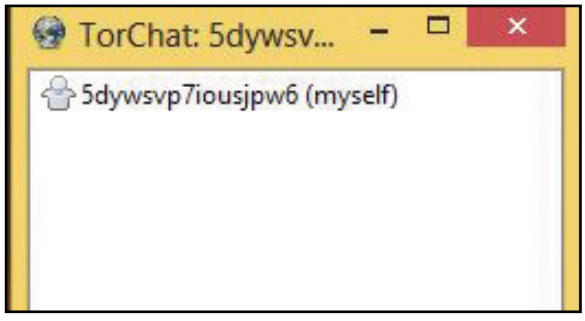
Una volta effettuato il login alla chat di Google apparirà la lista di tutti i nostri contatti, con tanto di foto del profilo. Anche qui possiamo impostare uno stato per la chat, mettendoci anche in modalità invisibile, qualora ci serva. Ora le nostre conversazioni saranno protette.

informazioni raccolte includono l'indirizzo IP, gli indirizzi di posta e in alcuni rari casi vengono configurati per "intercettare" le e-mail. Una chat, invece, è molto diversa, quasi paragonabile ad una partita di tennis, e richiede un sistema di comunicazione criptata più celere, come, ad esempio, l'***OTR. Off the Record è un protocollo crittografico che si pone sopra i protocolli di comunicazione già esistenti.*** Inizialmente venne utilizzato per rendere riservate le conversazioni tra utenti di un server IRC, ma può essere usato anche su servizi più "moderni" basati sul protocollo XMPP, come, ad esempio, Hangouts, la chat di Facebook e altri sistemi simili. Il punto di forza di questo protocollo è la possibilità di stabilire una comunicazione cifrata senza dover necessariamente effettuare uno scambio preventivo delle chiavi. Il rovescio della medaglia prende forma in tutte le problematiche relative all'autenticazione dell'interlocutore. Quando due persone entrano in contatto con OTR, il protocollo stabilisce un cifrario comune per la sessione utilizzando la propria chiave. Dopo questo "handshake" i successivi messaggi sono già criptati e, quindi, inaccessibili ad una terza persona. Ma stiamo parlando con il vero interlocutore? Il protocollo, infatti, introduce il concetto di "autorizzazione". Dopo aver chiesto una domanda segreta e ottenuto la chiave OTR su un canale sicuro (e-mail criptata con PGP, ad esempio) possiamo terminare la comunicazione o memorizzare la chiave tra quelle affidabili, che sarà automaticamente riconosciuta durante le chat successive. Possiamo usare OTR con diversi client, ma noi preferiamo usare Jitsi. A prima vista sembra essere il classico programma multi protocollo, ma sotto l'apparenza si nasconde il migliore amico di ogni "paranoico" della sicurezza. Dopo avere aggiunto nella configurazione gli account per i vari servizi di chat in cui siamo registrati (Facebook, Yahoo, Hangouts ecc.), potremo utilizzare OTR con ognuno di essi. Ovviamente, l'unico requisito è che anche il nostro interlocutore faccia uso di un client che supporti questo protocollo.

Comunicare in anonimato

Se non vogliamo lasciare tracce durante le sessioni di chat, Torchat è proprio quello che fa per noi, perché usa la rete Tor per scambiare messaggi e garantirne la non tracciabilità.



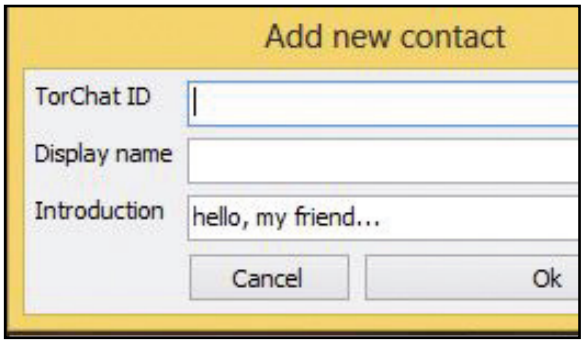


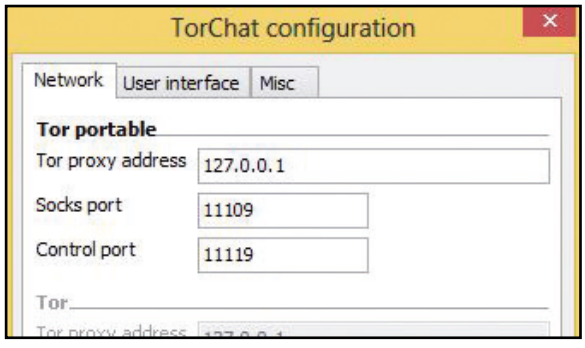
1 Una semplice installazione

Estraiamo il contenuto dell'archivio compresso *Torchat.zip* (presente sul Win DVD-Rom) e copiamo sul *Desktop* il file *torchat.exe* presente nella cartella *bin*: il software è infatti distribuito in versione portable e quindi non necessita di installazione.

2 Conserviamo l'indirizzo

Verrà creato un ID causale formato da 16 numeri e lettere: questo è il nostro ID univoco e temporaneo. Visto che è facile dimenticarlo, selezioniamo il nostro contatto col tasto destro, clicchiamo *Copy ID to clipboard* e incolliamolo (*Ctrl+V*) in un file di testo da conservare al sicuro.





3 Aggiungiamo gli amici

Per aggiungere un amico ai contatti, dobbiamo conoscere il suo nick univoco. Clicchiamo col tasto destro sull'interfaccia del programma e selezioniamo *Add contact*. Facciamoci inviare l'ID tramite e-mail (magari usando il protocollo crittografico PGP) e incolliamolo nell'apposito campo.

4 Se la connessione è bloccata…

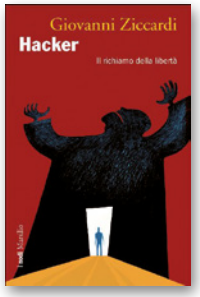
Il client non ha bisogno di alcuna configurazione, ma se il nostro provider dovesse bloccare determinate porte, basta indicare quelle giuste cliccando col tasto destro e selezionando *Settings*. Da *User interface* possiamo inoltre specificare la lingua da utilizzare per l'interfaccia.

UN BUON LIBRO

HACKER - IL RICHIAMO DELLA LIBERTÀ

Un libro che parla delle migliaia di dissidenti digitali attivi in tutto il mondo che rischiano la vita per opporsi a forme di governo liberticide e a politiche votate al controllo dei comportamenti dei cittadini.

AUTORE: G. Ziccardi
PREZZO: € 19,50
PAGINE: 286
ANNO: 2011
EDITORE: Marsilio



LEGGI SUL WEB

https://ssd.eff.org
Home page del progetto Surveillance Self-Defence sviluppato dalla EFF (Electronic Frontier Foundation, https://www.eff.org), con tante utili linee guida per la protezione della privacy e dei propri dati personali

Non solo testo

Fino ad ora ci siamo occupati solo della comunicazione testuale o basata sullo scambio di file. Qualcosa di più "dinamico" è stato mostrato con OTR. Ma qual è il modo più naturale di comunicare? L'essere umano apprende per primo l'uso della parola e solo in seguito l'arte della scrittura. Peccato che ancora oggi la quasi totalità dei sistemi di comunicazione audiovisiva si basa su protocolli poco documentati o totalmente chiusi. Ovviamente, non si possono pretendere miracoli e siamo "costretti" a fare uso di servizi più o meno affidabili. Consideriamo, ad esempio, Skype: tutti credono che sia "sicuro" e che le comunicazioni siano riservate. Ma al di là di alcuni problemi legati alla sicurezza del protocollo e alla possibilità di hijacking, Microsoft, proprietaria del client, non ha mai smentito la possibilità di poter intercettare i messaggi di chat o le comunicazioni audio/video in caso di richieste da parte delle autorità. Quindi, è palese che un programma non Open Source, con un protocollo chiuso, che non permette l'utilizzo di sistemi non centralizzati di criptazione dei messaggi dà solo la falsa illusione di poter comunicare in totale "libertà". Ma questo non è il caso di Jitsi: infatti, anche se teoricamente il protocollo nativo non supporta le "nuove" funzionalità, il client tenterà sempre di instaurare una comunicazione audiovisiva criptata e, in caso di fallimento, proverà con una connessione in chiaro e ci avvertirà di essere cauti in quanto non saremo sotto la "coperta protettiva" di un algoritmo di criptazione. Il nostro viaggio alla scoperta dei sistemi di comunicazione cifrati termina qui. I media di ogni genere e importanza non fanno altro che parlare di intercettazioni, quindi si tratta sicuramente di un argomento "caldo", non solo perché di attualità, ma soprattutto perché è la nostra stessa privacy ad essere in pericolo. Adesso non abbiamo più scuse, conosciamo gli strumenti per evitare che ciò accada e dobbiamo abituarci ad usarli!

BUONI CONSIGLI

AL SICURO SU FACEBOOK

Purtroppo, non tutte le nostre comunicazioni in Rete possono essere criptate. Il caso Datagate ha dimostrato che le nostre bacheche su Facebook sono facilmente accessibili dalle autorità impegnate in indagini e attività giudiziarie. Possiamo però nascondere almeno a spioni di ogni genere la nostra password e i post che pubblichiamo sul Diario. Per farlo, è sufficiente ricordarsi di aggiungere il suffisso *https* all'indirizzo www.facebook.com. In questo modo useremo il protocollo sicuro di comunicazione ed eviteremo che qualche malintenzionato, sniffando la nostra connessione a Internet, possa intercettare le password e i dati personali scambiati col social network.

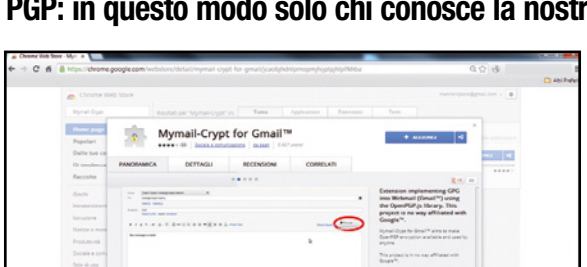
PER SAPERNE DI PIU'

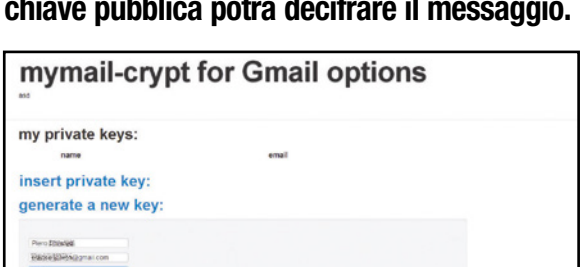
SKYPE NON E PIU SICURO

Dopo anni di onorato servizio, è caduto uno dei baluardi delle comunicazioni sicure. Anche le chat su Skype, infatti possono adesso essere intercettate. Il perché è presto detto: dopo l'acquisizione da parte di Microsoft, il programma non utilizza più una rete P2P e quindi anonima per lo scambio di messaggi tra gli utenti, ma una struttura a server centralizzati, gestita direttamente da Microsoft. Da Redmond garantiscono sulla totale sicurezza delle comunicazioni via Skype, ma ancora una volta il caso Datagate insegna che in certi casi fidarsi è bene, ma non fidarsi è meglio!

La mia posta è riservata!

Impariamo a usare un'estensione per Chrome che permette di inviare e-mail con la cifratura PGP: in questo modo solo chi conosce la nostra chiave pubblica potrà decifrare il messaggio.



