ATACURI PRIVIND SECURITATEA REȚELEI. ARP POISONING – ATTACK MITM (Man-in-the-Middle).

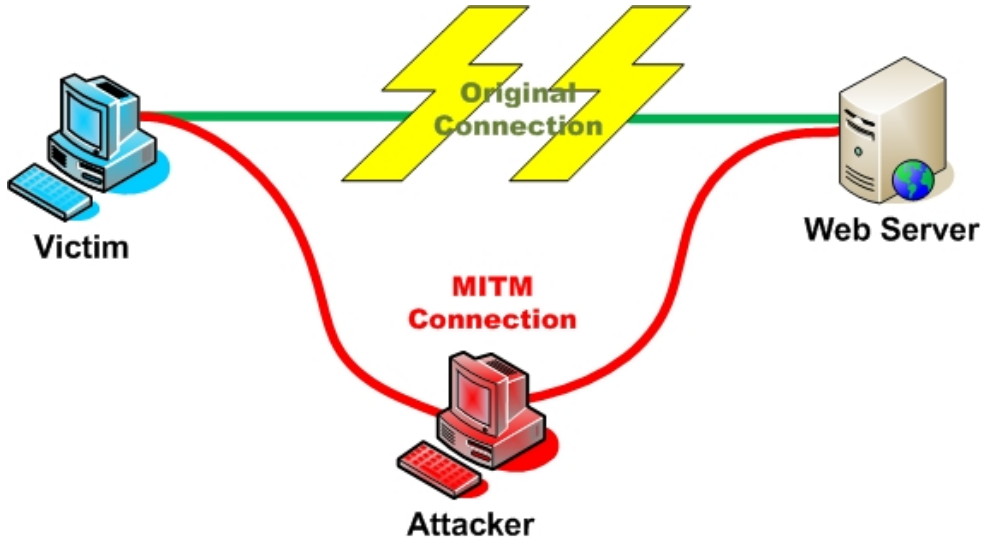
1. Descrierea principiului de attack MITM (Man-in-the-Middle).
2. Înțelegerea principiului adresarii în rețeaua locală. Arp Poissoning.
3. Studierea functionalitatii programului Cain & Abel.
4. Cain & Abel – capturarea trafficului.
5. Kali Linux (Arpspoof, Driftnet, Urlsnarf, Ettercap, Aircrack) – capturarea traficului.
6. Soluții de prevenire a atacului de tip MITM.

1. Descrierea principiului de attack MITM (Man-in-the-Middle).

MITM – este un tip de attack, care presupune ca atacatorul isi mascheaza identitatea cu acea entitate la care victima incearca sa apeleze pentru crearea unei sesiuni fie web, telnet, ssh, ftp, rdp etc, astfel incat victima nu-si poate da seama ca ea comunica printr-un canal nesigur.

Scopul atacatorului este, ca de exemplu, de a-si pozitiona PC-ul personal intre Client(victima) si Web Server – pentru interceptia traficului si obtinerea posibilitatii de a cauza careva modificari in el, sau de a obtine date confidentiale.

Atacul de obicei se incepe de la faptul ca este “ascultat” canalul de retea si se termina cu aceea ca atacatorul incearca sa schimbe mesajul obtinut, sa extraga din el informatia utila, si sa-l retransmita la un careva resurs extern.



Din figura de mai sus, se observa ca sesiunea web originila este intrerupta, iar atacatorul a facut intruziunea intre aceste doua host-uri, cu ajutorul unui attack de tip MITM.

Sunt careva tipuri de programe software, utilizate pentru intruziuni de tip MITM, mai ales pentru retele locale:

