PenTest::DNS Spoofing

Beginner Tutorial v.1

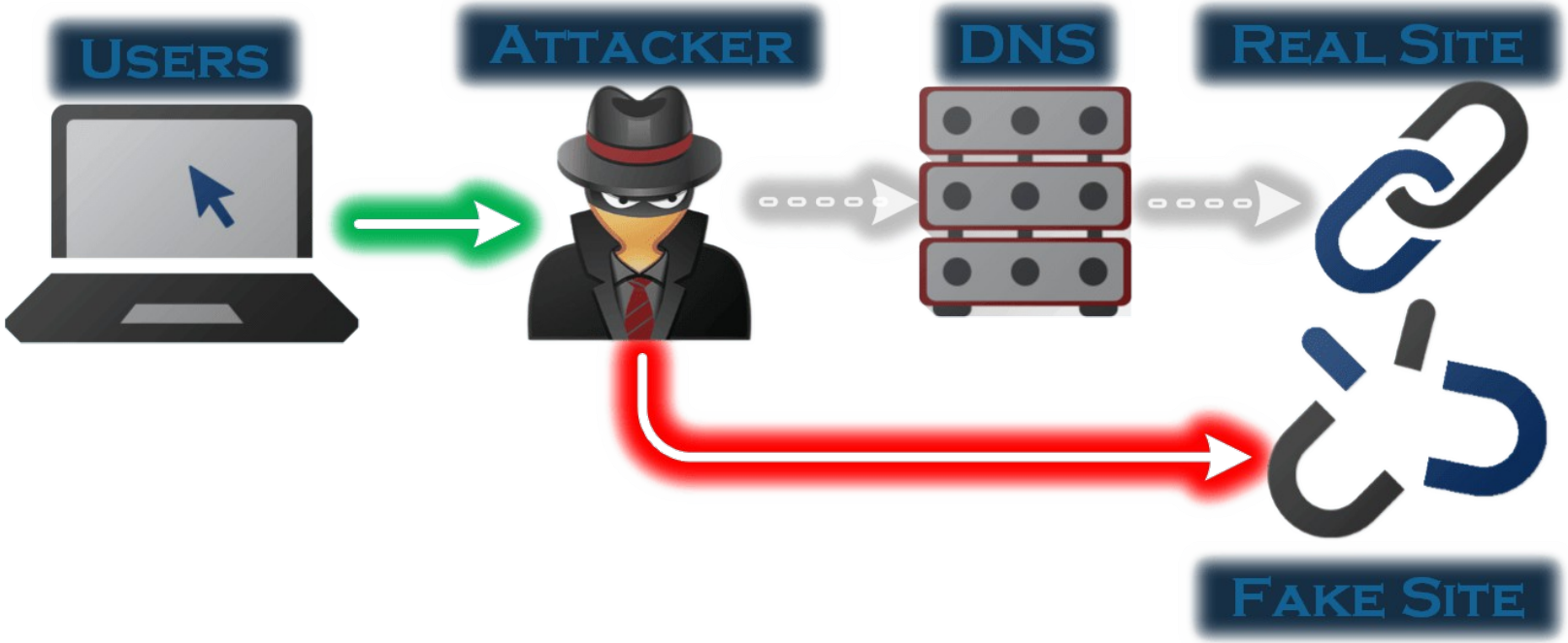
DNS Spoffing Tools

1. Ettercap
2. DNS Spoof Plugin Ettercap
3. Kali Linux

Sumber:csoonline

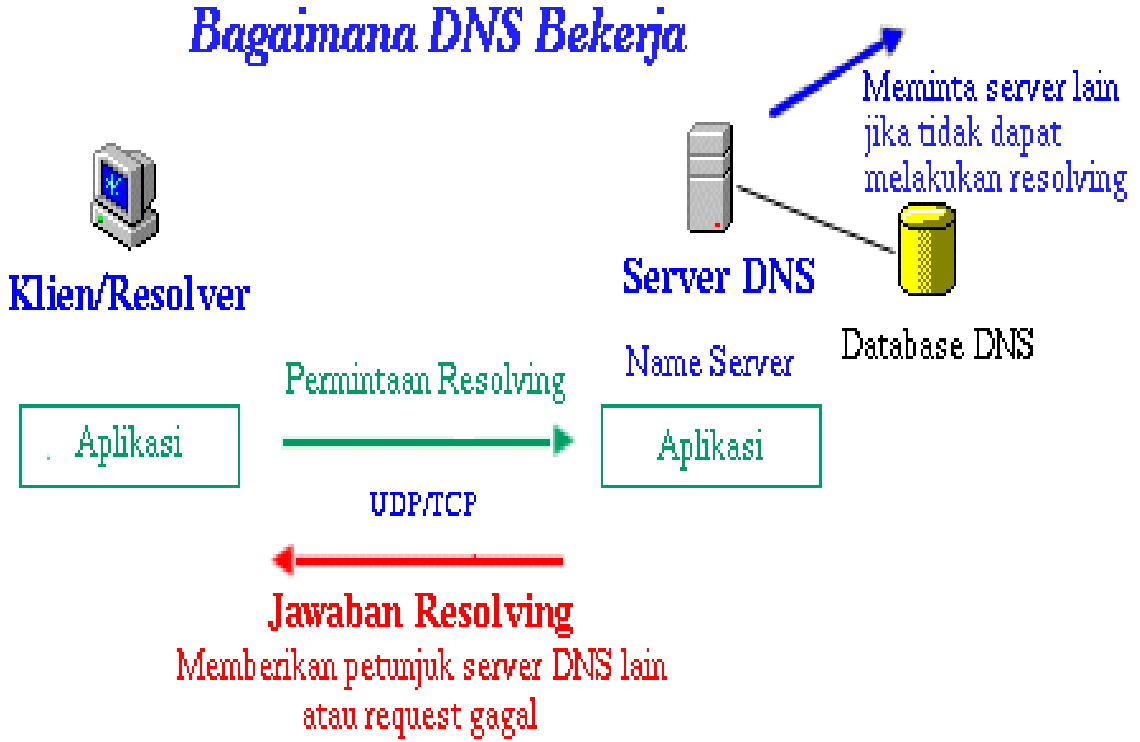
DNS Spoofing

DNS Spoofing adalah salah satu metode hacking Man In The Middle Attack (MITM). Hampir sama konsepnya dengan ARP Spoofing, tapi yang membedakan adalah Attacker akan memalsukan alamat IP dari sebuah domain.



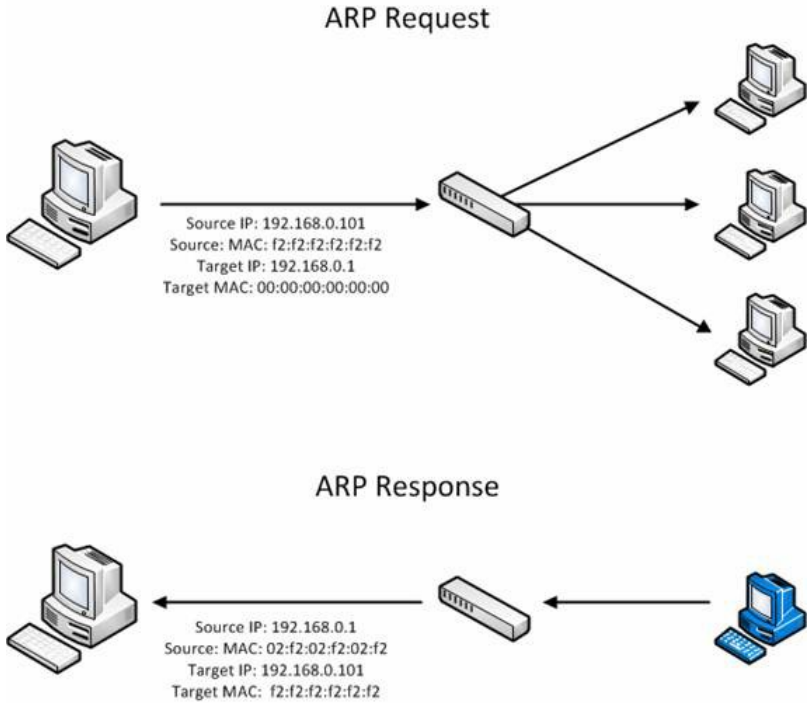
DNS ???

DNS adalah Domain Name Server, yaitu server yang digunakan untuk mengetahui IP Address suatu host lewat host name-nya. Dalam dunia internet, komputer berkomunikasi satu sama lain dengan mengenali IP Address-nya. Namun bagi manusia tidak mungkin menghafalkan IP address tersebut, manusia lebih mudah mengingat kata-kata seperti www.yahoo.com, www.google.com, atau www.facebook.com. DNS berfungsi untuk mengkonversi nama yang bisa terbaca oleh manusia ke dalam IP addresshost yang bersangkutan untuk dapat dilakukan komunikasi.