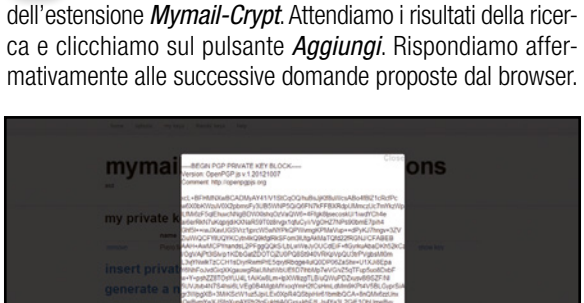


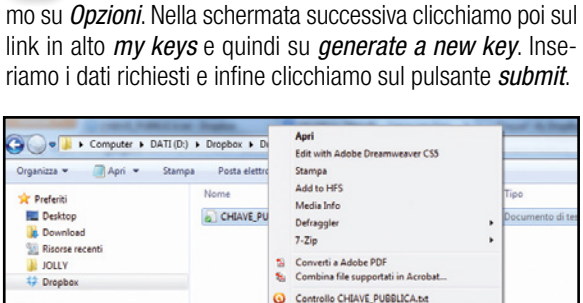
1 Installiamo Mymail-Crypt

Visitiamo l'URL https://chrome.google.com/webstore e nel campo di ricerca sulla sinistra digitiamo il nome dell'estensione *Mymail-Crypt*. Attendiamo i risultati della ricerca e clicchiamo sul pulsante *Aggiungi*. Rispondiamo affermativamente alle successive domande proposte dal browser.

2 Generiamo le nostre chiavi

Dal *Menu* di Chrome selezioniamo *Strumenti/Estensioni*. Nella lista individuiamo *Mymail-Crypt* e clicchiamo su *Opzioni*. Nella schermata successiva clicchiamo poi sul link in alto *my keys* e quindi su *generate a new key*. Inseriamo i dati richiesti e infine clicchiamo sul pulsante *submit*.



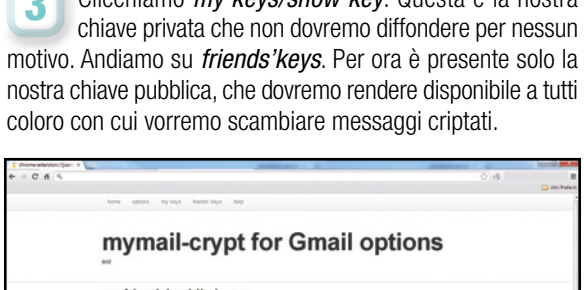


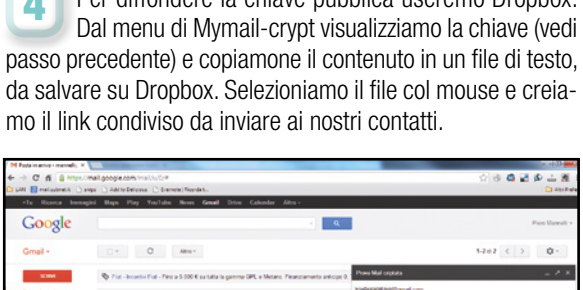
3 La chiave pubblica per gli amici

Clicchiamo *my keys/show key*. Questa è la nostra chiave privata che non dovremo diffondere per nessun motivo. Andiamo su *friends'keys*. Per ora è presente solo la nostra chiave pubblica, che dovremo rendere disponibile a tutti coloro con cui vorremo scambiare messaggi criptati.

4 Condivisione in corso

Per diffondere la chiave pubblica useremo Dropbox. Dal menu di Mymail-crypt visualizziamo la chiave (vedi passo precedente) e copiamone il contenuto in un file di testo, da salvare su Dropbox. Selezioniamo il file col mouse e creiamo il link condiviso da inviare ai nostri contatti.





5 Le chiavi dei nostri amici

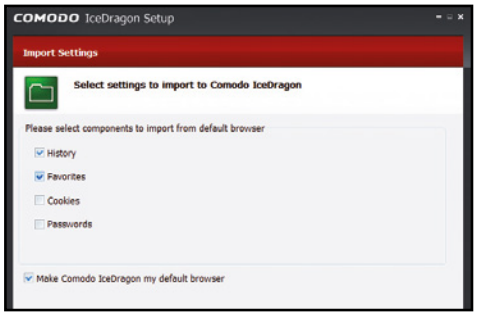
Per leggere i messaggi criptati dei nostri amici abbiamo bisogno della loro chiave pubblica. Contattiamo un amico e, dopo avergli fatto installare Mymail-crypt, facciamoci inviare la sua chiave. Da *friend's keys* clicchiamo *insert public…* e incolliamo il contenuto della sua chiave pubblica.

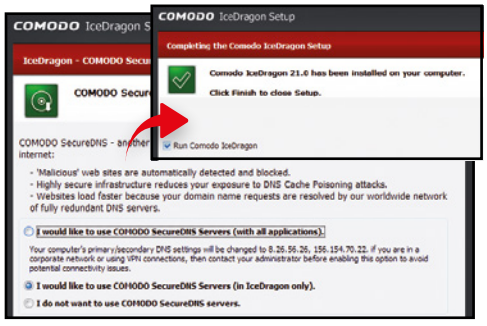
6 Facciamo qualche prova

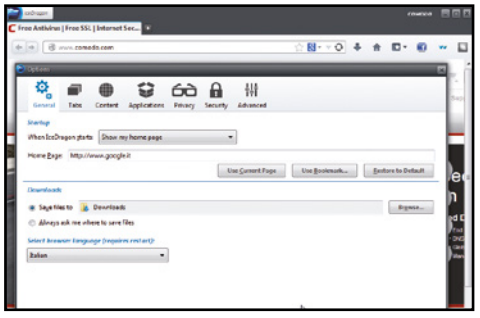
Scambiate le reciproche chiavi, testiamo il funzionamento di PGP. Componiamo un'e-mail: dopo aver scritto il testo, inseriamo la nostra password sul campo in basso, clicchiamo *Encrypt* e inviamo il messaggio. Alla ricezione, il nostro amico dovrà cliccare *Encrypt* per visualizzarlo.

Massima protezione sul Web

Usando Comodo IceDragon possiamo verificare la presenza di malware nelle pagine Web. Inoltre, grazie ad uno script per Greasemonkey, disponiamo di una tastiera virtuale che vanifica l'azione di keylogger e spyware.







1 Installiamo il browser

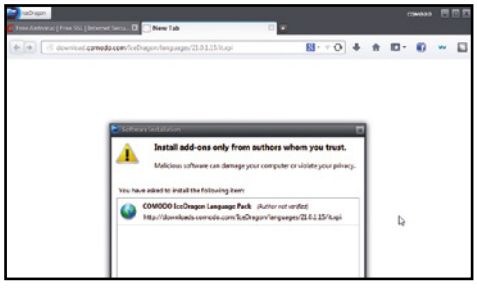
Scompattiamo l'archivio *IceDragon.zip* (scaricabile gratuitamente da *Win Extra*) ed eseguiamo il file *icedragonsetup.exe*. Clicchiamo su *I Agree* e poi su *Next*. Scegliamo gli elementi da importare dal browser di default, ad esempio cronologia (*History*) e preferiti (*Favorites*).

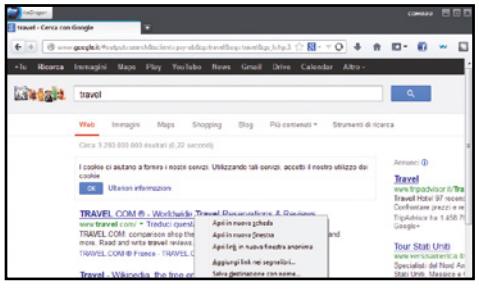
2 DNS sicuri per il Web

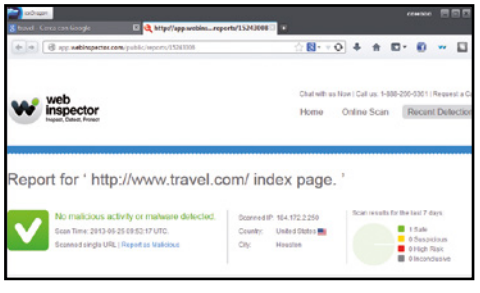
Per impostare IceDragon come browser di default selezioniamo *Make Comodo Browser my default browser* e premiamo *Next*. Lasciamo invariate le opzioni nella schermata *IceDragon - Comodo SecureDNS* e premiamo *Install*, poi *Next*, quindi *Finish*. IceDragon si aprirà automaticamente.

3 Alcune veloci impostazioni

Clicchiamo *IceDragon* in alto a sinistra, quindi su *Options*. Andiamo nella scheda *General*, digitiamo in *Home Page* la pagina Web da aprire all'avvio del browser (ad esempio www.google.it), dal menu a tendina *Select browser language* selezioniamo *Italian* e premiamo infine *OK*.







4 Un'interfaccia in italiano!

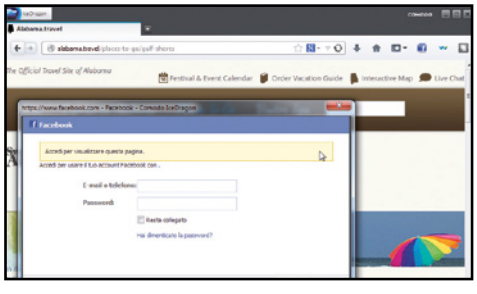
A questo punto il browser scaricherà automaticamente il pacchetto che consente di tradurre l'interfaccia utente in lingua italiana. Una volta terminato il download, facciamo clic su *Install Now*, quindi premiamo *Restart now* per riavviare il browser e rendere effettive le modifiche.

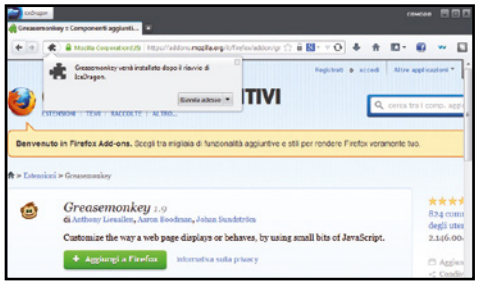
5 Alla larga dai malware

Un'operazione fondamentale che possiamo compiere è quella di eseguire una scansione di una pagina Web per verificare la presenza di eventuali malware prima di aprirla. Per farlo basta cliccare con il tasto destro su un link e poi sulla voce *Scan link with Web Inspector*.

6 Questo sito Web è sicuro!

Il browser eseguirà on-line una scansione completa della pagina Web e visualizzerà al termine un report dettagliato. In alternativa, se ci troviamo già su una pagina Web possiamo effettuarne una scansione cliccando sul pulsante in alto *Make a page scan with Comodo Web Inspector*.





7 Condividere link sui social

Possiamo usare IceDragon anche per condividere una pagina Web su un social network: clicchiamo con il tasto destro sul tasto in alto con l'icona di Facebook e selezioniamo dal menu *Facebook*, *Twitter* o *LinkedIn*. Inseriamo quindi le nostri credenziali di accesso al social network.

8 Un'estensione indispensabile

Colleghiamoci ora al sito www.winmagazine.it/link/2193 e clicchiamo sul pulsante *Aggiungi a Firefox*. Scaricato il Greasemonkey, compare la finestra di installazione: clicchiamo sul tasto *Installa adesso* per installare il plug-in e premiamo *Riavvia adesso* per riavviare il browser.

9 Ecco la tastiera virtuale

Apriamo il sito www.winmagazine.it/link/2194 e clicchiamo *Install* per installare la tastiera virtuale. Nella nuova finestra premiamo *Installa*. Per aprirla basta un doppio clic su un campo di una pagina Web. Per impostare il layout italiano dal menu della tastiera scegliamo *Italiano*.

La mia casa è cablata!