- PacketCreator

- Ettercap
- Dsniff
- Cain & Abel

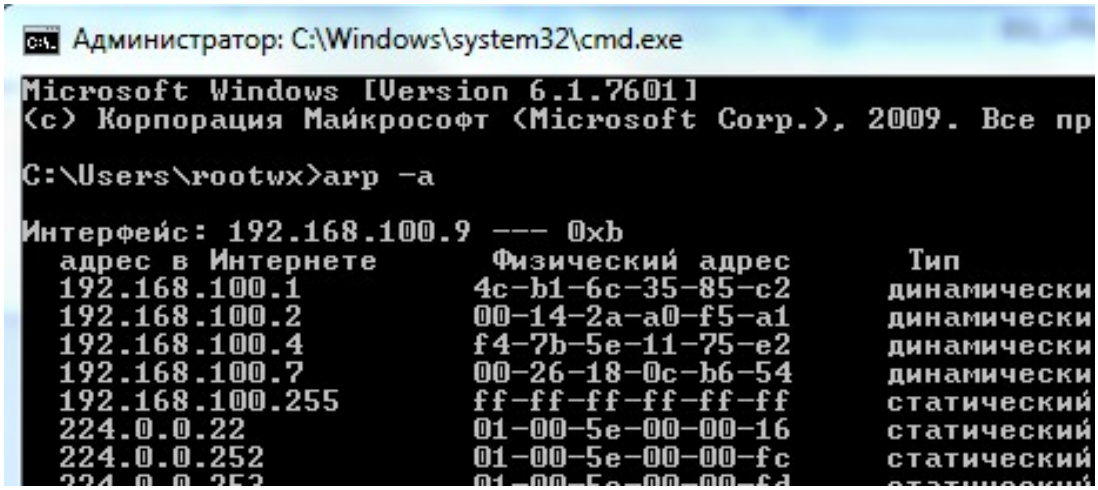
Pentru exemplu de un astfel de attack, va fi folosit software tools Cain & Abel si va fi demonstrat pe baza unui intrusion cu ajutorul tehnicii Arp Poissoning (infectarea Arp-ului). In continuare va fi descris careva principiu de functionare a Arp-ului, pentru a fi mai clar ce se intimpla, dupa ce se va trece la efectuare.

2. Intelegerea principiului de adresare in retea locala. Arp si Arp poissoning.

Deci, pentru a nu intra in detalii, voi incerca sa explic pe scurt dar clar cum are loc adresarea in retea locala. In reteaua locala – deasemeni adresarea are loc prin IPv4 address, ceea ce inseamna ca atunci cand calculatorul genereaza un trafic de transmitere el trebuie sa cunoasca doua lucruri: ip-ul celui care acest trafic ii este predestinat si respectiv mac adresa acelui care ii este predestinat traficul.

IP-ul este necesar pentru a determina entitatea logica careia ii este predestinat traficul, iar mac-ul este pentru a determina si explica switch-ului (la care sunt conectate host-urile de un broadcast domain) la ce port trebuie transmis acest trafic.

E necesar de mentionat, ca aceasta mac adresa , este continuta la orice sistem de operare in asa numita arp-table. Predestinatia acesteia este de a cunoaste corespondenta dintre ip-ul logic si mac adresa fizica a unui host, pentru realizarea sesiunii tcp/ip in reteaua locala.

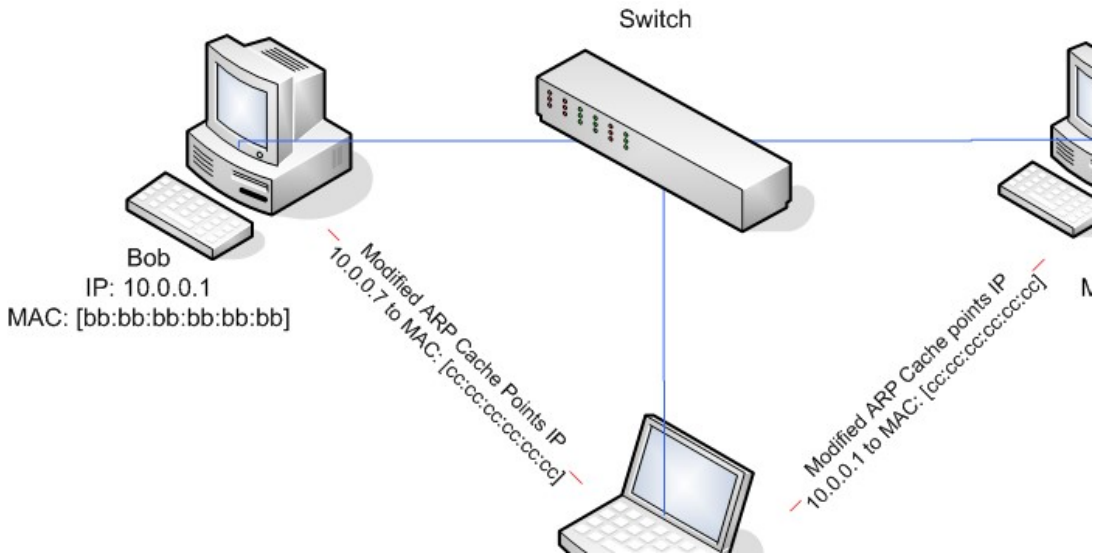


Asa arata arp-table in consola de comanda CMD. Acesta arp-table – este inscris dinamic, adica poate fi curatit si se va umple automat cu rindurile vazute, datorita arp interogarilor in retea locala, care intreaba “ce mac are ip adresa respectiva?” si este primit raspunsul “eu sunt cu acest ip, si am mac adresa respectiva *******”. Astfel se obtin datele din acest arp-table.