ARP

Address Resolution Protocol disingkat ARP adalah sebuah protokol dalam TCP/IP Protocol Suite yang bertanggungjawab dalam melakukan resolusi alamat IP ke dalam alamat Media Access Control (MAC Address).

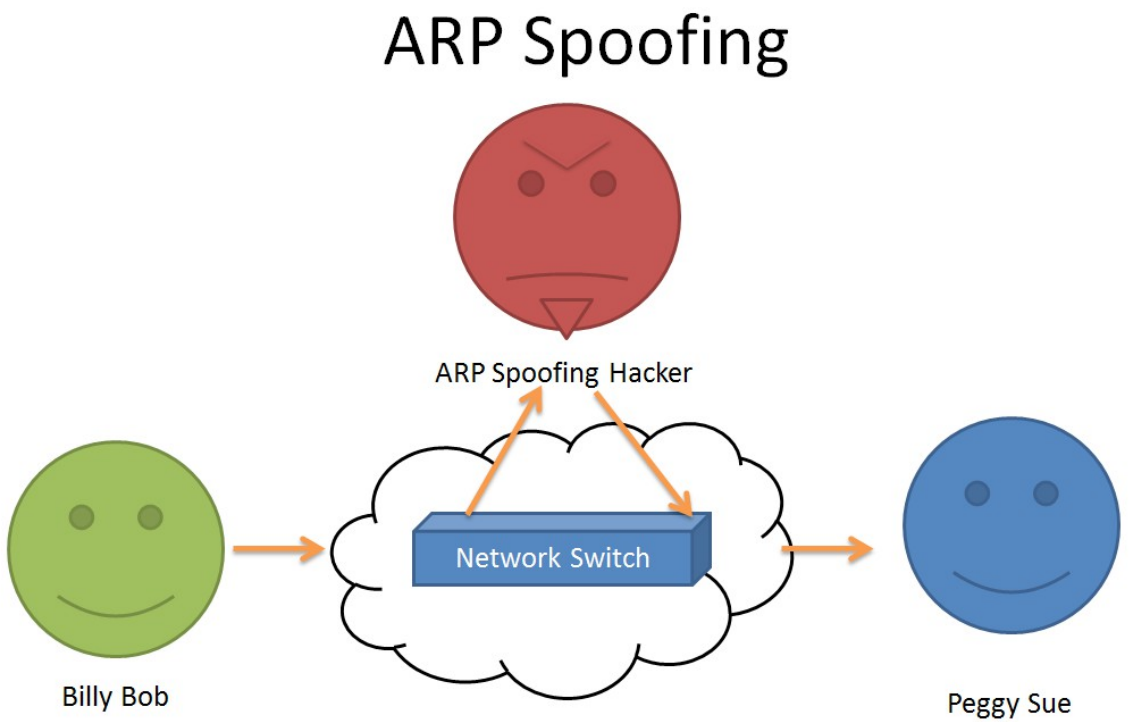


ARP

ARP adalah protocol yang berfungsi memetakan ipaddress menjadi MAC address. Dia adalah penghubung antara datalink layer dan ip layer pada TCP/IP. Semua komunikasi yang berbasis ethernet menggunakan protocol ARP ini. Pada dasarnya komputer atau device yang akan berkomunikasi pasti akan melakukan transaksi atau tukar menukar informasi terkait antara IP dan MAC address. Setiap transaksi akan disimpan di dalam cache OS Anda. Bisa dilihat menggunakan perintah arp (baik di Windows atau Linux).

ARP

Namun protocol ini punya kelemahan serius, karena setiap komputer bisa saja memberikan paket transaksi ARP yang dimanipulasi. Dengan merubah MAC address yang sesungguhnya. Kelemahan ini dimanfaatkan untuk jenis serangan ARP Poisoning atau ARP Spoofing atau Man In The Middle Attack. Siapa pun dapat menyadap bahkan meng-kill koneksi aktif pada LAN!