Tutte le soluzioni per condividere ADSL, file, cartelle e stampanti tra i dispositivi della tua rete LAN domestica

Tutti i nuovi dispositivi hi-tech hanno ormai bisogno di una connessione a Internet per funzionare correttamente e aumentare le loro potenzialità. Questo mini corso nasce proprio con l'intento di guidarci passo passo nella realizzazione di una rete locale domestica: vedremo come configurare i vari device in maniera adeguata, risolvendo così problemi dovuti a impostazioni errate o non propriamente indicate. Solo così potremo connetterli a Internet e metterli in comunicazione tra loro. Partiremo con un accenno alla struttura di una tradizionale rete locale, per poi passare ad assegnare ai nostri dispositivi un indirizzo IP statico in modo da mantenere la nostra rete stabile e sicura. I passi successivi illustreranno come trasferire e riprodurre, in streaming, file multimediali tra computer e smartphone Android. Seguendo le dritte dei nostri esperti saremo quindi in grado di connettere tutti i dispositivi multimediali alla rete domestica, permettendoci così di stampare, ascoltare musica e trasferire file da un dispositivo ad un altro senza intoppi.

Ad ognuno il suo indirizzo

Prima di cominciare è bene ricordare che ogni rete LAN è identificata da un indirizzo IP: per poter funzionare correttamente, quindi, ogni dispositivo connesso ad essa deve disporre di un suo indirizzo IP valido e univoco. Senza scendere nel dettaglio, ci basti sapere che, per convenzione, la classica LAN domestica, composta da un modem/router, alcuni smartphone e uno più computer, viene rappresentata dall'indirizzo IP: 192.168.1.0. Dopodiché, ogni dispositivo che accede alla rete può registrarsi usando e occupando un indirizzo IP compreso tra il 192.168.1.1 e il 192.168.1.254. Sulla base di queste informazioni, assegneremo il primo indirizzo disponibile (192.168.1.1) al router, mentre agli altri dispositivi assegneremo un IP crescente 192.168.1.2, 192.168.1.3, 192.168.1.4 e così via. La nostra rete può supportare fino ad un massimo di 254 dispositivi.

RIPOSTIGLIO

ROUTER

TP-LINK ARCHER C9

Grazie allo standard 802.11ac è capace di raggiungere una velocità in wireless 3 volte superiore rispetto al wireless N

Quanto costa: € 149,90

Sito Internet: www.tp-link.it

PARAMETRI DI RETE
Indirizzo IP: 192.168.1.1
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1
DNS: "assegnato dal provider"

PARAMETRI DI RETE
Indirizzo IP: 192.168.1.25
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1
DNS: 192.168.1.1

NAS

SYNOLOGY DISKSTATION DS115

Il suo sistema operativo mette a disposizione applicazioni per configurare un server multimediale, un download manager e tanto altro ancora.

Quanto costa: € 152,50

Sito Internet: www.synology.it

CUCINA

TABLET

GALAXY TAB 3 10.1 3G+WI-FI

Integra un avanzato equalizzatore audio Sound Alive che garantisce bassi più profondi e un suono più pulito.

Quanto costa: € 499,90

Sito Internet: www.samsung.it

PARAMETRI DI RETE
Indirizzo IP: 192.168.1.2
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1
DNS: 192.168.1.1

STUDIO

STAMPANTE MULTIFUNZIONE

HP ENVY 7640
È compatibile con la connessione NFC: basta avvicinare il dispositivo mobile per mandare subito in stampa le foto.
Quanto costa: € 199,90
Sito Internet: www.hp.com/it

PARAMETRI DI RETE
Indirizzo IP: 192.168.1.15
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1
DNS: 192.168.1.1

PARAMETRI DI RETE
Indirizzo IP: 192.168.1.8
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1
DNS: 192.168.1.1

NOTEBOOK

ASUS N551JK-CN034H
Capace di coniugare un design eccellente con un hardware capace di fornire performance elevate con qualsiasi tipo di applicazione.
Quanto costa: € 1.290,00
Sito Internet: www.asus.it

CAMERETTA

SMARTPHONE ANDROID

HTC DESIRE 610
Restituisce un'ottima ergonomia d'uso, che si affianca ad un design accurato e a materiali di buona qualità
Quanto costa: € 299,00
Sito Internet: www.htc.com

PARAMETRI DI RETE
Indirizzo IP: 192.168.1.20
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1
DNS: 192.168.1.1

PARAMETRI DI RETE
Indirizzo IP: 192.168.1.4
Subnet mask: 255.255.255.0

PARAMETRI DI RETE
Indirizzo IP: 192.168.1.5
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1
DNS: 192.168.1.1

SOGGIORNO

SMART TV

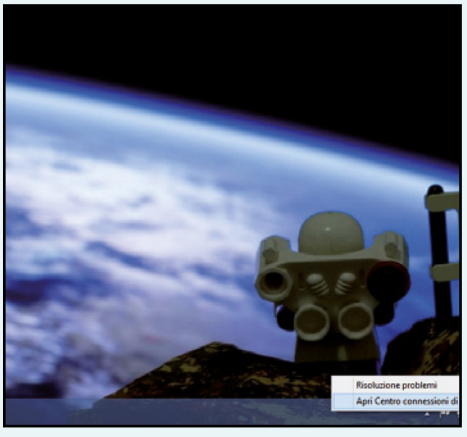
SAMSUNG UE48H6600
Immagine estremamente nitida, una ricca dotazione e una straordinaria scelta di app scaricabili direttamente dallo Store.
Quanto costa: € 699,00
Sito Internet: www.samsung.it

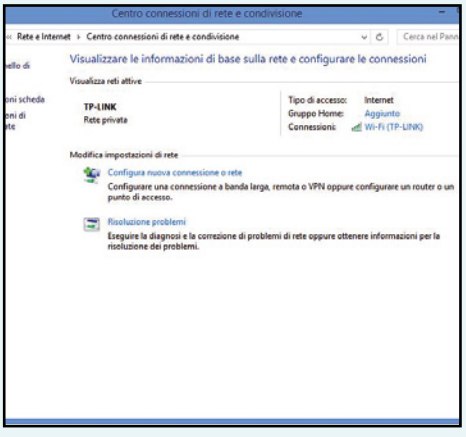
CONSOLE DI GIOCO

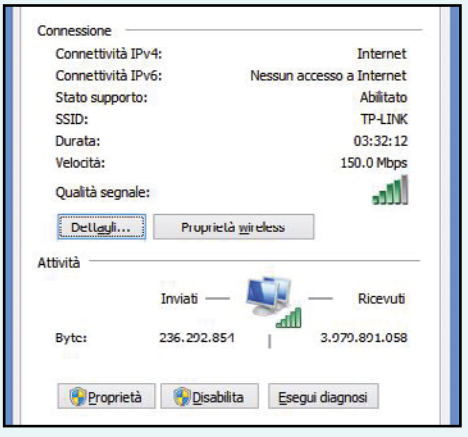
PLAYSTATION 4
Nata per i videogiochi, è dotata di varie funzioni multimediali oltre a quelle di intrattenimento videoludico.
Quanto costa: € 369,99 (con HD da 500GB)
Sito Internet: www.sony.it

Il nostro computer va in rete per

Ecco la procedura da seguire per configurare un indirizzo IP statico ad un computer dotato di sistema operativo Windows. Nel tutorial useremo una connessione Ethernet, ma i passi sono identici anche con il Wi-Fi.







1 Tutto da pannello di controllo

Accediamo al *Centro connessione di rete e condivisione* di Windows: selezioniamo semplicemente con il tasto destro del mouse l'icona della rete (*Ethernet* o *Wi-Fi*) posta sulla barra degli strumenti in basso, di fianco l'orologio di sistema, e clicchiamo sulla voce omonima.

2 Che nome ha la rete?

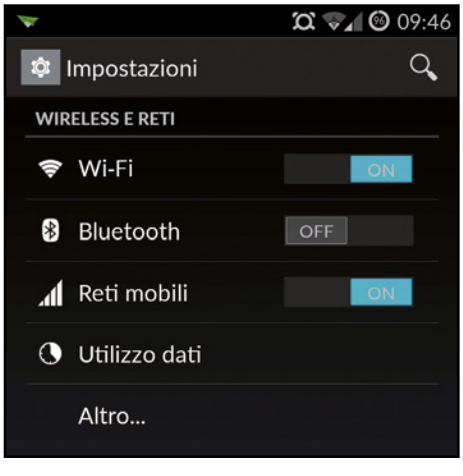
Nel *Centro connessione di rete e condivisione* possiamo visualizzare l'elenco di tutte le connessioni attive: nel nostro esempio, il PC è connesso ad una rete dal nome *(SSID) TP-LINK*. Per accedere alle proprietà, facciamo doppio clic sulla connessione attiva: *Wi-Fi (TP-LINK)*.

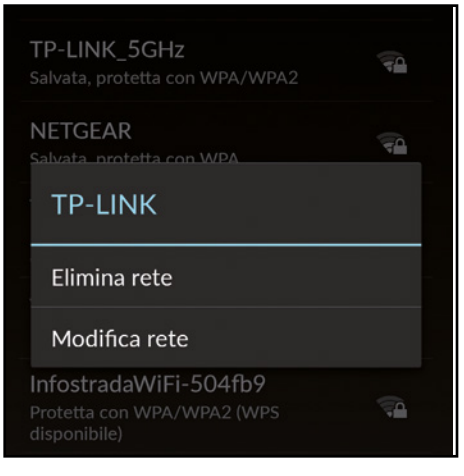
3 Connessione in buono stato

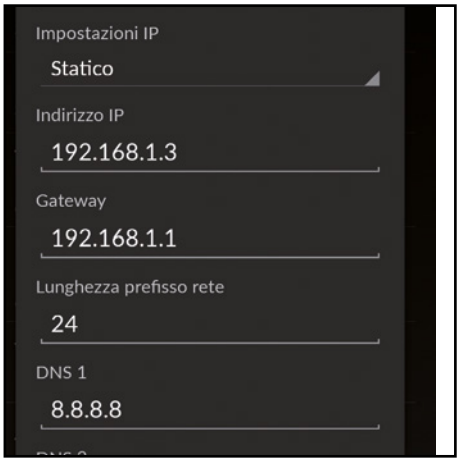
Nella schermata di riepilogo vengono visualizzate le informazioni utili a valutare lo stato di salute della rete: la velocità e la qualità della connessione, la quantità di byte trasferiti e altri valori. Clicchiamo sul pulsante *Proprietà* per accedere alle impostazioni avanzate.

Anche Android è connesso

Analogamente a quanto visto sui computer con sistema operativo Windows, impareremo ora a configurare anche gli smartphone e i tablet dotati del sistema operativo di Google. Pochi tocchi e saremo in rete!







1 Le giuste impostazioni

Dal menu *Applicazioni/Impostazioni* attiviamo la voce *Wi-Fi* e connettiamoci alla LAN. Ci verrà chiesto di inserire la chiave *WPA/WPA2*: digitiamo quella predefinita da 16 cifre del router (indicata sul manuale d'uso) o, se l'abbiamo modificata, quella scelta da noi.

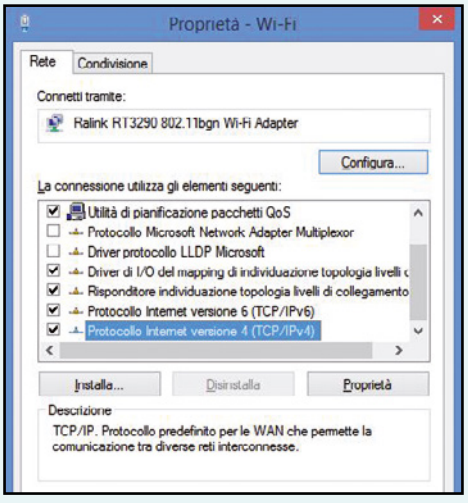
2 I parametri della nostra rete

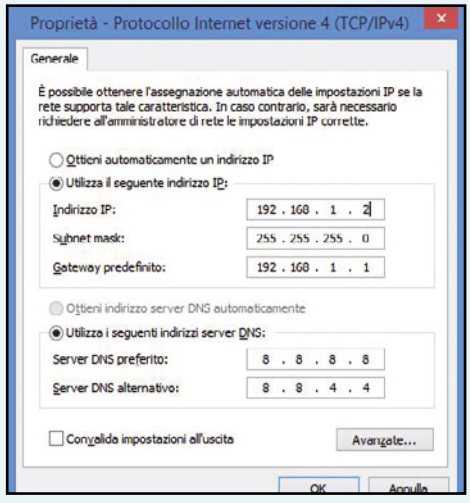
Torniamo alla lista delle reti Wi-Fi disponibili, tocchiamo e teniamo premuto il dito sul nome della nostra rete: nella nuova schermata che appare scegliamo la voce *Modifica rete*, per accedere alle proprietà della connessione e impostare i corretti parametri di rete.

