Come craccare una rete WiFi, protetta WEP, WPA o WPA2

In questa piccola guida, vedremo come poter ottenere accesso ad una rete WiFi, protetta da password WEP, WPA oppure WPA2.

Questo articolo è stato scritto SOLO PER FINALITà CONOSCITIVE E PER TESTARE LA PROPRIA RETE. Ricorda così dice l'articolo 615.
*Chiunque **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.*

Dopo questa piccola, ma doverosa promessa, andiamo a vedere un po' quali sono gli strumenti disponibili per poter testare una rete WiFi, contro possibili attacchi. Prima di continuare, è utile fare un po' di glossario, per poter conoscere nuovi termini:

- **SSID**: è il nome della rete, che compare quando facciamo una scansione WiFi con il nostro dispositivo
- **MAC**: è un codice che identifica un dispositivo, all'interno di una rete, meglio noto come BSSID.
- **Canale:** le reti WiFi comunicano sulle frequenze 2.4 GHz e 5 GHz e in diversi canali, che variano in base alla legislazione del paese in cui ci si trova.
- **Wardriving**: è un'attività che consiste nel mappare le reti WiFi che sono presenti in un area geografica, attraverso un dispositivo con scheda wireless e modulo GPS per la localizzazione.

Come effettuare una scansione delle reti WiFi

Uno dei primi passi per poter ottenere informazioni riguardo alla rete WiFi presenti in zona, è quello di effettuare una ricerca attraverso software. Tale operazione prende il nome di

wardriving e per farla basta avere anche uno smartphone. Ci sono diverse applicazioni disponibili sullo store, specialmente per il mondo Android, dove è possibile far lanciare questa procedura, che permette di raccogliere informazioni, come posizione GPS del router, nome della rete WiFi, tipologia di protezione, canale di trasmissione e se il WPS è attivo.

Ecco i principali tool che si utilizzano:

- Wigle Wifi Wardriving
- Kismac
- inSSIDer
- Netstumbler

I dati generati da questi software sono facilmente esportabili e analizzabili.

Reti WiFi WEP

Le reti WiFi WEP sono quelle più vecchie e dal momento che stanno diventando in disuso, sono meno frequenti durante le ricerche. L'algoritmo di cifratura dello scambio di pacchetti, durante la fase di connessione ad una rete protetta da WEP è stato bucato, nel senso che attraverso la raccolta di un determinato numero di pacchetti (tipicamente più di 10.000), è possibile scovare la password, che protegge la rete. I tool disponibili per procedere con un'attacco ad una rete WiFi protetta da WEP sono i seguenti:

- Fern WiFi Cracker
- Aircrack-NG
- Wifite

Questi software sono abbastanza semplice da poter utilizzare, in quanto dispongono di interazione guidata con l'utente e,

come nel caso d Fern WiFi Cracker, una vera e propria interfaccia grafica, che ne migliora l'usabilità. Occorre aggiungere, che un altro tipo di attacco a cui sono soggette le reti WiFi WEP, è quello della correlazione tra l'SSID e la password di default della rete. Quindi attraverso il nome della rete WiFi, che è facilmente reperibile da una scansione delle reti wireless presenti in zona, è possibile ottenere una password, che in caso non fosse stata cambiata dal proprietario della rete, permette di accedervi. Questo attacco funziona con reti WiFi di router prima del 2014, come ad esempio quelli di Alice, Telecom, Fastweb, Libero etc…, ovvero dei provider Italiani e non solo, che sono soggetti a questo tipo di attacco.

Uno dei programmi più famosi è WPA Tester disponibile per Android, che è molto semplice da usare.

Reti WiFi WPA/WPA2

Per quanto riguarda questi tipologie di reti WiFi, non esiste ancora una procedura simile a quella per le reti WEP, in quanto il meccanismo di protezione è più sofisticato rispetto a quest'ultimo. Gli attacchi possibili, riguardo il mondo del **bruteforce**, ovvero si continuano a fare tanti tentativi di password, fino a quando non si trova quella corretta. I tempi di questi attacchi, possono durare da pochi minuti ad anni, in quanto se la password è di questo tipo, si@3!£98″£NDWb123é*ff)DJIAnda, il processo è molto, ma molto lungo. L'attacco può durare meno, se si utilizzano delle liste preconfigurate, che riducano il numero di tentativi, da quasi infinito ad un numero più ridotto. Ad esempio alcune liste sono già disponibili in base al paese delle rete WiFi, dove tipicamente sono comprese le parole chiave più famose, che possono essere combinato tra di loro. Ci sono anche software, che generano delle liste di password, in base ad informazioni legate al proprietario della rete WiFi. Se ad esempio la rete

WiFi è protetta da una password, che contiene il nome del cane e il nome di battesimo del figlio del proprietario della rete, con un attacco di questo genere, è possibile risparmiare molto, ma molto tempo.