Pentru a intelege principiul de adresare, vom presupune ca un host A cu ip adresa A, are nevoie sa transmita un careva trafic in reteaua de internet.

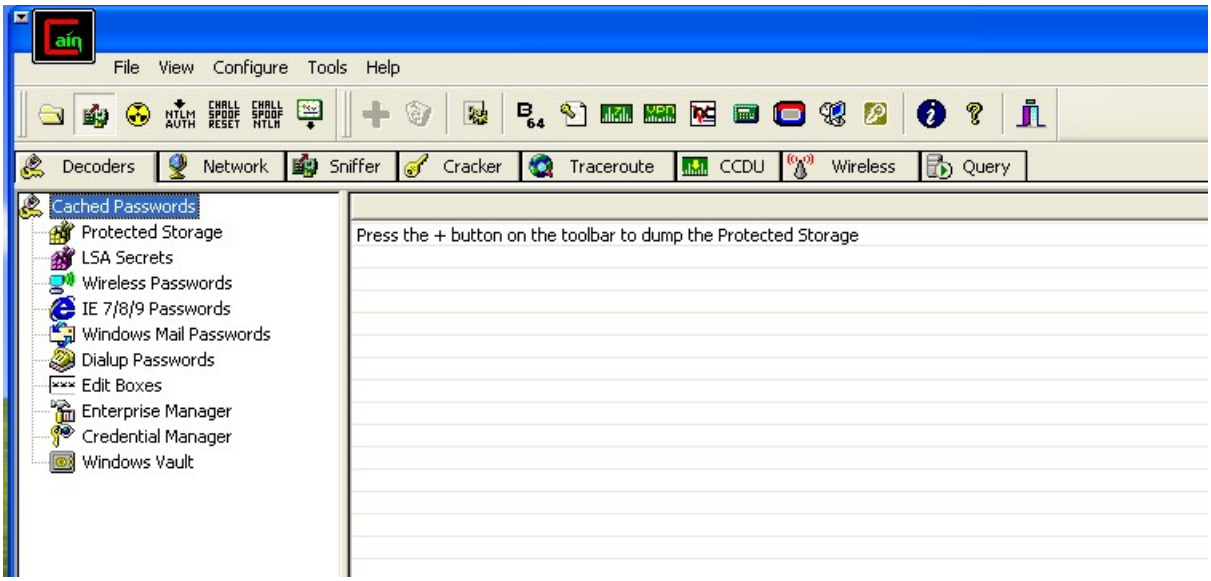
Deci la destination IP – el va inscrie ip adresa B a ruterului care are iesire la internet service provider si respectiv mac adresa care corespunde acestui IP. In cazul meu interface-ul ruterului are ip 192.168.100.1 , ceea ce implica si mac adresa de alaturi. La fel are loc si schimbul de date cu un host din retea locala, fie cu 192.168.100.4 sau altul.

Acum sa intelegem ce inseamna arp-poissoning. Sa ne imaginam acum, ca in timpul realizarii acelei interogari “ce mac are ip adresa respectiva?” , in loc sa raspunda entitatea adevarata, raspunde atacatorul care zice “ca el are acest ip, si respectiv indeamna victima sa-si faca inscrierea neadevarata in arp-table”. Acest lucru inseamna ca daca un careva trafic va veni la destinatar, el va trece mai intii prin canalul atacatorului, dupa aceea atacatorul il va directiona inspre destinatie, si respectiv raspunsul poate fi deasemenea capturat in mod similar. Interceptia traficului poate fi efectuata bidirectional.



3. Studierea functionalitatii software Cain & Abel.

Acest software, are mai multe utilitati: captureaza parole facind sniffing de retea, crack-ul parolelor criptate utilizind dictionare, brute-force si crypt analys atacuri, inregistreaza conversatiile VoIP, decoding la parolele criptate, descoperirea parolelor din cache si analiza protocoalelor de rutare.