3 L'IP per lo smartphone

Spuntiamo *Mostra opzioni avanzate* e assegniamo *Statico* a *Impostazioni IP*. Usiamo il solito schema di indirizzamento assegnando il primo IP disponibile: *192.168.1.3*, *192.168.1.1* al *Gateway* e lasciamo la lunghezza del prefisso a *24*. Come *DNS* usiamo *8.8.8.8* e *8.8.4.4*.

condividere musica, foto e video





4 Impostiamo i parametri di rete

Scorriamo l'elenco La connessione utilizza gli elementi seguenti, selezioniamo *Protocollo Internet versione 4 (TCP/IPv4)* e clicchiamo *Proprietà*. Gli utenti più smanettoni possono modificare (se la configurazione di rete lo supporta) anche il nuovo Protocollo Internet versione 6.

5 DHCP? No, grazie!

Assegniamo *192.168.1.2* come *Indirizzo IP* al primo computer, *192.168.1.3* al secondo e così via. L'IP è l'unico valore che varia a seconda del device, gli altri parametri, come *Gateway (192.168.1.1)*, *Subnet Mask (255.255.255.0)* e *Server DNS (8.8.8.8 e 8.8.4.4)* restano invariati.

6 E se abbiamo Windows XP?

Apriamo il *Pannello di controllo*, clicchiamo su *Connessioni di rete* e poi sull'icona della rete da modificare: scegliamo *Proprietà* e selezioniamo *Protocollo internet (TCP/IP)*, clicchiamo *Utilizza il seguente indirizzo IP* e impostiamo i parametri come visto nei passi precedenti.

In rete anche con iPhone e iPad

Anche gli smartphone e i tablet della Apple dotati di sistema operativo iOS devono essere correttamente configurati per poterli connettere alla nostra rete LAN. Ecco la semplice procedura da seguire.

1 Impostiamo il Wi-Fi

A prescindere dalla versione di iOS installata, inserire un indirizzo IP statico è un'operazione semplicissima. Ci basterà dirigerci nelle *Impostazioni di sistema* e cliccare sulla voce *Wi-Fi*. Assicuriamoci che il dispositivo sia abilitato e che la connessione con la nostra rete sia attiva.

2 Una Mela con l'IP statico

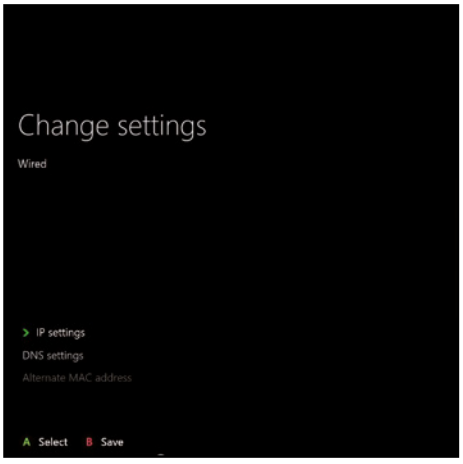
Ricerchiamo la nostra rete e tocchiamo l'icona *Informazioni* che compare a destra del nome della rete. Nei tab *DHCP*, *BootIp* e *Statico* assicuriamoci che sia attivo il pulsante *Statico*: modifichiamo l'indirizzo IP e gli altri valori manualmente inserendo i valori nei campi che compaiono sotto.

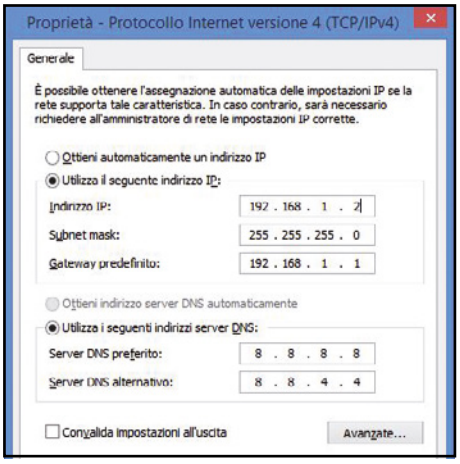
3 iPhone e iPad sono connessi

Usiamo il solito schema di indirizzamento, assegnando all'Apple device il primo indirizzo IP disponibile della nostra rete (*192.168.1.4.*). Alla voce *Subnet Mask* digitiamo *255.255.255.0*. In *iOS*, la voce *Gateway* non compare, ma troviamo *router*: digitiamo *192.168.1.1*. Come *DNS* usiamo *8.8.8.8*.

La console di gioco è on-line

Quasi tutti i nuovi titoli hanno la modalità di gaming on-line che permette di sfidare gli amici via Internet o scaricare contenuti extra. È indispensabile, quindi, che anche PlayStation e Xbox siano connesse in rete.





1 Iniziamo con la Xbox One

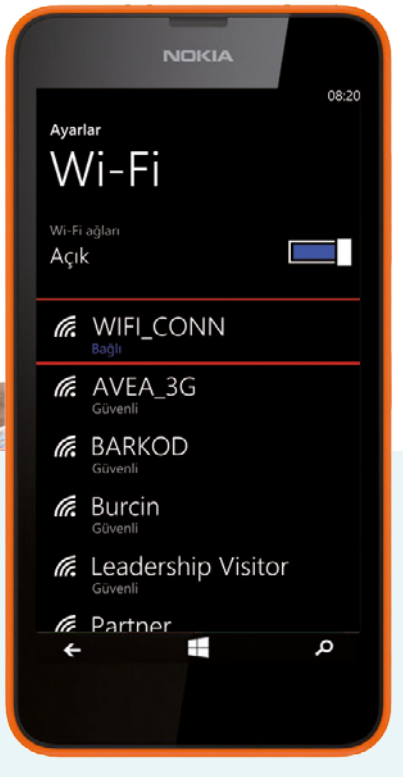
Come già detto anche le console utilizzano un sistema di indirizzamento IP, pertanto è opportuno che anche queste periferiche vengano configurate al meglio. In *Impostazioni/Rete* sono presenti le opzioni di configurazione avanzate. Clicchiamo su *Impostazioni IP* e poi clicchiamo su *Manuale*.

2 I parametri della PlayStation 4

Dalle *Impostazioni di sistema* spostiamoci in *Rete*: premiamo il tasto *X* del gamepad su *Imposta Connessione Internet*. Selezioniamo *Usa Wi-Fi* o *Usa un cavo di rete LAN*. Dalla lista delle reti presenti selezioniamo la nostra e nelle impostazioni dell'indirizzo IP selezioniamo *Manuale*.

3 Ad ognuna il suo IP

Inseriamo un indirizzo IP differente da quelli già usati per gli altri dispositivi: ad esempio *192.168.1.5*. In *Maschera di sottorete* digitiamo *255.255.255.0*. Come gateway predefinito inseriamo l'IP del modem, *192.168.1.1*. Come *Server DNS* primario utilizziamo quello di Google: *8.8.8.8*.



SU WINDOWS PHONE NON SERVE L'INDIRIZZO IP STATICO

Ad oggi non è possibile inserire un indirizzo IP statico, sugli smartphone Windows Phone. Microsoft ha annunciato un update per risolvere tale inconveniente. Comunque, anche se non è possibile modificare manualmente tale parametro, la connettività funzionerà ugualmente: si potrebbero avere alcune limitazioni nell'utilizzo dei servizi. E' possibile assegnare un indirizzo IP anche ad altri dispositivi, come stampanti, NAS, videoproiettori, insomma ogni dispositivo in grado di connettersi alla rete, necessita di un indirizzo IP opportuno.

ABBONATI A
WIN MAGAZINE

Collegati all'indirizzo http://abbonamenti.edmaster.it/winmagazine
e scopri le nostre offerte di abbonamento

Condividiamo i dati in LAN

Ecco come creare una cartella condivisa sul PC accessibile via rete dal nostro smartphone o dal tablet Android

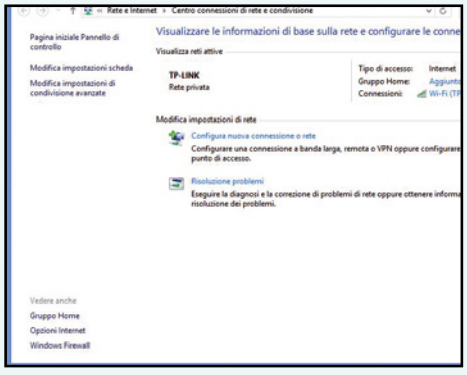
Nelle pagine precedenti abbiamo visto come cablare casa per creare una rete locale a cui connettere tutti i nostri dispositivi tecnologici e condividere la connessione a Internet. Configurati i parametri necessari siamo ora pronti a metterli in comunicazione tra loro: così facendo, potremo scambiare facilmente qualsiasi tipo di file. Il segreto è tutto nelle cartelle condivise che andremo a creare sul computer e che saranno accessibili, oltre che dagli altri PC della rete, anche mediante apposite app per smartphone e tablet che funzionano a tutti gli effetti come l'Esplora risorse di Windows.

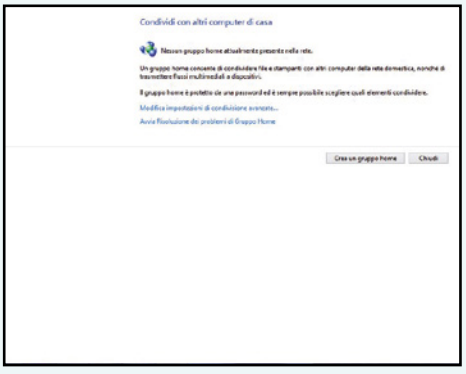
E parametri giusti di rete da configurare

Per configurare correttamente un dispositivo e connetterlo alla LAN di casa è necessario indicare, oltre all'indirizzo IP (come indicato nella prima parte del corso), altri parametri di rete come la Subnet Mask, il Gateway e il server DNS. La prima serve a definire la "dimensione" della rete (indica, cioè, il numero di dispositivi che possono essere connessi) e generalmente avrà valore **255.255.255.0**. Il Gateway, invece, è l'indirizzo IP del dispositivo che fornisce l'accesso a Internet: sarà quindi l'IP del router. Il server DNS, infine, è un computer remoto in grado di "localizzare" fisicamente i siti Internet. Possiamo eventualmente usare i DNS di Google (**8.8.8.8** come DNS primario e **8.8.4.4** come DNS secondario). Per impostare questi parametri, accediamo al **Pannello di controllo/Rete e Internet/Centro connessione di rete e condivisione e selezioniamo la rete LAN**. Clicchiamo **Proprietà**, selezioniamo **Protocollo Internet versione 4** (TCP/IPv4) e clicchiamo ancora **Proprietà**. Non perdiamo altro tempo e scopriamo assieme come condividere in rete tutti i nostri file.

Scegliamo le cartelle sul PC

Dopo aver messo in rete il computer, possiamo creare e configurare il Gruppo Home: con pochi clic potremo così condividere in rete i nostri file e renderli accessibili anche dal nostro smartphone o dal tablet Android.





1 Creiamo un gruppo di rete

Su Windows possiamo configurare il *Gruppo Home* per condividere facilmente in rete i file contenuti nelle cartelle *Immagini, Musica, Video* e *Documenti* o qualsiasi altra noi desideriamo. Accediamo al *Centro connessione di rete e condivisione* e clicchiamo *Gruppo Home* in basso a sinistra.