I software più importanti per le reti wireless protette da WPA/WPA2 sono:

- AirCrack-NG
- Fern WiFi cracker
- CoWPatty

Come nel caso delle reti WEP, con password **generata** dal valore **dell'SSID**, un tool come WPA Tester può verificare se la password di default è stata cambiato oppure no, anche per le reti WPA/WPA2.

C'è anche un nuovo tipo d'attacco, che non si basa tanto sulla tecnologia di protezione della rete, più che altro da un'azione fatta dall'utente, che prende il nome di attacco **phishing.** Il tool in questione si chiama wifiphisher (link) e l'attacco si basa sulla seguente dinamica;

1. La vittima, che è già connessa alla rete WiFi in questione, viene de-autenticata, attraverso espedienti hardware come jammer, oppure software
2. Il dispositivo della vittima a questo punto tenterà di connettersi ad una rete WiFi diversa dall'originale, che però ha lo stesso SSID e una potenza maggiore
3. Una volta connessa a questa nuova rete, la vittima verrà re-indirizzata in una pagina web di configurazione, dove per qualche motivo tecnico, dovrà re-inserire la password del WiFi originale
4. A questo punto il PC attaccante, avrà a disposizione la password, per poter accedere alla rete WiFi originale

Questa tipologia d'attacco è molto potente, ma richiede

un’azione da parte dell’utente e qualora si dovesse insospettire di qualcosa, potrebbe in poche minuti trovarvi fisicamente, in quanto l’attacco funziona bene quando l’attaccante si trova in prossimità dalla vittima.

Reti WIFI con tecnologia WPS

La tecnologia WPS è molto comoda, in quanto permette ad un dispositivo ed un router, di scambiarsi una chiave, sfruttando la possibilità di poter accedere fisicamente al router, premendo un pulsante. Purtroppo, questa tecnologia, si è scoperta fragile nella prima versione, perché il pin che viene scambiato tra i due dispositivo è composto da 8 cifre, ma le ultime 4 sono generali dalle prime 4.

Il WPS non è una tecnologia di protezione di una rete, come WEP, WPA/WPA2, ma bensì una tecnologia d’aiuto per collegarsi ad un rete. Per questo motivo, è possibile craccare una rete WiFi utilizzando questo exploit, con uno dei seguenti tool:

- Fern WiFi Cracker
- Reaver
- WPS Pixie (link)

Linee guide per evitare attacchi

Ecco un po’ di linee guide, per evitare intrusioni nella propria rete wireless:

- Utilizzare come livello di protezione WPA2
- Cercare di utilizzare una password composta lettere minuscole, maiuscole, numeri, caratteri speciali e abbastanza lunga
- Cercare di cambiare la password durante l’anno
- Disabilitare il WPS
- Effettuare aggiornamenti il più possibile al router
- Evitare di inserire la password del vostro WiFi in

pagine WEB
- Evitare di fornire la password della vostra rete ad amici, meglio creare una rete apposta per logo (rete Guest)

Conclusione

Nel mondo della sicurezza informatica, si può tranquillamente sostenere che ottenere accesso ad un qualunque dispositivo, come ad esempio ad una rete WiFi, è questione di tempo e di risorse a disposizione. L'obiettivo degli sviluppatori/ingegneri informatici, è quello di rendere il più lungo possibile tale spazio temporale. Per quanto riguarda le reti WiFi, ci sono diverse tipologie d'attacchi, che funziona a seconda del livello di protezione della rete WiFi e di chi l'amministra. Come già accennato all'inizio, questa guida ha il solo scopo di dare una panoramica riguarda al mondo delle rete WiFi, in modo da potersi adoperare per evitare intrusioni.

TP-Link TL-WR710N: un router con cui si può fare di tutto

In un mercato ricco di tante opportunità è difficile scegliere il router che alla proprie esigenze. Oggi parliamo di un Router, economico, che permette di fare praticamente tutto: il TL-WR710N di TP-Link.