Din cate vedem, sunt multe posibilitati, utilitati, sniffer, decodere, crack passwords etc.

Vom realiza doar arp spoofing, sau arp poissoning.

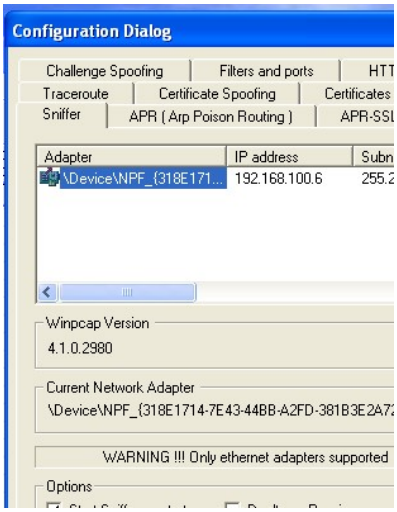
4. Cain & Abel – capture HTTP traffic.

Acest program este freeware, distribuit gratis. Are develop atat pentru linux cat si pentru windows.

Il putem accesa de pe web site-ul insecure.org, sau de pe linkul direct http://sectools.org/tool/cain/

Dupa ce descarcam programul, il instalam si verificam daca a fost instalat winPcap driver.

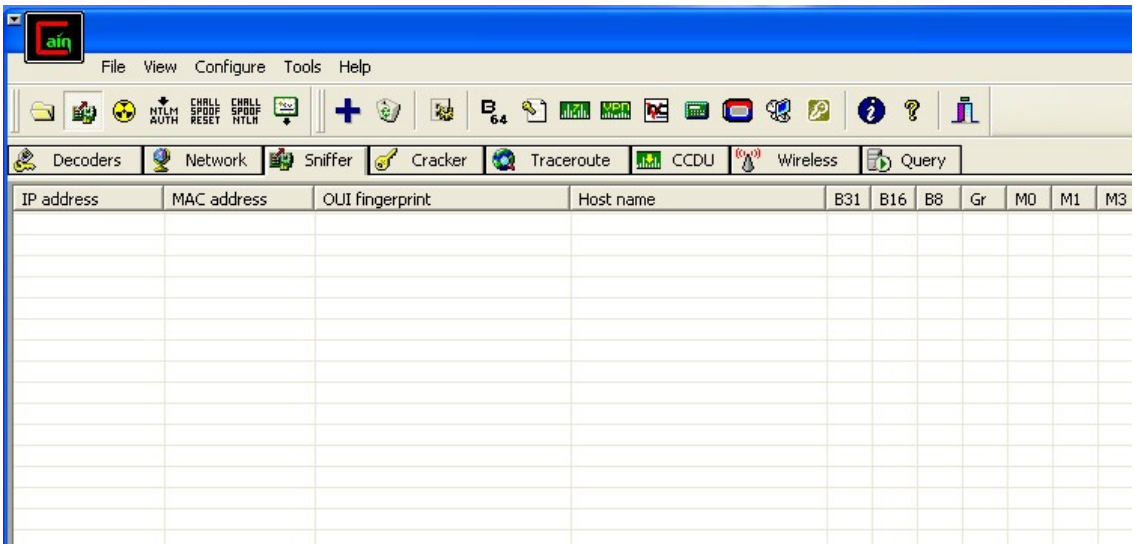
La prima lansare – accesam Setarile (Configure) din menu.



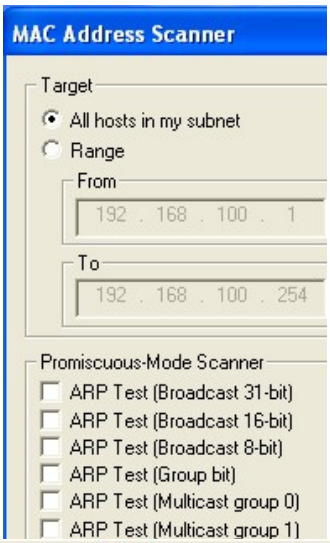
Verificam sa fie ales Network Interface Adapterul corect. Pentru ca – prin el vom realiza legatura in retea si apasam ok.

Dupa aceasta, apasam butonul din stinga Start/Stop capture traffic care va setat cartela de retea in regim de ascultare traficului.

Dupa aceasta, trecem in compartimentul Sniffer -> Hosts(jos).



In aceasta fereastra, apasam pe unul din rindurile libere, ca sa se activeze butonul plus. Il apasam apoi pe el si scanam reteaua, apasam ok.