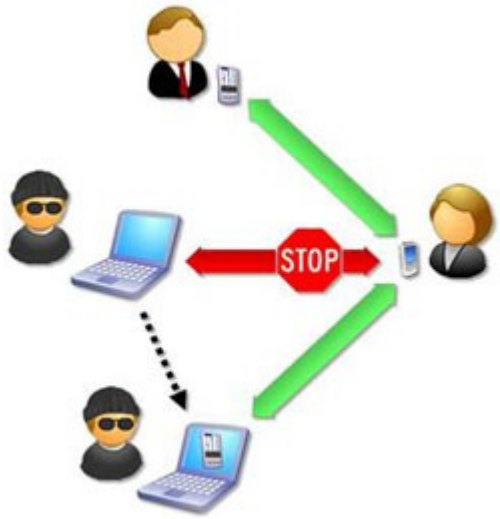
Ettercap

Ettercap memungkinkan membentuk serangan melawan protokol ARP dengan memposisikan diri sebagai “penengah, orang yang ditengah” dan, jika sudah berada pada posisi tersebut, maka akan memungkinkan untuk :

- menginfeksi, mengganti, menghapus data dalam sebuah koneksi
- melihat password pada protokol-protokol seperti FTP, HTTP, POP, SSH1, dan lain-lain.
- menyediakan SSL sertifikasi palsu dalam bagian HTTPS pada korban.
- dan lain-lain.

DNS Spoofing / MITM

Jadi ketika target melakukan request terhadap sebuah alamat domain dengan alamat IP A, dengan DNS Spoofing, oleh gateway request user tersebut akan di forward ke alamat IP palsu dari attacker.



Practice

Beginner Tutorial

Konfigurasi Jaringan

Konfigurasikan jaringan pada satu kelas yang sama, sebagai contoh:

Komputer	IP Address	MAC Address
Gateway	192.168.137.1	08:00:27:00:C0:1B
Target	192.168.137.8	08:00:27:21:6C:6F
Attacker	192.168.137.238	08:00:27:77:B5:07

Configurasi DNS Plugin

1. Modifikasi file konfigurasi DNS Spoofing
   Ketikkan perintah berikut di terminal:

```
1 root@bt:~# nano /usr/local/share/ettercap/etter.dns
```

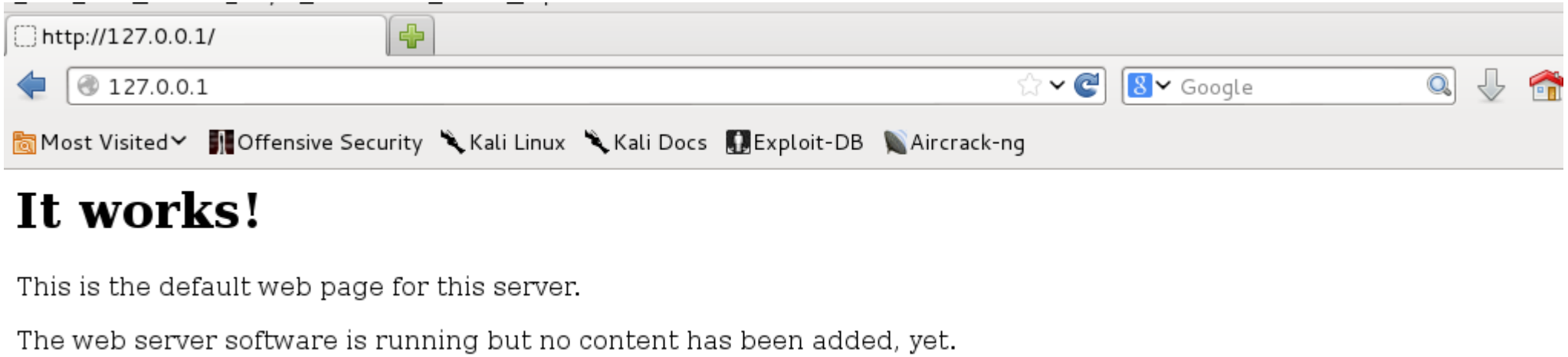
Sebagai contoh kita akan memalsukan alamat IP server dari domain detik.com. Geser scrool terminal Anda ke bawah hingga menemukan konfigurasi domain dari detik.com. Ubah alamat IP domain tersebut menjadi alamat mesin attacker Anda. Kemudian simpan konfigurasi tersebut dengan menekan tombol "Ctrl + O"

Menjalankan Service Apache

Ketikkan sintaks berikut pada konsol terminal:

```
1    root@bt:~# apache2ctl start
```

Lakukan percobaan dengan membuka aplikasi browser internet dan ketikkan alamat IP komputer attacker pada browser. Pastikan service apache di komputer attacker telah berjalan.



