DIFENDIAMO LA NOSTRA WLAN

Scritto da Matteo Giardino

Le **WLAN** (**Wireless Local Area Network**) sono tutte quelle reti dove gli hosts (ovvero i computer che fanno parte della rete) sono collegati fra di loro mediante una connessione senza fili (generalmente mediante WI-FI). Le WLAN sono molto utilizzate in ambito domestico perchè permettono di connettersi a internet da qualunque parte della casa senza utilizzare dei cavi.
Il segnale emesso dal router, il dispositivo centrale delle rete WLAN che gestisce tutta la rete occupandosi di inviare i pacchetti giusti all' host giusto, copre solitamente un' area molto più estesa della casa; ne consegue che se la rete non è sufficientemente protetta anche dall' esterno è possibile collegarsi alla rete WLAN e usufruire dei servizi internet.

- MISURE DI SICUREZZA

PROTEZIONE MEDIANTE PASSWORD: WEP/WPA/WPA2

Per evitare che qualcuno si impossessi della rete WLAN altrui sono stati inventati alcuni sistemi di protezione mediante password tra i quali i sistemi **WEP**, **WPA** e **WPA2**. Il protocollo **WEP** (**Wired Equivalent Privacy**) risale al 1999 ed è ritenuto un sistema di protezione appena sufficiente ad impedire l' accesso casuale ad una rete WLAN altrui.
Il WEP si basa sull' algoritmo di cifratura **RC4**, ma, l' errata implementazione di questo algoritmo, la quale prevede l' inclusione in tutti i pacchetti dei **vettori di inizializzazione** (detti **IV**) sia in forma criptata che in chiaro (non criptati), permette ai cracker mediante un tecnica detta “sniffing” di analizzare il traffico di rete ed ottenere la password.
Nel 2001 è stato dimostrato che il WEP è un sistema poco sicuro e facilmente oltrepassabile. Nel 2003 è stato progettato un nuovo sistema di sicurezza denominato **WPA** (**Wi-fi Protected Access**) che garantisce una sicurezza nettamente superiore a quella offerta da WEP.
Anche questo sistema di protezione contiene delle falle e gli hacker hanno presto scoperto come raggirarlo.

Il **WPA2** è un' evoluzione del WPA che garantisce una sicurezza quasi assoluta, visto che non esistono ancora procedure per portare a termine attacchi finalizzati a ottenere l' accesso ad una WLAN protetta con questo sistema.
Molto recentemente è stato scoperto un bug nel sistema WPA2 denominato **Hole 196** che permette agli hosts della rete di catturare e decriptare i pacchetti indirizzati ad altri hosts. Per sfruttare questo bug bisogna essere però già autenticati nelle rete, quindi si può dire che il WPA2 costituisce uno standard ancora sicuro.

FILTRO MAC

Un' altro sistema utilizzato per proteggere le reti WI-FI è il **filtro MAC** che consente di permettere la connessione solo a determinate di schede di rete indentificate mediante l' **indirizzo MAC** (**Media Access Control**). L' indirizzo MAC è un indirizzo di **6 byte** tipico di ogni scheda di rete, perciò, non esistono due schede di rete che hanno lo stesso MAC.
Questo sistema di protezione, è però inutile contro gli utenti più esperti, poichè esistono alcuni tools come **GNU Mac Changer** (per Linux) o **MAC Manager** (per Windows) che permettono di modificare a piacimento l' indirizzo MAC della propria scheda di rete.

FILTRO IP

Su tutti i router, è presente un altro filtro, che però non si basa sull' indirizzo MAC della scheda di rete ma sull' **indirizzo IP** del computer. L' indirizzo IP è una stringa di **12 byte** composta da quattro gruppi di tre numeri separati tra di loro da un punto fermo.
L' IP indentifica un host inequivocabilmente solamente all' interno di una rete e non è quindi tipico di una sola macchina come è invece il MAC. Ogni volta che un computer accede a una rete WLAN, il router provvede ad assegnargli un IP che in quel momento non è ancora stato assegnato a nessun' altra macchina.
Per questo motivo una macchina, anche all' interno della stessa rete, può assumere diversi IP.