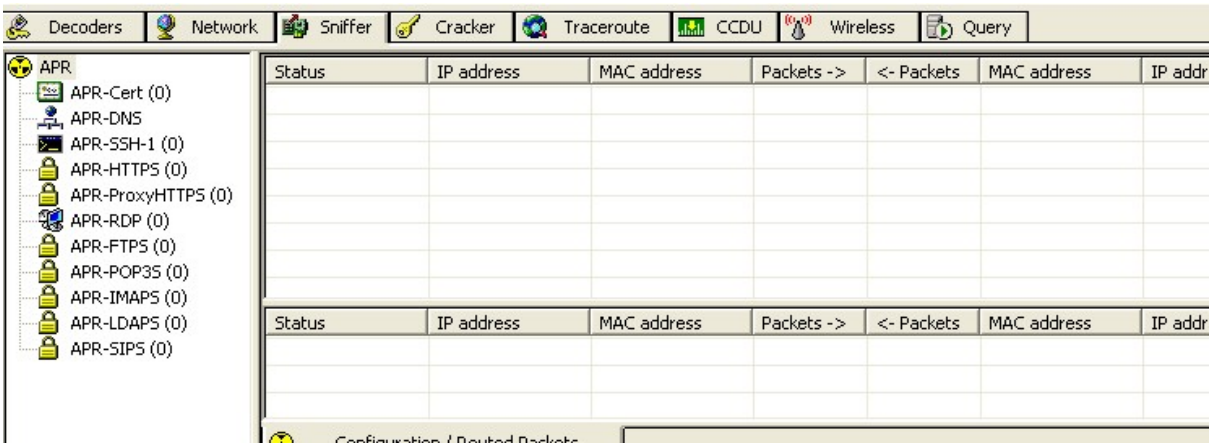


Dupa ce au fost scanate subreteaua, avem un astfel de rezultat:

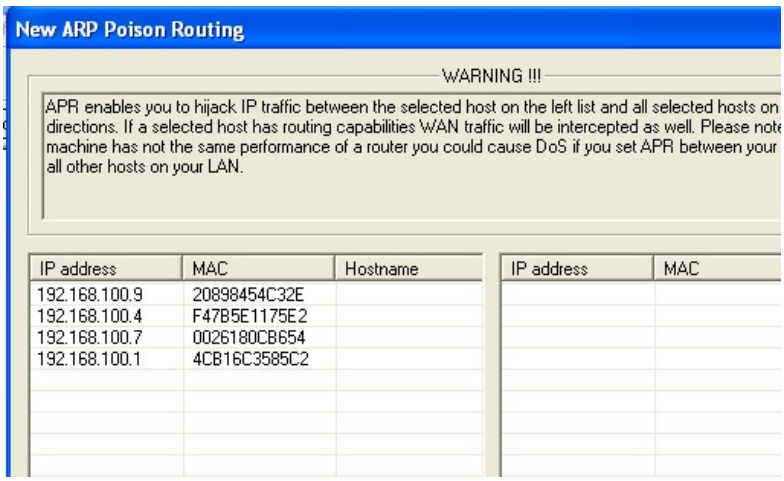
Observam ce host-uri au fost identificate: 2 calculatoare, un televizor samsung, si ruterul.

Vom realiza arp spoofingul pentru calculatorul cu ip-ul 192.168.100.7. Astfel vom incerca sa devenim ruter pentru el, facind un arp poisson vom avertiza calculatorul victima – ca noi sintem ruterul ☺

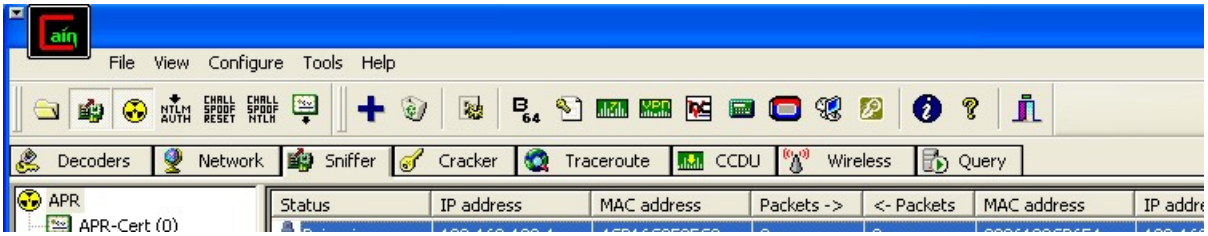
Apasam pe compartimentul APR (de linga Hosts).