Menjalankan Aplikasi Ettercap

Dengan mengetikkan perintah berikut di terminal Kalilinux Anda:

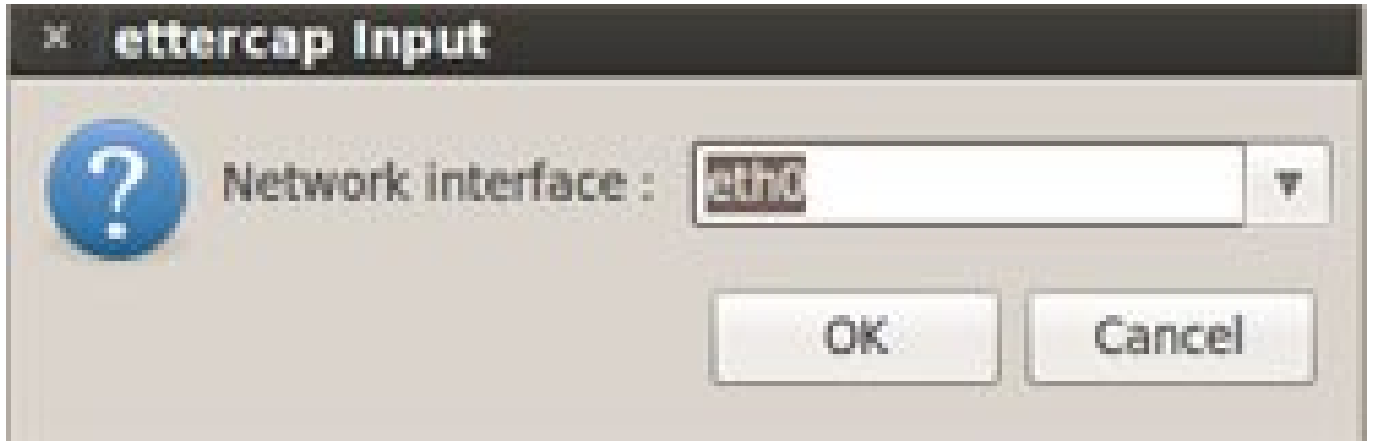
```
1    root@bt:~# ettercap -G
```

Maka akan muncul tampilan berikut:

Pemilihan Interface

4. Memilih interface LAN Card yang akan digunakan untuk melakukan DNS Spoofing pada komputer Attacker

Pada aplikasi Ettercap, pilih menu ***Sniff -> Unified Sniffing*** , lalu akan muncul kotak dialog seperti gambar di bawah. Jika menggunakan ethernet card pilih interface eth0, jika menggunakan wireless network pilih wlan0, klik tombol Ok untuk memilih.