SSID NASCOSTO

L' **SSID** (**Service Set Identifier**) è il nome della rete Wi-Fi. Generalmente, effettuando una semplice scansione delle reti disponibili, l' SSID di una rete è visibile.
L' SSID è indispensabile per connettersi a una rete: se l' SSID è visibile, il sistema operativo lo estrae automaticamente al momento della connessione, altrimenti, per connettersi, è necessario digitarlo manualmente.

Per aumentare leggermente la sicurezza di una rete è possibile nascondere l' SSID, disabilitando nel pannello di configurazione del router la funzione **SSID Broadcast**. Questa misura non rende comunque la rete invulnerabile da attacchi, infatti, utilizzando appositi programmi come **Kismet** è possibile risalire al SSID di una rete anche se questo è stato nascosto.

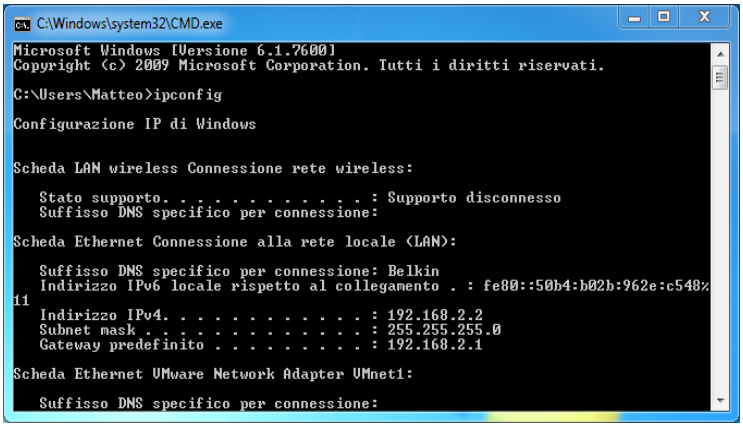
- COME CI SI COLLEGA ABUSIVAMENTE A UNA WLAN

Un hacker che vuole collegarsi abusivamente a una rete WLAN utilizza dei sistemi operativi concepiti per questo scopo cine **Backtrack** o **nUbuntu**. Entrambi sono due sistemi operativi basati su Ubuntu e progettati per eseguire penetration tests.
Una volta avviato uno di questi sistemi operativi (che si possono avviare anche il modalità live CD per non lasciare nessuna traccia sul computer utilizzato) è necessario attivare il **monitor mode** (o **modalità passiva**) sulla propria scheda di rete wireless. La modalità passiva permette alla scheda di rete di intercettare tutti i pacchetti emessi da un router o dalla schede di rete di altri computer. Attivato il monitor mode e scoperto l' SSID della rete a cui connettersi il pirata attiva un particolare software, chiamato **sniffer,** per catturare i pacchetti necessari a portare a termine l' attacco. Se il pirata non riesce a cattuare abbastanza pacchetti "solleciterà" il router ad emetterne mediante una tecnica detta **packet injection**. Raggiunto un certo numero di pacchetti, il pirata utilizzerà un software come **aircrack-ng** per estrarre la **chiave WEP** dai pacchetti catturati in precedenza. A questo punto, il pirata può connettersi liberamente alla rete wireless, poiché possiede la chiave WEP di accesso.