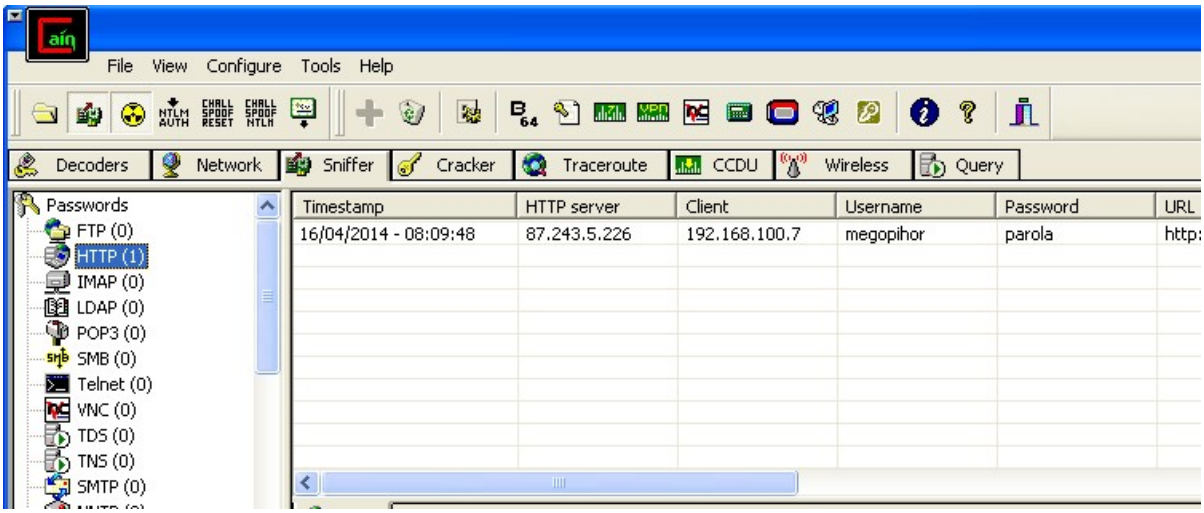
Apasam pe spatiul liber (acele campuri goale.) sa ne apara plusul. Si apoi apasam plus.



Aici alegem mai intii ip adresa celui care va fi spoofed (adica 92.168.100.1), indicam cu alte cuvinte cine dorim sa fim noi. Pentru aceasta apasam click pe ip adresa respectiva. Mai apoi – din dreapta ne vor aparea toate celelalte ramase. Din ele alegem numai acele adresa care vor fi victimele noastre, in cazul dat doar 192.168.100.7, dupa ce apasam OK. Alegem sus linga Start/Stop capture – butonul arp- poisson si asteptam ☺



Trecem la compartimentul password (jos) si alegem din stinga field-ul HTTP(1). Aici observam traficul capturat – loginul si parola pentru website-ul http://www.torrentsmd.com/ cu datele respectiva ale serverului, si timestamp. Deci daca utilizatorul de pe masina 192.168.100.7 va mai incerca careva logari vom observa in http si alte parole/date de logare.



5. Kali Linux (Arpspoof, Driftnet, Urlsnarf, Ettercap, Aircrack) – capturarea traficului.

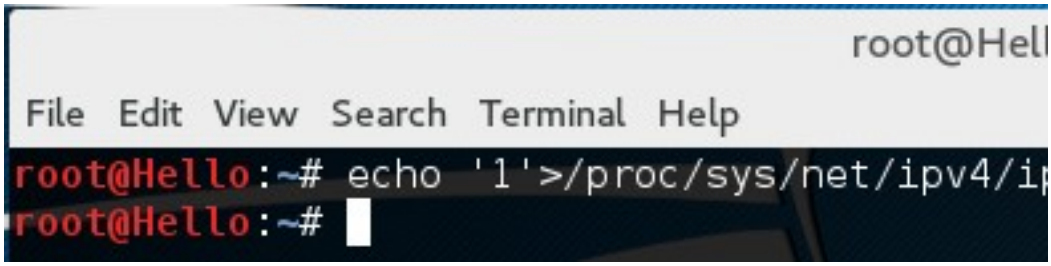
Configurăm mașina noastră Kali Linux, pentru a putea permite transmiterea de pachete deoarece acționează ca un man-in-the-middle.