2 Quali cartelle condividere?

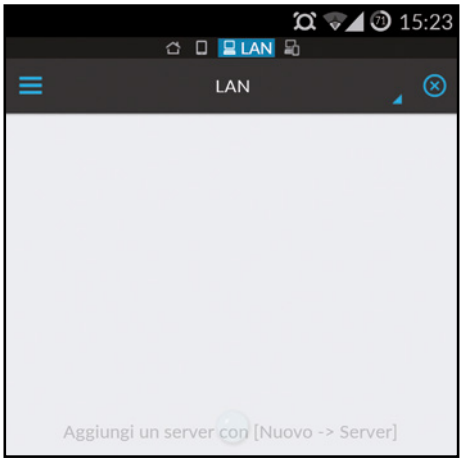
Nella schermata che appare clicchiamo *Crea un Gruppo Home*. Verrà aperta una nuova finestra dalla quale dovremo scegliere le cartelle predefinite che vogliamo condividere in rete, concedendo le varie *Autorizzazioni*: attiviamo solo quelle su cui vogliamo garantirci l'accesso da Android.

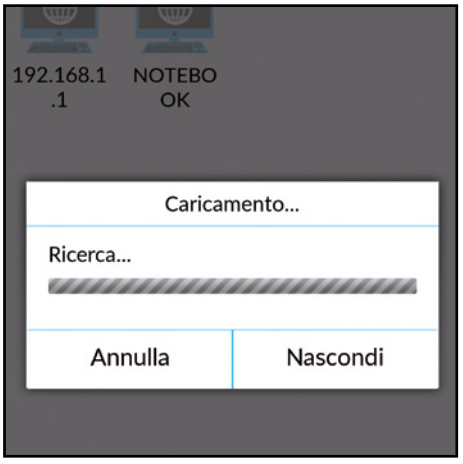
3 La chiave giusta per entrare nel gruppo

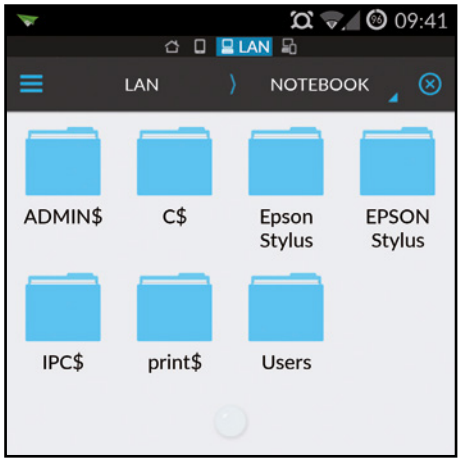
Verrà generata una password alfanumerica che useremo per connettere automaticamente altri dispositivi Windows al gruppo. Annotiamoci o stampiamo la password e clicchiamo *Fine*: anche se per la condivisione con Android non lo useremo, ci tornerà utile per connettere altri PC alla rete.

Da Android a Windows…

Create le cartelle condivise sul nostro computer, possiamo adesso configurare lo smartphone e il tablet per accedere da remoto ai contenuti. Per farlo, useremo un'app gratuita. Ecco come usarla al meglio.







1 File e cartelle su Android

Dallo smartphone possiamo accedere alle cartelle condivise installando un file manager come *ES Gestore File*. Avviamola e dal menu *Rete* selezioniamo *LAN*. La schermata risulterà vuota: per visualizzare i dispositivi clicchiamo *Scansiona* per avviarne la ricerca all'interno della rete.

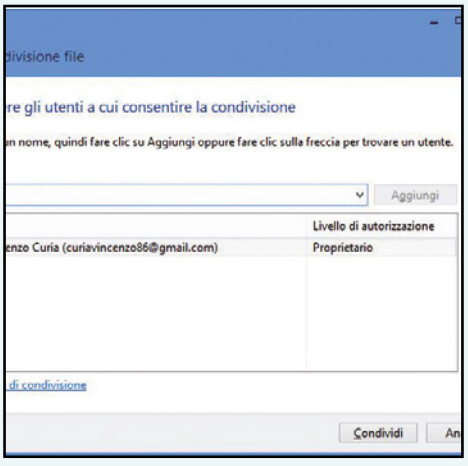
2 Connettiamoci al PC

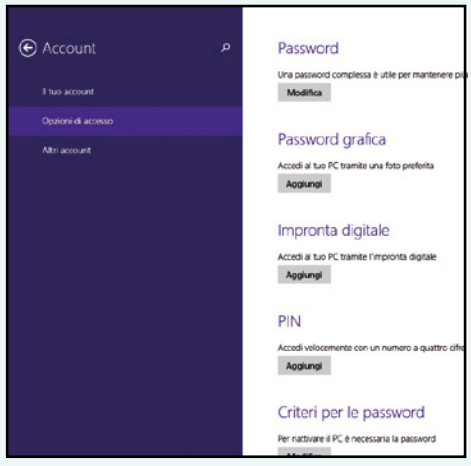
Dalla lista dei dispositivi scegliamo il nostro computer (identificabile tramite il nome di rete o tramite l'IP assegnato in precedenza). Ci verrà chiesto di inserire nome utente e password di Windows. Immettiamo i dati ricavati nel Macropasso precedente, salviamo e clicchiamo *OK*.

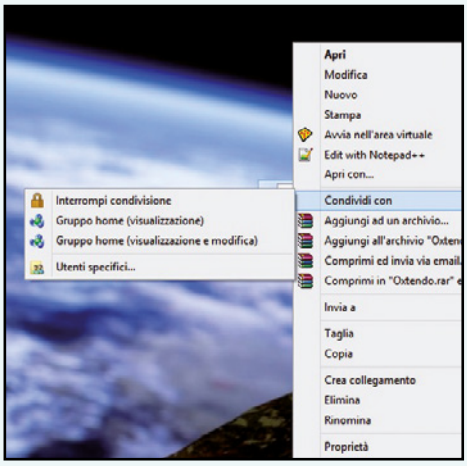
3 Sfogliamo le cartelle

Se abbiamo fatto tutto correttamente, avremo accesso alle cartelle condivise sul gruppo Home. Saremo pertanto in grado non solo di modificare e trasferire file, ma anche riprodurre in streaming i contenuti multimediali come video e musica, direttamente sul display dello smartphone.

che vogliamo condividere







4 Creiamo un account utente

Possiamo procedere con la condivisione delle cartelle. Selezioniamo quella che ci interessa col tasto destro del mouse e scegliamo *Condividi con/Utenti specifici* dal menu contestuale. Digitiamo un nome utente nel campo di testo in alto e clicchiamo *Aggiungi*. Confermiamo con *Condividi*.

5 Proteggiamo la condivisione

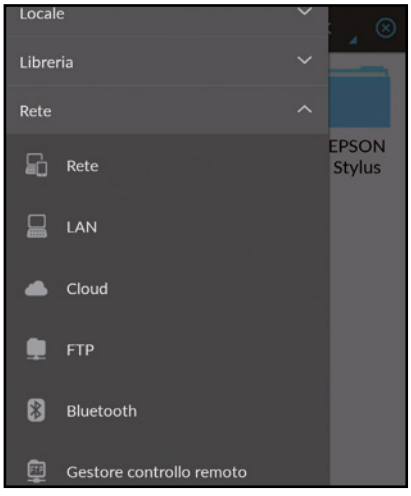
La password di accesso è obbligatoria per condividere file in rete. Se non abbiamo impostato una password di accesso a Windows, facciamolo adesso. Da *Pannello di controllo/Account Utente*, selezioniamo il nostro utente e clicchiamo *Cambia Password* o *Modifica* (se abbiamo Windows 8/8.1).

6 Altri file e cartelle

Abbiamo creato il gruppo Home e condiviso correttamente le cartelle predefinite *Musica, Immagini* e *Video*. Per aggiungere alla condivisione altre cartelle, clicchiamo con il tasto destro del mouse su una cartella o un file da condividere e scegliamo la voce *Condividi con/gruppo Home*.

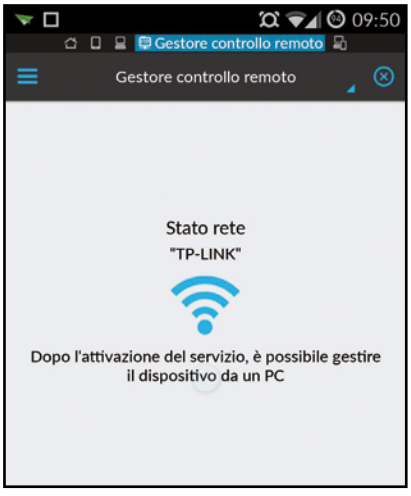
...e da Windows ad Android!

Grazie ad ES Gestore File possiamo configurare sullo smartphone un mini server FTP per consentire di accedere da remoto anche ai contenuti archiviati nella memoria interna dello smartphone.



1 Un server FTP su Android

Abbiamo avuto accesso ai file del computer: e se volessimo realizzare il processo inverso, ovvero accedere ai file dello smartphone dal PC? Dobbiamo abilitare la funzionalità di *Server FTP* sul dispositivo Android. Dal *Menu* dell'app ES Gestore File clicchiamo *Gestione controllo remoto*.



2 L'accesso si fa da remoto

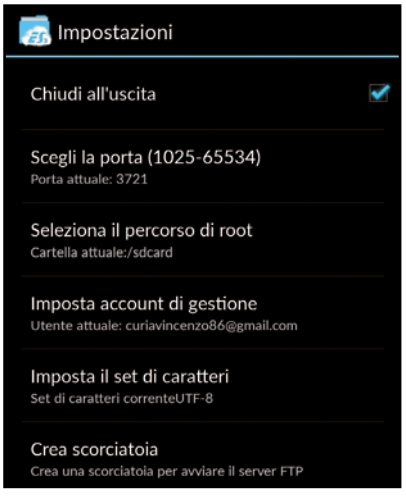
Si aprirà una nuova schermate. A confermare la correttezza della procedura, dovremmo visualizzare un avviso che ci ricorda che, dopo l'attivazione del servizio, saremo in grado di controllare il nostro smartphone dal PC. Clicchiamo quindi su *Inizia* per avviare il server FTP su Android.

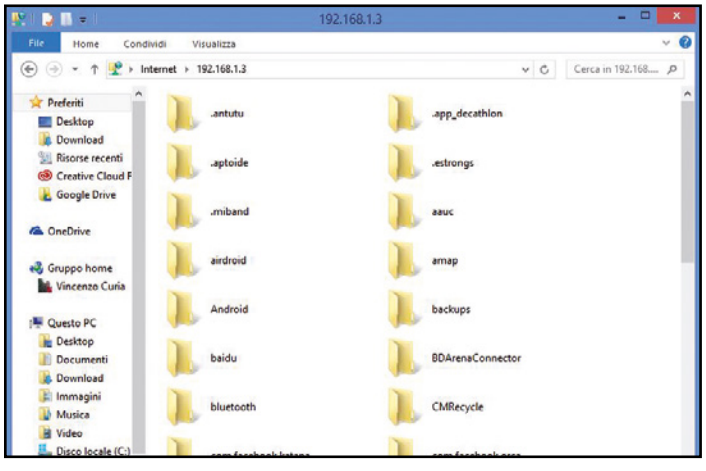
3 L'indirizzo dello smartphone

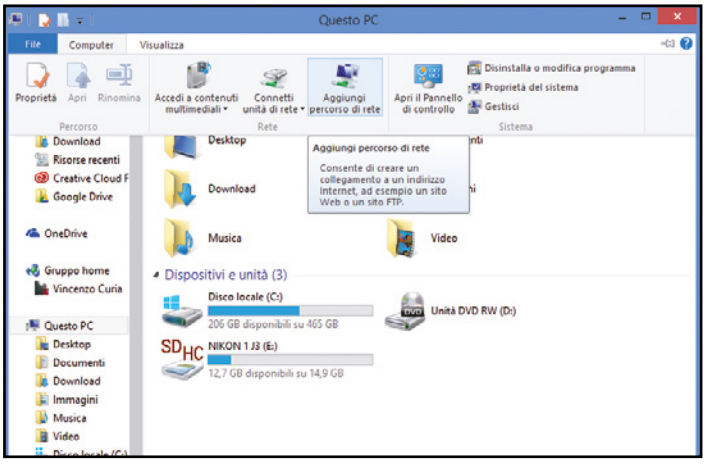
Verrà generato un indirizzo FTP tramite il quale saremo in grado di visualizzare la memoria dello smartphone da qualsiasi browser. Copiamo (*Ctrl+C*) il link per intero: ci servirà per accedere alla memoria dello smartphone. Android utilizza un server SMB per la gestione del servizio FTP.