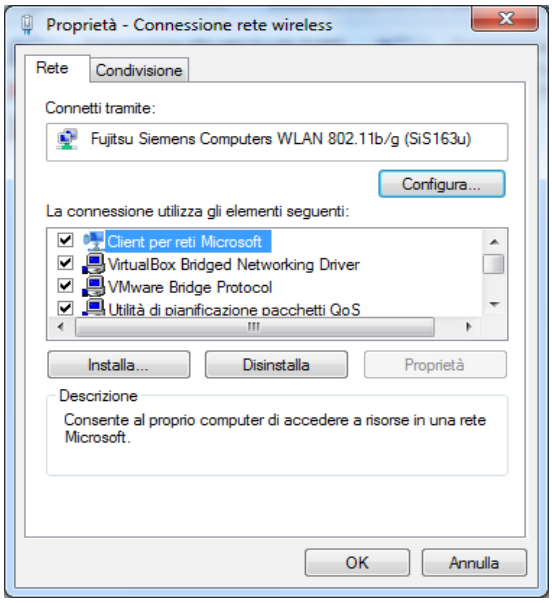
- AUMENTARE LE DIFESE DEL PROPRIO ROUTER

IMPOSTARE UN IP STATICO

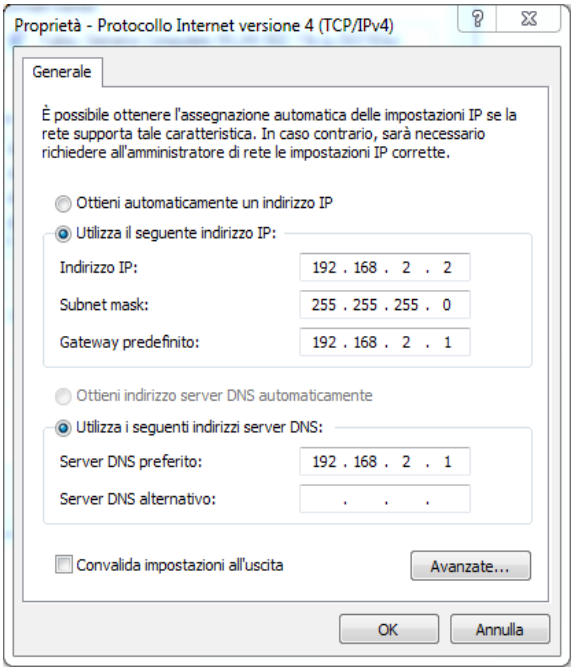
Avviare il prompt dei comandi di Windows, digitare **ipconfig** e premere **INVIO**. Cercare la voce corrispondente alla scheda di rete Wireless e annotare l' i**ndirizzo IP della macchina** e l' **indirizzo IP del gateway** (indirizzo IP del router wireless).



Avviare dal **Pannello di Controllo**, il **Centro connessioni di rete e condivisione**. Nella colonna di destra, selezionare **Modifica impostazioni scheda**.
Nella finestra che appare, cercare la voce corrispondente alla scheda di rete wireless e fare click su di essa con il tasto destro del mouse. Dal menu a tendina che appare selezionare **Proprietà**.

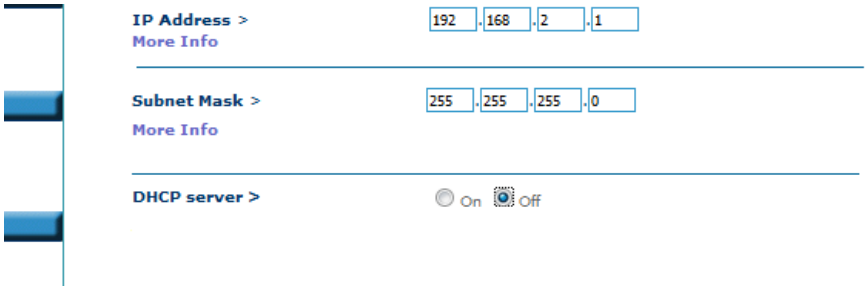


Scorrere la lista di elementi fino a trovare la voce **Protocollo Internet versione 4 (TCP/IPv4)**; fare doppio click su di essa.
Nella finestra che appare selezionare **Utilizza il seguente indirizzo IP**.
A questo punto bisogna inserire i dati richiesti per l' impostazione dell' IP statico. Nella casella **Indirizzo IP** inserire l' IP della macchina ottenuto in precedenza con il comando ipconfig.
Nella casella **Subnet Mask** inserire il valore **255.255.255.0** e nella casella **Gateway predefinito** inserire l' IP del router.
Infine nella casella **Server DNS predefinito** inserire nuovamente l' IP del router. Lasciare la casella **Server DNS alternativo** vuota. Premere **OK** per salvare le impostazioni.