Kali Linux trebuie să acționeze ca un router între router-ul real și victima.

Pentru a face ca Kali Linux să acționeze ca un router între route-ul real și victimă, trebuie de schimbat valoarea din 0 în 1 din /proc/sys/net/ipv4/ip_forward.

Linia de comandă :

```
echo '1' > /proc/sys/net/ipv4/ip_forward
```

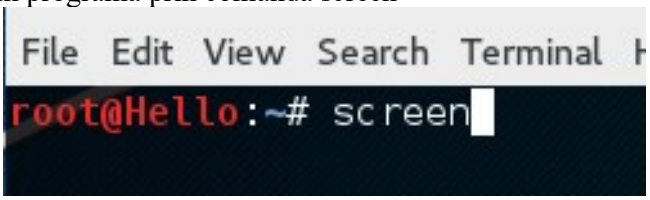


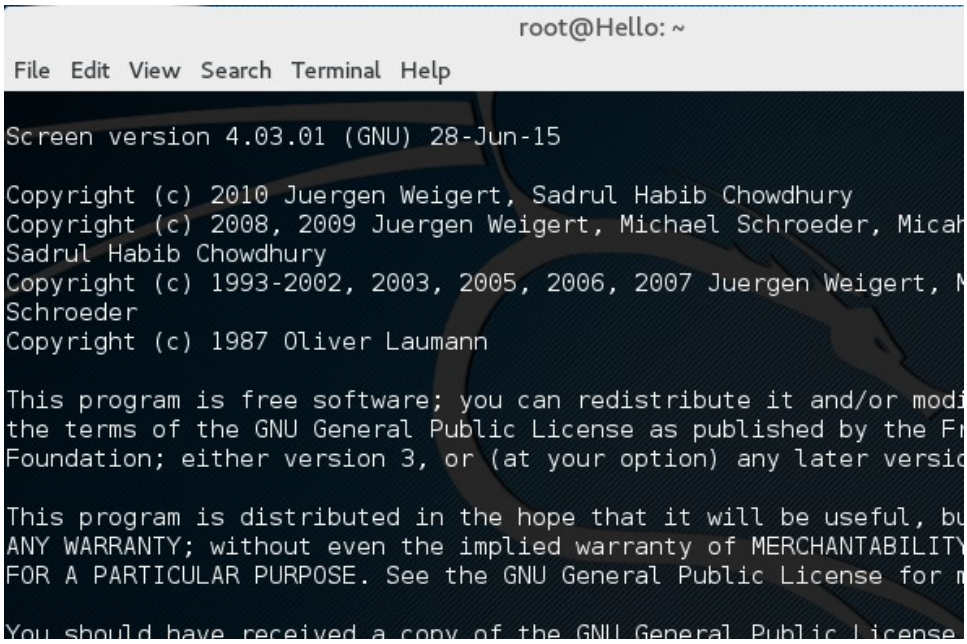
Avem posibilitatea să modificăm interfața de terminal pentru a face vizualizarea mult mai prietenoasă și ușor de monitorizat prin separarea ferestrei terminalului Linux.

Pentru aceasta ne vom folosi de screen . Screen este un manager de ferestre full-screen, care multiplexează un terminal fizic în mai multe procese.