4 Una scorciatoia per Android

Conviene creare un collegamento rapido direttamente dalla home screen di Android per accendere e spegnere il server FTP senza dover ogni volta avviare ES Gestore File. Basta cliccare in basso su *Impostazioni*, poi su *Crea scorciatoia*. È anche possibile impostare una password di accesso.







5 Computer chiama smartphone

Spostiamoci sul PC, avviamo *Esplora risorse* e nella barra indirizzi digitiamo (*Ctrl+V*) quello del server FTP Android. Verrà mostrata la memoria interna dello smartphone e la micro SD (se presente). A questo punto, possiamo trasferire file come faremmo con una qualsiasi chiavetta USB.

6 Da Windows basta un clic

Per evitare di digitare ogni volta l'indirizzo del server FTP Android, da *Risorse del computer* selezioniamo *Computer* col tasto destro del mouse e clicchiamo *Aggiungi percorso di rete*. Seguiamo quindi la procedura guidata per creare una scorciatoia per l'accesso diretto al server FTP.

Una stampante mille computer

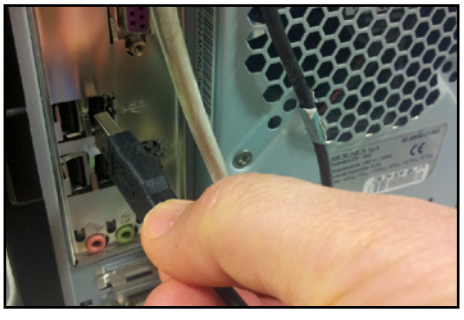
Ecco come condividere la periferica per stampare da qualsiasi PC o smartphone connesso in rete domestica

Dopo aver ultimato la configurazione di base della nostra rete, ed aver abilitato lo scambio di file tra i vari dispositivi che la compongono, vediamo come è possibile utilizzare un'unica stampante e condividerla, rendendola così disponibile per la stampa remota a tutti gli altri dispositivi connessi alla stessa rete. Questo tipo di condivisione può essere realizzato a prescindere dal tipo di stampante utilizzata e dalla tecnologia di stampa, supporta infatti tutti i modelli, basta che la stampante sia collegata ed installata su un computer che svolge la funzione di server. In questo modo, tutti gli utenti della stessa rete, con cui si decide di condividere la stampante potranno utilizzarla proprio come se fosse collegata fisicamente.

BUONI CONSIGLI

SE IL PC NON VEDE LA STAMPANTE

Dal Pannello di controllo del nostro PC clicchiamo su Rete e Internet e poi su Centro connessioni di rete e condivisione. Da *Modifica impostazioni di condivisione avanzate* spuntiamo la voce *Attiva condivisione file e stampanti* presente nelle sezioni *Domestico* (o *Privato*) e *Guest* (o *Pubblico*). Quindi salviamo le modifiche.



1 Si parte con le connessioni

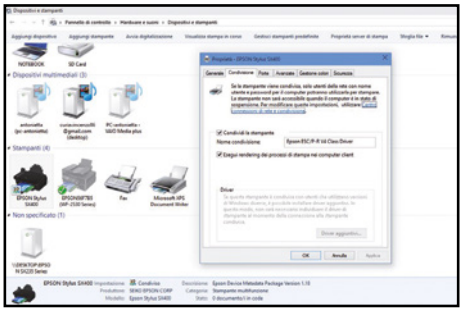
Colleghiamo la stampante al computer principale (che svolge la funzione di server) tramite porta USB, nel nostro caso, abbiamo utilizzato il PC installato nello studio (ambiente ideale per posizionare la stampante). Non accendiamo la periferica!

2 Scegliamo il driver giusto

Inseriamo il CD/DVD di installazione del driver fornito a corredo della stampante. Se non siamo in possesso del disco, colleghiamoci al sito del produttore e nella sezione download o supporto, scarichiamo il driver più recente compatibile con il nostro modello.

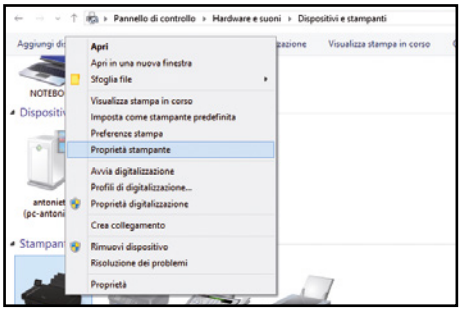
3 Accendiamo la stampante quando richiesto

Avviamo il setup del programma seguendo le istruzioni a video. Accendiamo la stampante quando richiesto e attendiamo l'installazione dei driver di stampa e del software di gestione del dispositivo.



4 Dispositivi e stampanti

Rechiamoci nel pannello di controllo di Windows (*Start/Impostazioni/Pannello di Controllo*) e clicchiamo sulla voce *Visualizza dispositivi e stampanti*. Clicchiamo con il tasto destro sulla stampante appena installata e scegliamo la voce *Proprietà Stampante*.



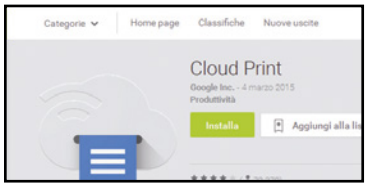
5 È il momento di condividere

Dalla nuova finestra, spostiamoci nel tab *Condivisione*, quindi spuntiamo la voce *Condividi la stampante*. Digitiamo nel campo *Nome condivisione* il nome che da assegnare alla stampante e clicchiamo prima su *Applica* e poi su *OK* per salvare le modifiche.

6 Stampa da remoto

Per avviare una stampa da un PC della LAN, occorre che sia la stampante che il "server" siano accesi. Spostiamoci sul secondo computer, apriamo un documento ed avviamo la fase di stampa, selezionando come dispositivo di stampa la nostra stampante remota.

LE TOP APP PER STAMPARE DIRETTAMENTE DA SMARTPHONE

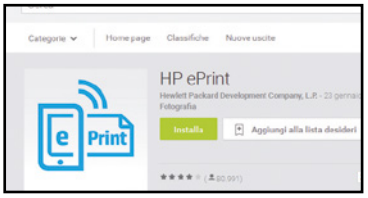


CLOUD PRINT

L'app made in Google che permette di utilizzare l'omonimo servizio. Dopo aver registrato la stampante possiamo usare l'app per avviare la stampa da qualsiasi dispositivo in nostro possesso.

PRINTERSHARE

Consente di stampare sfruttando diverse tipologie di collegamento, come il Wi-Fi Direct, il Bluetooth o la classica USB. Compatibile con il servizio Google Cloud Print. Costa €13,95.



HP EPRINT

Supporta ogni stampante con connessione di rete, anche i modelli meno recenti. Permette la stampa gratuita delle postazioni di stampa pubbliche HP sparse in tutto il mondo.

BREEZY PRINT AND FAX

Per completare il collegamento PC-Smartphone, bisogna prima installare un programma sul computer e poi l'app su Android. Permette anche di inviare Fax.

PRINTHAND MOBILE PRINT

Stampa di tutto e da qualunque posizione, cloud storage compreso, e persino tramite USB con Android 4.0. Costa € 9,35.

IO STAMPO CON LA TECNOLOGIA NFC

La tecnologia senza fili NFC (Near Field Communication) permette lo scambio di informazioni senza fili tra due dispositivi che si trovano a brevissima distanza tra loro. Con stampanti che supportano l'NFC, è quindi possibile stampare i propri documenti, avvicinando lo smartphone alla stampante. A differenza della classica connessione Wi-Fi, la stampa tramite NFC è estremamente semplice: non sono previste password o particolari configurazioni della connessione. Per stampare basterà solo installare l'app del produttore, selezionare il file da stampare ed avvicinare lo smartphone alla stampante.

Il nostro NAS finisce in rete

La guida per condividere i nostri contenuti multimediali tra i computer della LAN e avviarne la riproduzione in streaming

Abbiamo ormai ultimato la configurazione di tutti i dispositivi delle nostra rete domestica, ma per quanto possa apparirci completa (visto che è composta da più dispositivi come PC, console, smartphone e tablet), manca ancora qualcosa: un dispositivo in grado di archiviare tutti i nostri file, i film, la musica e le immagini. Insomma, un centro multimediale al quale poter accedere da PC, tablet, smartphone, ecc. I Network Attached Storage, noti anche come NAS, sono dispositivi in grado di condividere in rete il contenuto salvato su uno o più degli hard disk contenuti al suo interno. Per questo motivo il NAS è il candidato ideale a ricoprire questo ruolo perché è in grado di svolgere la funzionalità di multimedia center, permettendo così di immagazzinare, catalogare e servire una mole di dati mostruosa.

Il tuttofare della LAN

Per funzionare correttamente e gestire le richieste inviate dagli altri dispositivi connessi in rete, i NAS sono dotati di un sistema operativo proprietario che permette di ampliarne ulteriormente le potenzialità, permettendo ad esempio di installare applicazioni appositamente sviluppate. Con l'app giusta si può abilitare nel NAS una vera e propria download station, per scaricare file dai siti di file sharing (così come faremmo con software tipo JDownloader), o direttamente dalla rete Torrent. Ma non finisce qua: il NAS, infatti, supporta anche schede Tuner TV per godere dei contenuti televisivi in streaming, permettendo registrazione e riproduzione delle dirette televisive. Collegando una IPCam compatibile, infine, il NAS si trasforma anche in un DVR sul quale riversare o riprodurre diverse ore di registrazioni, permettendo di gestire anche la sicurezza di casa. In questa terza parte del corso sulle reti LAN vedremo proprio come installare e configurare correttamente un NAS e come accedere ai contenuti multimediali salvati nelle varie cartelle del dispositivo.

I DISPOSITIVI DI RETE IN GRADO DI SODDISFARE OGNI ESIGENZA

SYNOLOGY DS115J

Compatto, leggero e dai consumi ottimizzati, DS115j è perfetto per utenti domestici in cerca di un server NAS semplice ed economico. È possibile eseguire in modo rapido il backup dei documenti, monitorare impianti di sorveglianza o creare un cloud personale per la condivisione dei file con amici e familiari.

- **Quanto costa:** € 92,11
- **Sito Internet:** www.synology.com

SYNOLOGY DS415PLAY

È un NAS dotato di 4 bay. Si colloca nella fascia dei top di gamma, supporta lo streaming e la codifica di video in qualità Full-HD a 1080p in maniera fluida su dispositivi come Smart TV o smartphone. Supporta la trasmissione multicanale che consente che consente ai membri della famiglia di vedere i film in diverse stanze.

- **Quanto costa:** € 445,30
- **Sito Internet:** www.synology.com

SYNOLOGY DS214

Studiato per gruppi di lavoro e uffici, il DS214 è un server NAS a 2 vani ricco di funzioni. Grazie alle applicazioni per ufficio complete, consente di condividere e proteggere i dati in modo efficace, aumentando allo stesso tempo la produttività.