DISABILITARE IL SERVIZIO DHCP

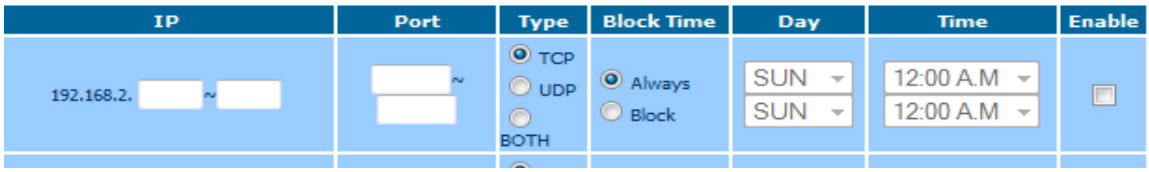
Il **DHCP** è un servizio che assegna automaticamente un indirizzo IP a tutti i dispositivi che si collegano alla rete. La sua disabilitazione rende necessaria l' impostazione manuale dell' indirizzo IP su tutti i dispositivi che vengono utilizzati per connettersi alla rete.
Per disabilitare il DPHC, collegarsi al portale di amministrazione del router digitando in un browser il suo indirizzo IP.
Generalmente l' IP di default è 192.168.2.1. Una volta entrati nella home page, effettuare l' eventuale login (se il router è protetto da password) e fare click **LAN Settings**.
A questo punto selezionare **Off** come valore per la voce **DHPC Server**.



Poi fare click su **Apply Settings**. Su alcuni modelli di router è necessario un riavvio affinchè l' impostazione venga applicata. Altri modelli, invece, si riavviano automaticamente dopo che è stato confermato il salvataggio delle impostazioni.

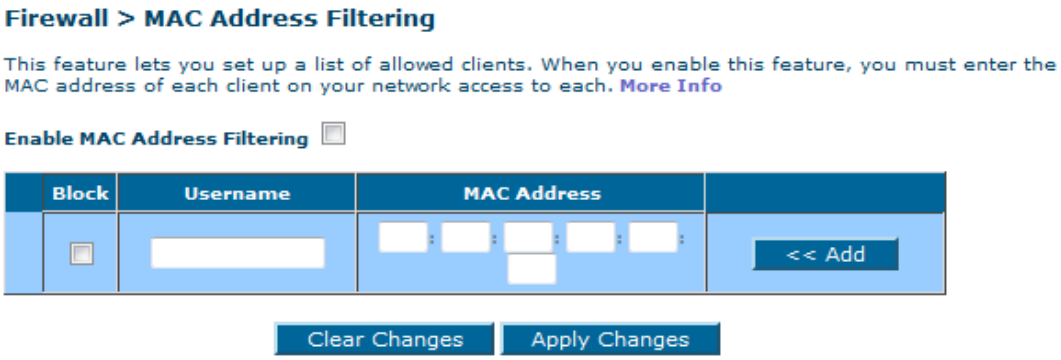
IMPOSTARE IL FILTRO IP

Ora che è stato impostato un IP statico sul computer ed è stato disabilitato il servizio DHCP è possibile abilitare il filtro IP sul router.
Fare click su **Client IP Filters** nella colonna a sinistra nel portale di amministrazione del router. Qui si possono impostare gli intervalli all' interno dei quali deve essere compreso l' IP della macchina per potersi collegare.
Supponendo che l' IP sia **192.168.2.1**, inserire un' intervallo che comprenda questo indirizzo e tutti quelli di eventuali altri computer o dispositivi che si intende utilizzare per collegarsi alla WLAN (es: **192.168.2.1~10**). Selezionare nella colonna di destra la casella **Enabled**. Fare click su **Apply Settings** per confermare l' impostazione.