Instalăm screen prin sudo apt-get install screen

Apoi pornim programa prin comanda screen

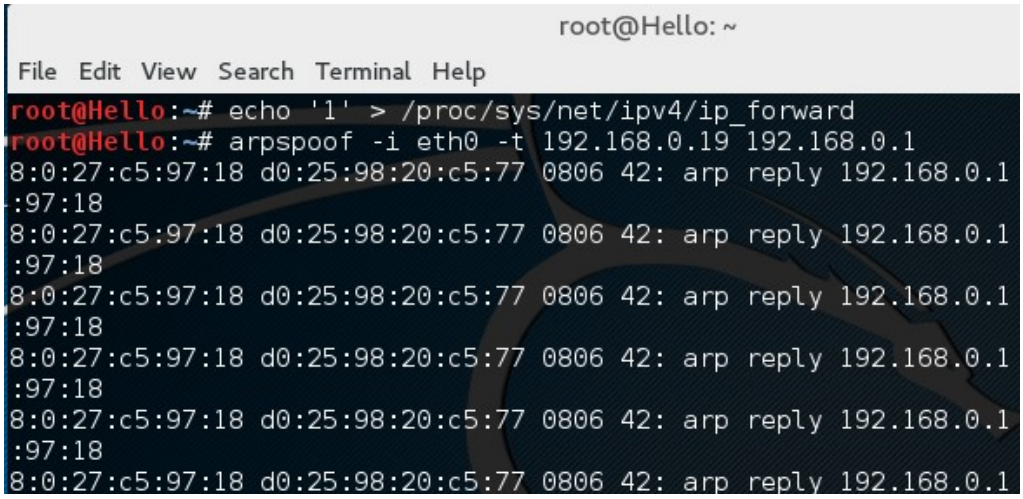




*Pentru a separa terminalul vertical formăm comanda de taste CTRL+A apoi |
*Pentru a separa terminalul orizontal formăm comanda de taste CTRL+A apoi SHIFT+S
* Pentru a ne mișca printre ferestre CTRL+A apoi TAB

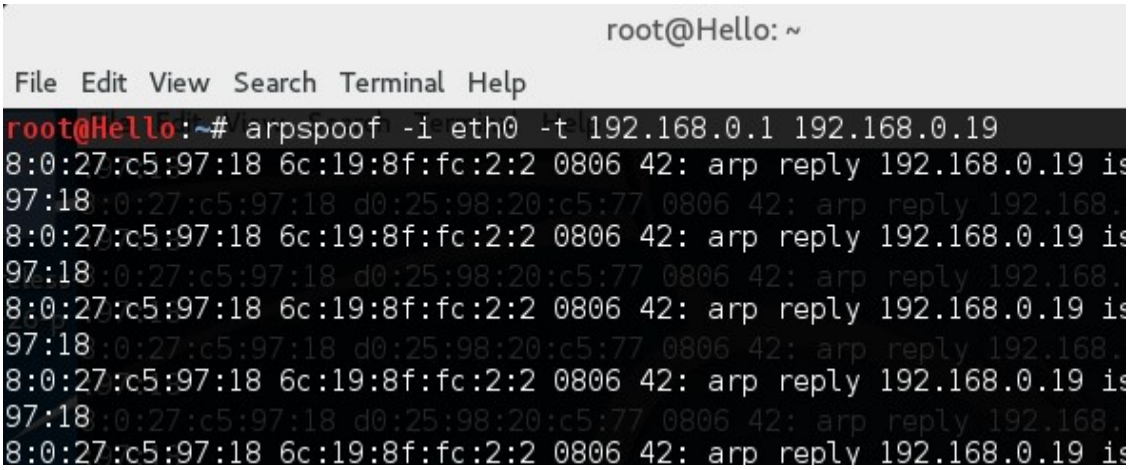
Următorul pas este să setăm arpspoof între victimă și router

arpspoof -i eth0 -t 192.168.0.19 192.168.0.1



Următorul pas este să setăm arpspoof între router și victimă

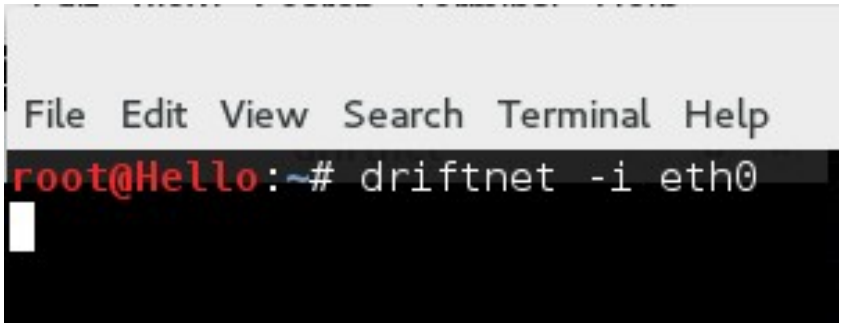
arpspoof -i eth0 -t 192.168.0.1 192.168.0.19



Acum toate pachetele trimise sau primite de către victimă ar trebui să treacă și prin mașină atacator.

Driftnet reprezintă o programă care preiea imaginile care le observă stream-ul TCP. Pentru a rula această program, în linia de comandă introducem

driftnet -i eth0



Atunci cînd victima va naviga pe un site web, cu imagine, driftnet va capta tot traficul de imagine așa cum se arată în imaginea de mai jos.

Pentru a captura informațiile și datele de pe website, vom folosi program *urlsnarf*. În linia

de comandă tastăm

urlsnarf -i eth0

Atunci când victima va accesa un site web, atacatorul va ști adresa acestui site.