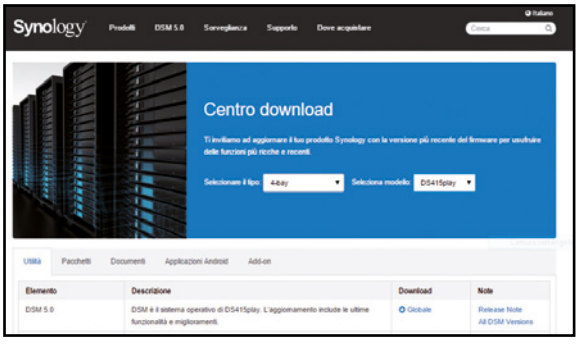
- **Quanto costa:** € 256,20
- **Sito Internet:** www.synology.com

Installiamo il centro multimediale

Inseriamo i dischi negli slot, colleghiamo i cavi di rete, quelli di alimentazione e avviamo il setup del sistema operativo. In poco tempo riusciremo a configurare il nostro NAS Synology DS415 PLAY.

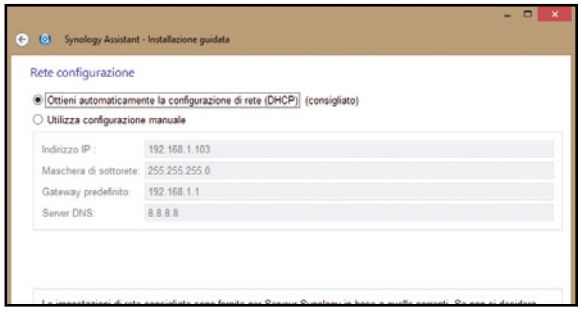
1 La prima accensione

Il NAS viene venduto senza hard disk, pertanto la prima cosa da fare è installarli. Per farlo dobbiamo estrarre i singoli bay dal NAS e fissare ad ognuno di essi l'unità, quindi reinserire la slitta nell'alloggiamento. Colleghiamo poi il cavo Ethernet, l'alimentazione e accendiamo il NAS.



2 Scarichiamo il sistema operativo

Per installare l'ultima versione disponibile del Disk Station Manager, scarichiamo il file *.pat* da www.winmagazine.it/link/3070 dopo aver specificato marca e modello del nostro NAS. Per installarlo, scarichiamo anche il Synology Assistant, che ci guiderà nell'installazione del DSM.



3 Una semplice installazione

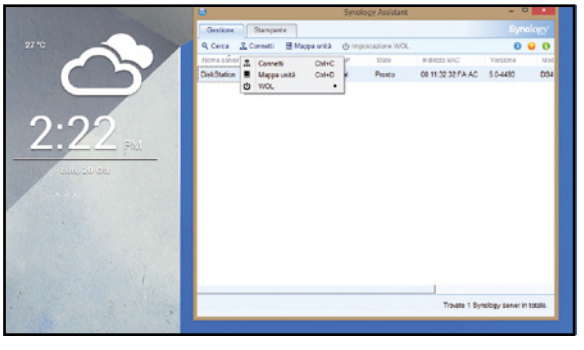
Installare il DSM è semplice come installare un qualsiasi software: avviamo Synology Assistant e attendiamo la scansione dei NAS disponibili nella LAN. Selezioniamo il NAS e seguiamo le istruzioni mostrate a video. Per i parametri di rete, impostiamo l'indirizzamento IP tramite DHCP.

4 Meglio il RAID 0 o 1?

Durante l'installazione del DSM Synology dobbiamo decidere come utilizzare i nostri hard disk, se in RAID *0* o *1*. Se abbiamo dati sensibili da archiviare e tutelare, scegliamo di creare un volume *Synology Hybrid RAID*. Nel caso in cui abbiamo necessità di spazio scegliamo, invece, *RAID 0*.

5 Un account per l'accesso

Ad installazione ultimata, avviamo la connessione al NAS. Si aprirà il browser Web alla schermata di autenticazione: inseriamo admin come username, mentre come password inseriamo la parola chiave scelta al passo precedente. Quindi completiamo la registrazione di un nuovo utente MyDS.



6 Accesso al dispositivo

Ogni volta che abbiamo necessità di accedere al pennello di controllo del nostro NAS, ci basterà avviare il browser Web sul computer e collegarci all'indirizzo http://find.synology.com. Il Web Assistant troverà automaticamente il NAS. Clicchiamo *Connetti* e inseriamo username e password.

BUONI CONSIGLI

ACCESSO ANCHE DALL'ESTERNO

Se abbiamo bisogno di accedere al NAS anche quando ci troviamo lontano da casa, non dovremo far altro che aprire il browser da un qualsiasi computer connesso a Internet, collegarci a http://myds.synology.com e cliccare *Sign up* per registrare un account sul *MyDS Center*. Effettuato poi il login con i nostri dati, ci troveremo davanti la schermata relativa ai NAS installati: clicchiamo sull'ID relativo al nostro NAS per accedere al dispositivo stesso. In alternativa, possiamo registrare un DynDNS, ad esempio su NoIP (www.noip.com) e poi digitare nel browser l'indirizzo associato al nostro NAS.

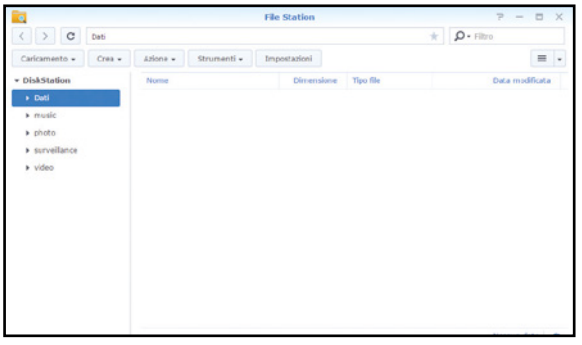
Carichiamo film, foto e musica

Ora che il nostro NAS e configurato e funzionante, possiamo trasferire tutti i nostri contenuti multimediali dal computer ai suoi hard disk del NAS, in modo da renderli accessibili da ogni periferica presente nella rete LAN.

BUONI CONSIGLI

HARD DISK SPECIFICI PER I NAS

I NAS supportano tutti i modelli di disco rigido presenti in commercio, ma conviene comunque acquistare HDD appositamente progettati, come il Western Digital WD60EFRX. Questi hard disk, infatti, hanno una durata media garantita nettamente superiore rispetto a quella dei normali dischi rigidi. Offrono inoltre prestazioni e affidabilità più elevate, riducendo, allo stesso tempo, il rumore prodotto ed i consumi energetici.

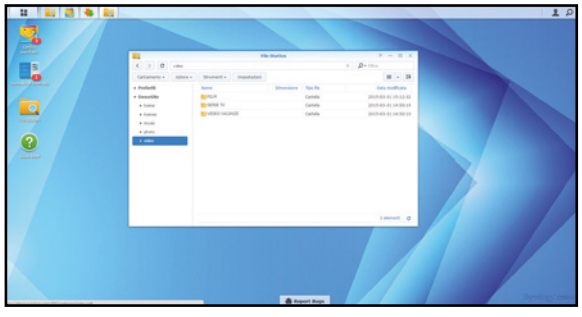


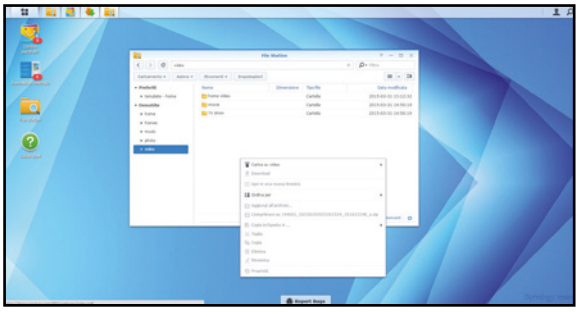
1 Un file manager ad hoc

Connettiamoci tramite browser Web al pannello di controllo del nostro dispositivo utilizzando le credenziali per l'accesso (**Passo A5**). Nella schermata principale clicchiamo sull'icona del menu principale posizionata nell'angolo in alto a sinistra, quindi avviamo l'applicazione *File Station*.

2 Creiamo le cartelle

Se è la prima volta che utilizziamo il nostro dispositivo, potrebbe essere necessario creare le cartelle nelle quali andremo a caricare i vari file. Dalla barra degli strumenti clicchiamo sul pulsante *Crea cartella*. Creiamo quindi le cartelle *Video*, *Musica*, *Immagini* e *Documenti*.



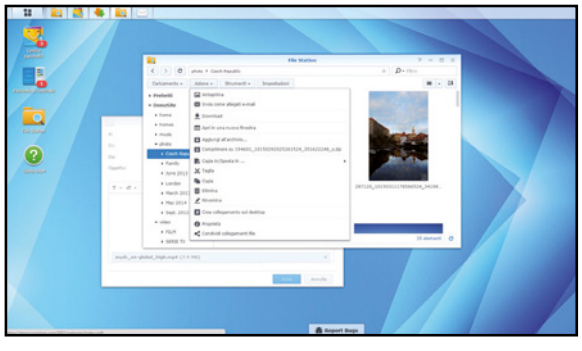


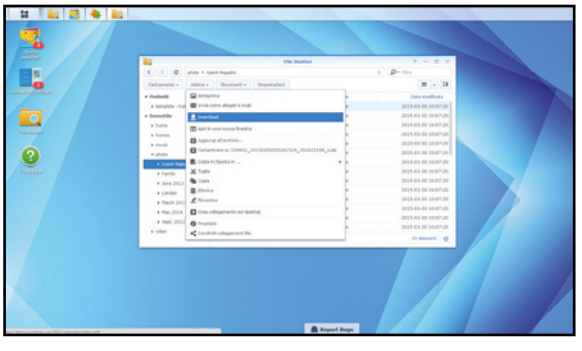
3 Una videoteca ordinata

Per mantenere i nostri file ordinati, creiamo sottocartelle nelle directory principali. Rechiamoci nella cartella *Video* e creiamo le directory in base ai contenuti da trasferire sul NAS. Creiamo quindi una cartella per le *Serie TV*, una per i *Film*, una per i video dei nostri viaggi ecc.

4 Upload di un file

Per trasferire i nostri file sul NAS, posizioniamoci nella cartella di destinazione corretta: ad esempio, se dobbiamo caricare un film assicuriamoci di essere nella cartella *Video\Film*. Clicchiamo su *Caricamento* posizionato nel menu in alto, selezioniamo il file da caricare e clicchiamo *OK*.





5 Modifiche sui file

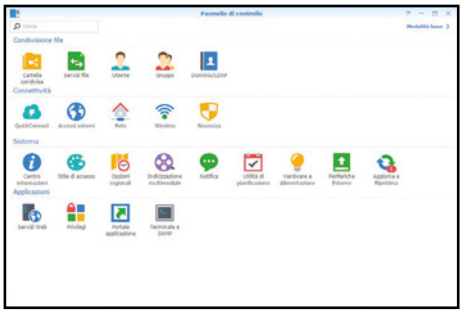
File Station offre la possibilità di effettuare semplici operazioni di modifica sui file. Possiamo rinominare un file, spostarlo o estrarre/comprimere un archivio. Se ne abbiamo bisogno, clicchiamo sulla voce *Azioni* del menu principale e scegliamo lo strumento di modifica opportuno.

6 Scarichiamo file sul PC

Il file manager del Synology permette anche di scaricare i file archiviati nei suoi hard disk sui computer della rete LAN. Per effettuare questa operazione, sfogliamo le directory tramite *File station*, scegliamo il file da salvare, quindi clicchiamo *Azione* e scegliamo la voce *Download*.

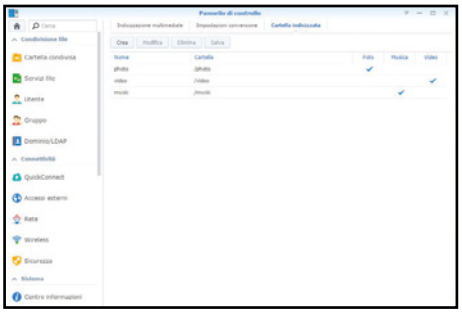
Download e riproduzione dei file

Configurato correttamente il NAS e riempiti i suoi dischi con tutti i nostri contenuti multimediali preferiti, possiamo ora imparare a scaricare i singoli file dalla rete e avviarne la riproduzione da qualsiasi dispositivo.