IMPOSTARE IL FILTRO MAC

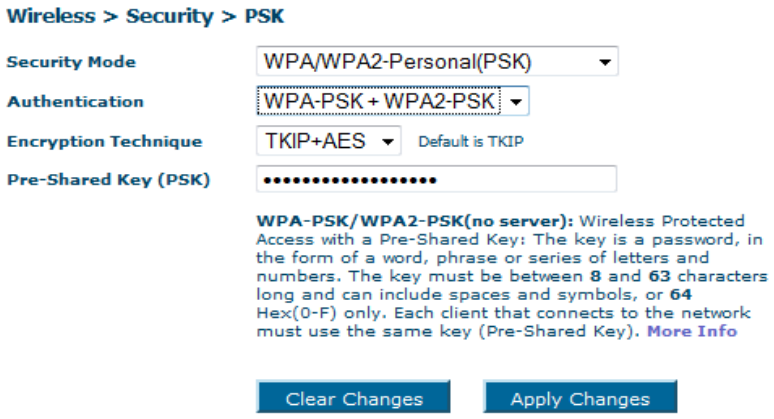
Il filtro MAC si attiva facendo click sulla voce **Mac Address Filtering** che si trova vicino alla voce **Clients IP Filtering**.



Per attivare questo filtro selezionare la casella **Enable MAC Address Filtering**. Una volta abilitato il filtro, è necessario procurarsi l' indirizzo MAC della propria scheda di rete.
L' indirizzo MAC è scritto sulla confezione e su un' etichetta posta sulla scheda. In alternativa è possibile risalire al MAC della propria scheda digitando nel prompt dei comandi di Windows il comando **ipconfig /all**.
Fatto ciò digitare il MAC nelle caselle di testo preposte, inserire un username per la scheda e cliccare su **Add**.
Si ricorda che tutte le schede di rete non presenti nella lista non potranno connettersi alla rete.

PROTEZIONE MEDIANTE PASSWORD

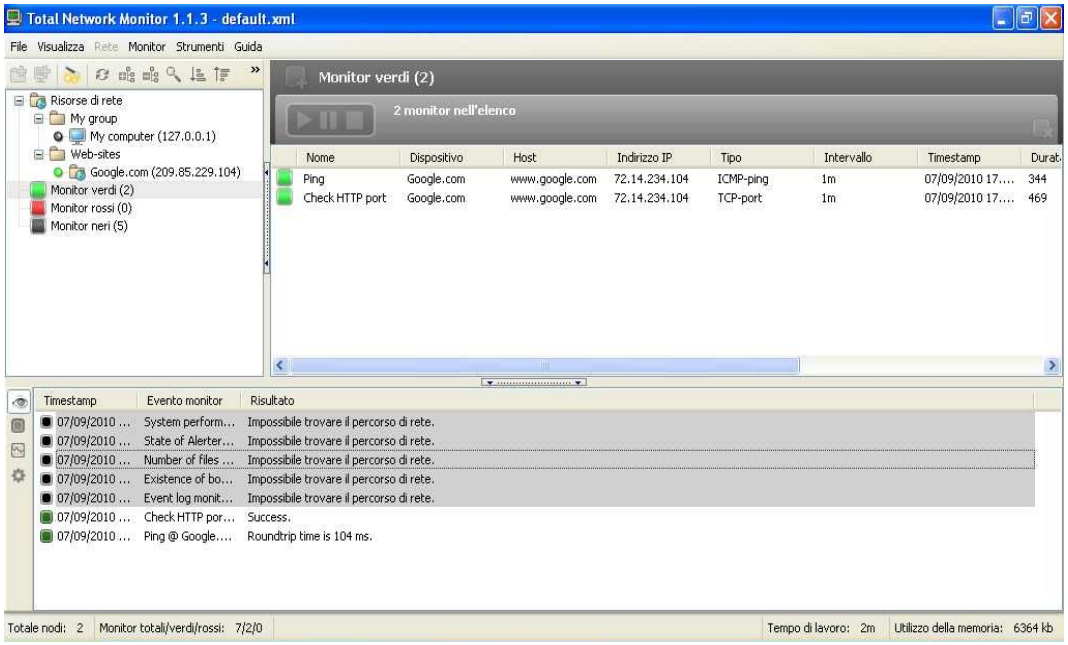
Per avere una rete protetta adeguatamente è buona norma evitare l' utilizzo del protocollo WEP, preferendo il WPA, o il WPA2 sui router che lo supportano. Impostare come sistema di cifratura il sistema AES, da preferire nettamente al sistema TKIP. Su alcuni router è possibile impostare il sistema di cifratura AES + TKIP che unisce i due standard per aumentare ulteriormente la sicurezza.
Impostare una chiave composta da molti caratteri (si consiglia almeno 20) utilizzando lettere maiuscole, minuscole, numeri e simboli speciali (!#?$£%&/()) per rendere più complicati gli attacchi brute-force.
Evitare assolutamente di utilizzare nomi o parole sensate che rendono la password vulnerabile agli attacchi a dizionario. Più lunga è la password più è difficile scoprirla mediante: il WPA supporta password fino a 63 caratteri e la massima sicurezza si ottiene sfruttando tutti e 63 i caratteri a disposizione.