Esso dispone di una porta USB, con la quale poter caricare il proprio smartphone, oppure collegare una memoria USB per condividere documenti in rete locale e in remoto e due porte ethernet, che svolgono differenti funzioni, in base alla modalità di funzione del Router.

Molteplici modalità di funzionamento per i diversi scenari

- **Modalità Wireless Router (Default)**

Crea una rete wireless privata immediata e condividere Internet a più dispositivi Wi-Fi, che è adatto per la maggior parte dell'hotel e alla rete domestica.

- **Client Mode (TV / console di gioco)**

Dà cablata dispositivi di solo accesso a una esistente reti Wi-Fi.

- **Modo ripetitore**

Estendere i prodotti Wi-Fi, migliorando la potenza del segnale e ottimizzando la copertura.

- **Modalità access point**

Crea una rete wireless per i dispositivi Wi-Fi.

- **Modalità WISP Client Router**

Simultaneo accesso wireless ISP e condivisione.

Porta USB multifunzione per la condivisione di file e di ricarica

Dotato di una porta USB 2.0 multifunzionale, è possibile condividere file e contenuti multimediali all'interno della rete locale tra i vostri diversi dispositivi come PC, smartphone e tablet. Inoltre, la porta USB in grado di fornire alimentazione elettrica (fino a 5V/1A) per dispositivi mobili come smartphone o tablet, in modo da poter evitare la fatica

di trasportare diversi caricatori durante il viaggio.

Quella più rilevante sono la modalità client e quella WISP. La prima permette, per esempio, di collegare la TV di casa che dispone della sola porta Ethernet, via WiFi, mantenendo la stessa classe di IP. In questo caso, si dispone di due porte Ethernet del TP-WR710N. La seconda modalità, che è stata da poco creata, permette di creare una rete WiFi aggiuntiva a quella presente e di usufruire delle due porte Ethernet, per connettere ad Internet periferiche che hanno soltanto porte RJ-45. Occorre sottolineare che in questo caso il TP-WR710N svolge il ruolo di NAT e quindi, per eventuali operazioni avanzate, è necessario aprire le porte dei servizi utilizzati. Esempio di rete con tecnologia WISP:

Router di Casa principale (connesso ad Internet, IP 192.168.0.x) —- 802.11, 2.4/5.0 GHz — TP-WR710N — Via Cavo Oppure via WiFi (con SSID: Nuova_Rete) (IP: 192.168.1.x)

Il router TP-WRL710N permette inoltre di accedere da remote facilmente alla rete di casa attraverso il protocollo VPN. Per esempio è possibile accedere al NAS di casa, anche dall'ufficio, oppure stampare da remoto. Il giudizio di questo Router è più che positivo, e permette di fare tantissimi cose, anche avanzate, a prezzi contenuti, dal momento che è possibile acquistare il prodotto su Ebay per 20 Euro.

Materiale del TP-WRL710N

TL-WR710N_V1_QIG

TL-WR710N_V1_Datasheet

TL-WR710N_V1_User_Guide

Dove scaricare e come installare Kali Linux, meglio noto come Backtrack 6

Kali Linux, per chi non lo sapesse, è la nuova versione di Backtrack, nella quale è stata rinnovata completamente la grafica e sono state aggiunte tante nuove applicazioni, per testare la sicurezza dei propri dispositivi. Per chi fosse interessato, ci sono tante guide sulla versione 5 R3 di Backtrack e si trovano al seguente link. Uno dei vantaggi di Kali Linux è quello di supportare tantissime architetture hardware, come quelle basate sui processori x86, ma soprattutto l'architettura ARM, dove spicca il piccolo PC Raspberry PI . Anche per questo dispositivo sono state scritte alcune guide, reperibili al seguente link, oppure è possibile scaricare gratuitamente il libro "Alla Scoperta del Raspberry PI" dalla seguente pagina WEB. Per scaricare il sistema operativo Kali Linux, è possibile farlo direttamente dal sito ufficiale, attraverso il seguente indirizzo http://www.kali.org, dove è possibile leggere alcune guide in Inglese, oltre che rimanere aggiornato sulle ultime novità del successore di Backtrack.

Come già detto precedentemente, Kali Linux è disponibile per varie piattaforme. In questo post, vedremo come installarlo sui processori x86, attraverso il lettore DVD. Prossimamente, vedremo come installare il sistema operativo attraverso una chiavetta USB. Per scaricare il corretto sistema operativo,

andiamo nella sezione **“Download”** e selezioniamo come architettura **i386**. Abbiamo la possibilità di scaricare l’Os come un normale download, oppure via Torrent; quest’ultima modalità è consigliata, dal momento che risulta essere più veloce il download e inoltre è possibile caricare il file tracker su un NAS in locale, per non dover tenere accesso il PC.