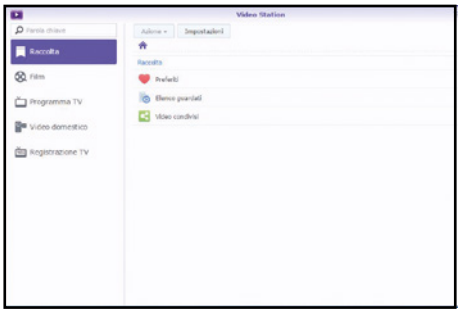
1 Cartelle da indicizzare

Dobbiamo innanzitutto consentire al nostro NAS di indicizzare e catalogare tutti i file multimediali archiviati. Colleghiamoci all'unità e dalla schermata principale avviamo il pannello di controllo: scegliamo quindi la voce Indicizzazione multimediale presente nella sezione *Sistema*.



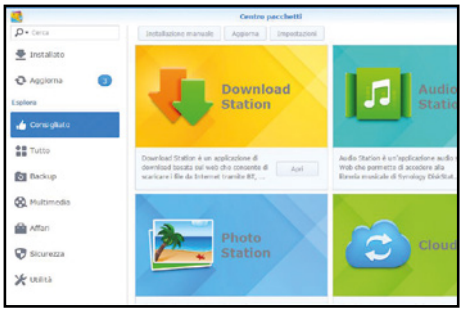
2 Una directory per ogni file

In *Cartella condivisa* verifichiamo che compaiano le directory con la relativa tipologia di file associata. In caso contrario, clicchiamo *Crea*, assegniamo un nome alla cartella, selezioniamola tra quelle presenti nel nostro NAS e scegliamo il tipo di file contenuto, confermando con *OK*.



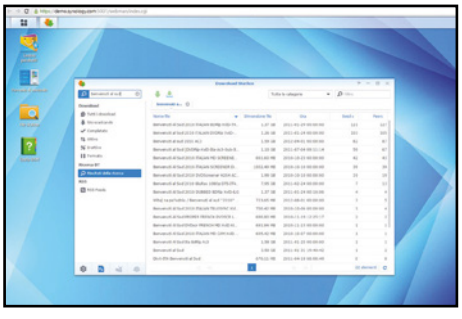
3 Riproduzione in corso

Al termine dell'indicizzazione, a seconda del tipo di file che intendiamo riprodurre, avviamo l'apposita applicazione (Photo Station, Video Station, Audio Station). Per vedere un video, piuttosto che lo slideshow delle foto, clicchiamo *Menu principale* e avviamo l'utility *Video Station*.



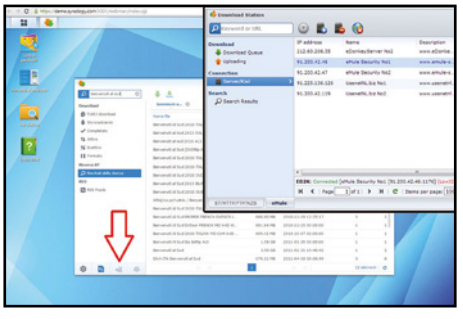
4 Il centro dei download

Se nella lista delle applicazioni installate non è presente *Download Station*, avviamo il *Centro Pacchetti del NAS*, installiamola (è presente nella sezione *Consigliato*) e avviamola. Al primo avvio della *Download Station*, occorrerà selezionare le cartelle in cui verranno salvati i file.



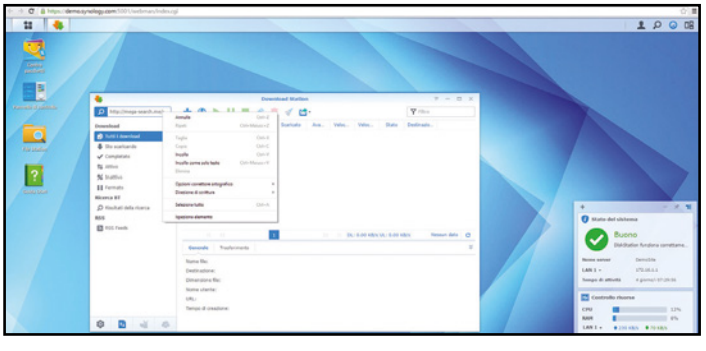
5 Cerchiamo i file su Torrent…

Per cercare un file su rete Torrent usiamo il motore di ricerca integrato in *Download Station*: inseriamo la stringa di ricerca nell'apposito campo e attendiamo che i peer disponibili vengano elencati. Scegliamo il file corretto e avviamone il download con un doppio clic.



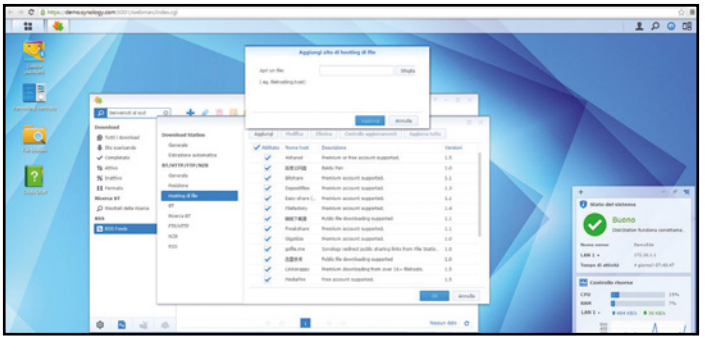
6 … oppure su eMule

Per effettuare la ricerca sui server eD2k, ci basterà invece selezionare l'icona di eMule in basso a sinistra ed effettuare la ricerca. Se non lo abbiamo ancora fatto, abilitiamo il servizio dalle impostazioni della *Download station*, confermando il messaggio che compare al primo avvio.



7 C'è anche il file hosting

Possiamo anche cercare i file sui servizi di file hosting: copiamo l'URL per il download ed inseriamolo nella casella di ricerca della *Download Station*. Sono supportati download multipli e servizi di hosting con autenticazione. È inoltre possibile caricare un file *TXT* con più link.



8 Quel che non c'è, si aggiunge

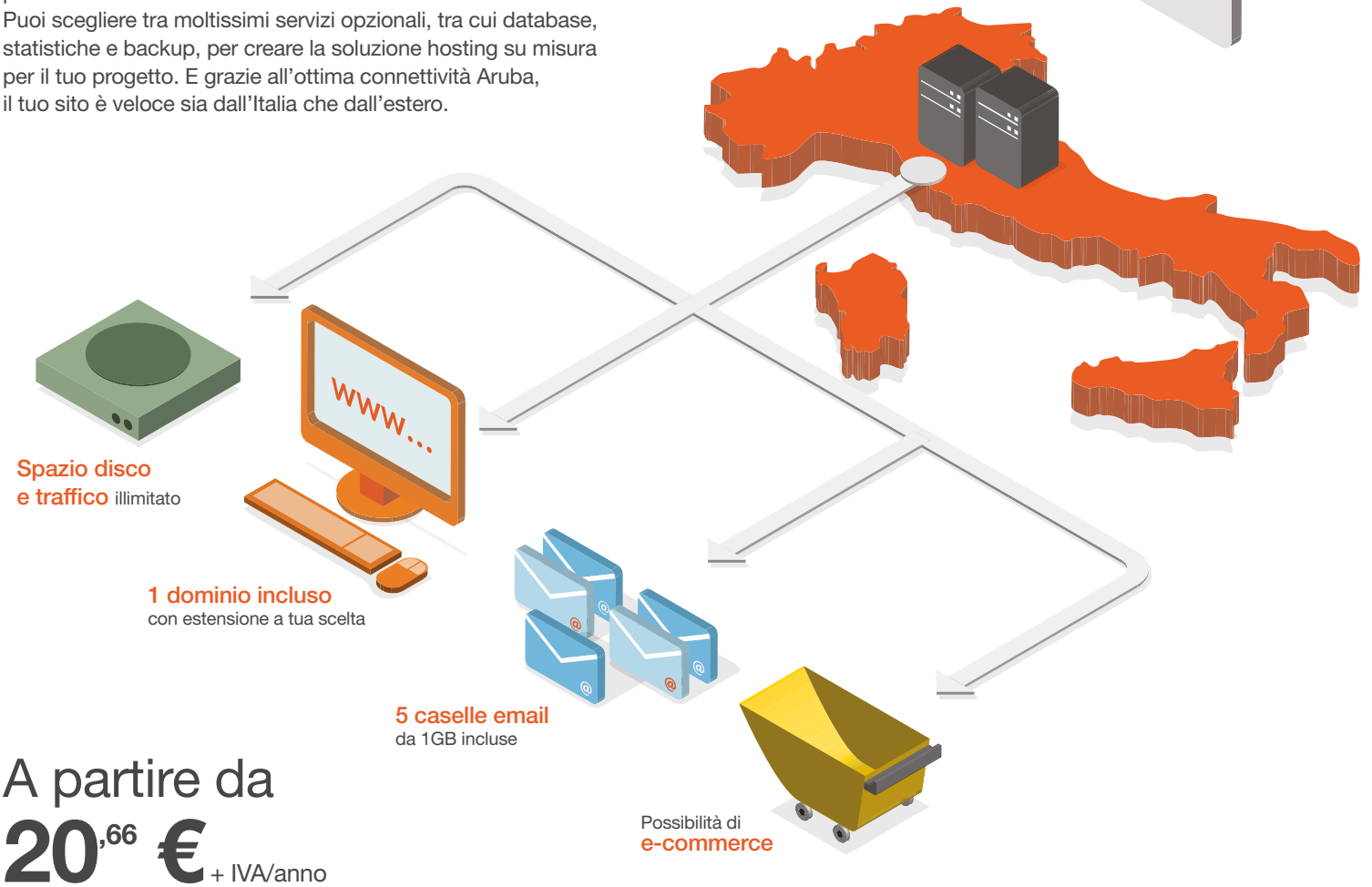
Con *Download Station* è possibile scaricare da numerosi hosting server, ma non tutti sono disponibili di default: per aggiungerne o rimuoverne qualcuno, clicchiamo sull'icona a forma di ingranaggio (*Impostazioni*), poi su *Hosting* di *File/Aggiungi* e inseriamo l'URL del servizio di hosting.

L'Hosting a km 0

Data Center
2 IN ITALIA
6 in Europa

Per la tua attività online scegli la garanzia del Made in Italy.

L'Hosting di Aruba è affidabile, potente e completamente personalizzabile.
Puoi scegliere tra moltissimi servizi opzionali, tra cui database, statistiche e backup, per creare la soluzione hosting su misura per il tuo progetto. E grazie all'ottima connettività Aruba, il tuo sito è veloce sia dall'Italia che dall'estero.



Spazio disco e traffico illimitato

1 dominio incluso
con estensione a tua scelta

5 caselle email
da 1GB incluse

Possibilità di
e-commerce

A partire da
20,66 € + IVA/anno

In più, con Application Installer installare CMS e app è facile e veloce.

WordPress · Joomla! · Drupal · PrestaShop The Best E-Commerce Experience

Per maggiori informazioni: www.aruba.it 0575 0505
assistenza in italiano

aruba.it

Hosting Linux e Windows | Hosting Managed | Hosting Personalizzato | Hosting Plesk | Hosting cPanel

La risorsa creativa n. 1 in Europa
ANCHE IN ABBONAMENTO, A PARTIRE DA 0,16€

37+ milioni di foto, video e vettoriali Royalty Free
in alta risoluzione.
Tel: 06 916.501.625 | http://it.fotolia.com/

fotolia
Royalty Free | Foto | Vettoriali | Video