MONITORARE LA PROPRIA WLAN

Per evitare che qualcuno si connetta alla nostra rete a nostra insaputa, si può utilizzare un software che monitora la WLAN e avverte quando un nuovo host si connette. Software di questo tipo sono facilmente reperibili in rete digitando in un qualsiasi motore di ricerca “LAN Monitoring”, “LAN Monitor” o altre parole chiave simili.
Tuttavia uno dei migliori software free di questo tipo è **Total Network Monitor** scaricabile gratuitamente dal seguente indirizzo web:

http://www.softinventive.com/it/products/total-network-monitor/



- ASPETTI LEGISLATIVI

Nel 1993 è stato inserito un articolo nel codice penale che introduce una nuova fattispecie di reato: l' **accesso abusivo a sistema informatico**. L' articolo in questione è il numero **615 ter**. L' articolo 615 ter dice:

"Chinque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni."

L' articolo 615 ter parla anche di alcune circostanze aggravanti il reato di accesso abusivo a sistema informatico:

"La pena è della reclusione da uno a cinque anni: 1)Se il fatto è commesso da pubblico ufficiale o da incaricato di pubblico servizio (...); 2)Se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3)Se dal fatto deriva la distruzione o il danneggiamento del sistema o l' interruzione totale o parziale del suo funzionamento ovvero la distruzione dei dati, delle informazioni o dei programmi in esso contenuti."

– *BIBLIOGRAFIA DELLE FONTI*

Alessandro Di Nicola, *"Hacking fai da te"*, da Linux Magazine (aprile 2010 - anno XII - n° 4), Edizioni Master

Giuseppe De Marco, *"LAN sotto assedio! Attacco e difesa"*, da Linux Magazine (settembre 2010 - anno XII - n° 9), Edizioni Master

AA.VV., *"ADSL Gratis"*, da Win Magazine (settembre 2010 - anno XIII - n° 8), Edizioni Master

AA.VV., *"Wi-Fi: difesa e monitoraggio"*, da Win Magazine (settembre 2010 - anno XIII - n° 8), Edizioni Master

Contributori di Wikipedia, "Wi-Fi", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=Wi-Fi&oldid=34389044 (in data 7 settembre 2010).

Contributori di Wikipedia, "Wi-Fi Protected Access", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=Wi-Fi_Protected_Access&oldid=34024084 (in data 7 settembre 2010).

Contributori di Wikipedia, "Wired Equivalent Privacy", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=Wired_Equivalent_Privacy&oldid=33946774 (in data 7 settembre 2010).

Contributori di Wikipedia, "Indirizzo IP", *Wikipedia, L'enciclopedia libera*, http://it.wikipedia.org/w/index.php?title=Indirizzo_IP&oldid=34728821 (in data 7 settembre 2010).