Una volta completato il download, basterà masterizzare un normale file .iso. Per gli utenti Mac, basterà aprire il programma “Utility Disco”, selezionare il file e la voce Masterizza, dopo aver inserito un DVD. Per gli utenti Windows, è possibile utilizzare i programmi come Nero, oppure Win Rar e masterizzare i file scompattati. Per gli utenti Mac è normale che il sistema operativo non riconoscerà il DVD appena masterizzato. Una volta terminata questa operazione, basterà aprire il lettore del PC su cui vogliamo installare il sistema operativo Kali Linux. L’unica eventuale impostazione da fare, è quella nel BIOS, per far partire il sistema operativo da CD/DVD. Una volta acceso il computer, apparirà la seguente schermata:

Ora basterà selezionare la voce “Install” per chi vuole installare il sistema operativo, mentre per chi vuole utilizzare in modalità Live, basterà selezionare la relativa voce. Attenzione che per chi selezionasse la voce Install, nei passaggi successivi verrà richiesto di formattare l’intero disco; questo comporterà la perdita di tutti i dati presenti nel disco rigido !

Una volta terminata l’installazione, che richiederà circa 15-20 minuti, si potrà finalmente giungerà alla schermata principale del sistema operativo Kali Linux.

Alla Scoperta di Backtrack 2° edizione disponibile in PDF

Dopo la pubblicazione sullo store di Apple, il libro Alla Scoperta di Backtrack 2° edizione è disponibile all'acquisto anche per gli utenti non Apple. Basterà effettuare il pagamento tramite Paypal, leader mondiale nelle transazioni online. In questo modo si potrà scaricare il libro in formato PDF, che permette di leggerlo comodamente sul computer o tablet. Sarà possibile trovare 30 nuove pagine, con 3 nuovi capitoli, dedicati a nuovi argomenti, come il VOIP, il mobile, oltre che ad una rivisitazione del capitolo 3 su come ottenere una password di una rete WiFI, con l'introduzione di nuove applicazioni come Fern WiFi Cracker e Wifite. La struttura è sempre la stesa, cioè argomenti spiegati in pratica, anche attraverso l'uso di immagini. Il prezzo non è cambiato ed è di 3,99 Euro. La terza edizione del libro, dovrebbe essere completata entro Giugno del prossimo anno. In tale edizioni, verrà ampliato ancora di più il libro, con inserimento delle sezione per testare la sicurezza dei siti web.

[purchase_link id="1063″ text="Acquisto" style="button" color="blue"]

Caine OS: L’indagine forense all’Italiana

L’informatica è davvero entrata nella vita di tutti i giorni. Ogni giorno si utilizzano per comunicare PC, smartphone, dove carichiamo anche i nostri dati personali. Ora sorge un problema ? Le nostre informazioni e dati sono davvero sicuro ? Come mostrato nella guide su Backtrack (che continueranno a breve), se si utilizza una connessione dati Wireless, i nostri dati possono essere rubati abbastanza facilmente, attraverso programmi anche semplice da usare. Un nuovo OS, che può essere utilizzato per tantissimi si scopi si chiama Caine e può essere scaricato presso il sito ufficiale http://www.caine-live.net/.

Questo progetto è tutto Italiano e merita davvero di essere seguito. Questo OS, può essere utile per quanto riguarda le indagine forense, che non sono altri ricostruzioni di documenti e di azioni che era/sono presenti su un dispositivo. Per esempio è possibile ricostruire un’immagine cancellata, oppure analizzare la cronologia dei siti visitati da una persona. Queste tecniche sono usate dai famosi “RIS” per ricostruire scene del crimini. Per chi fosse interessato a capire come vengono svolte queste indagini, può utilizzare questo OS davvero ben fatto. All’interno di Caine, è possibile trovare i seguenti software:

iphonebackupanalyzer
exiftool phil harvey
tcpflow
tshark
john
wireshark

firefox
vinetto
mdbtool
gdisk
LVM2
tcpdump
Mobius
QuickHash
SQLiteBrowser
FRED
docanalyzer
nerohistanalyzer
knowmetanalyzer
PEFrame
grokEVT
zenmap (nmap)
blackberry tools
IDevice tools