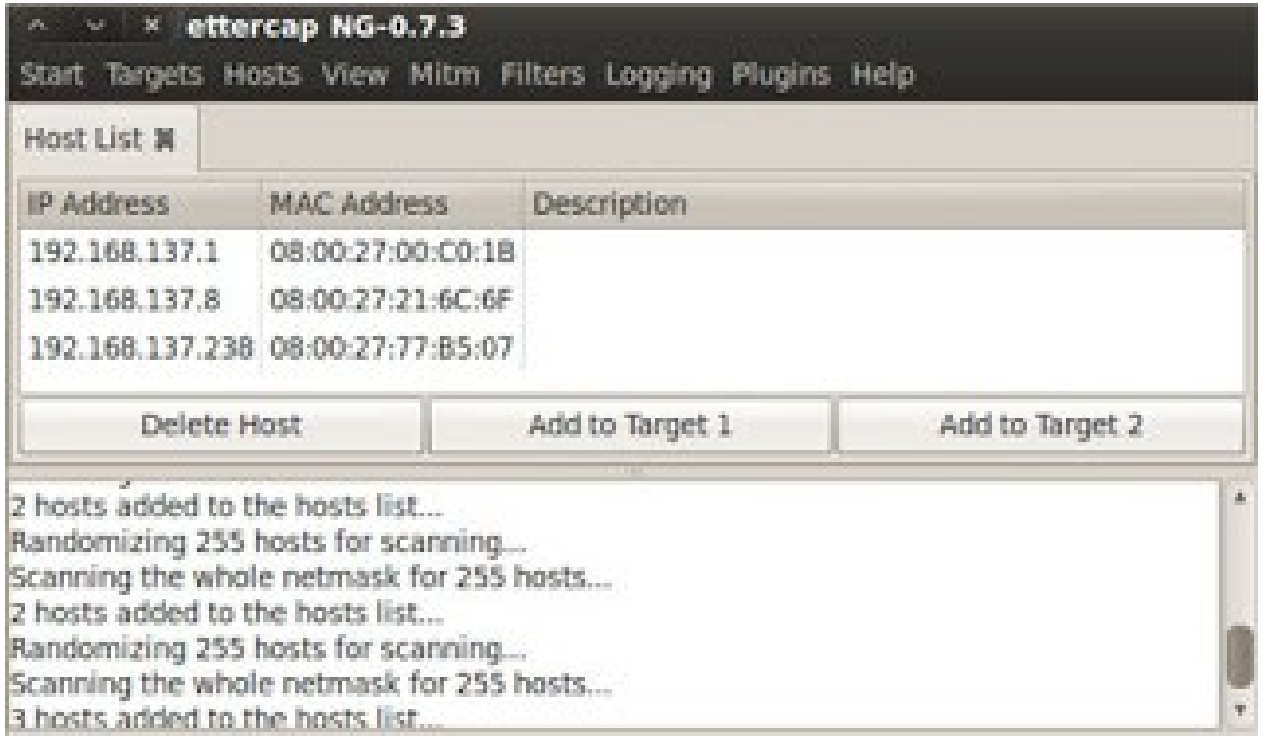
Scan Host / Target

Scan host komputer target, gateway, dan komputer attacker

Yaitu dengan memilih ***Host -> Scan for host***, maka Ettercap akan melakukan scanning komputer mana saja yang aktif mulai dari IP 192.168.137.0 sampai 192.168.137.255. Jumlah host yang aktif tergantung dari jumlah komputer yang ada pada satu jaringan tersebut. Pada jaringan virtual terdapat 3 buah komputer, maka ettercap akan mendeteksi 3 buah komputer yang aktif, seperti gambar di bawah ini.

Melihat daftar target / hasil scan host

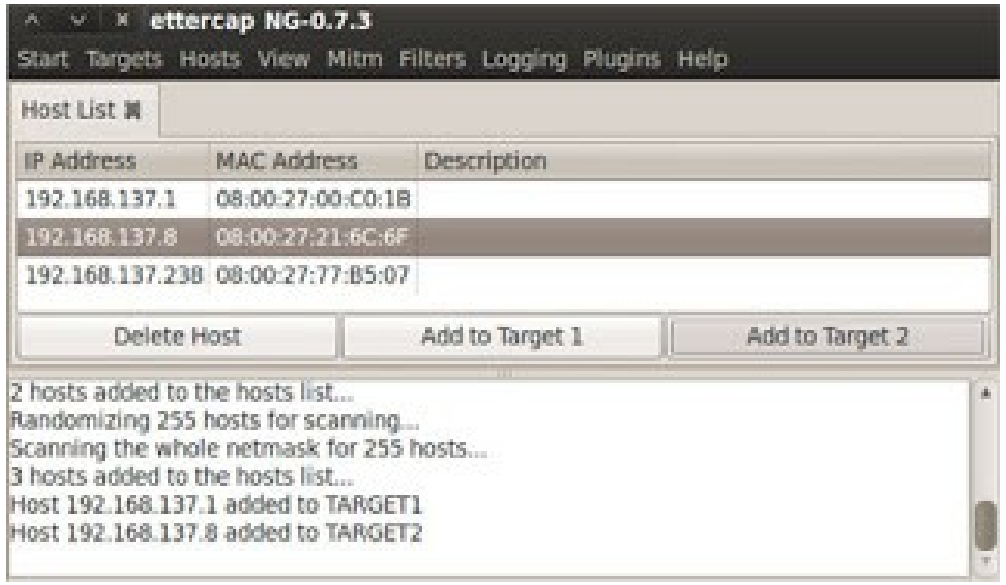
Pilih menu ***Hosts -> Hosts List,*** maka akan tampilan seperti berikut:



Memilih target yang akan diserang

Seperti telah diketahui sebelumnya bahwa komputer gateway memiliki IP 192.168.137.1, klik sekali pada IP komputer gateway dari daftar list hosts hasil scan sebelumnya, kemudian klik tombol "**Add to Target 1**".

Lakukan cara yang sama untuk komputer target dengan IP 192.168.137.8 dan klik tombol "**Add to Target 2**“

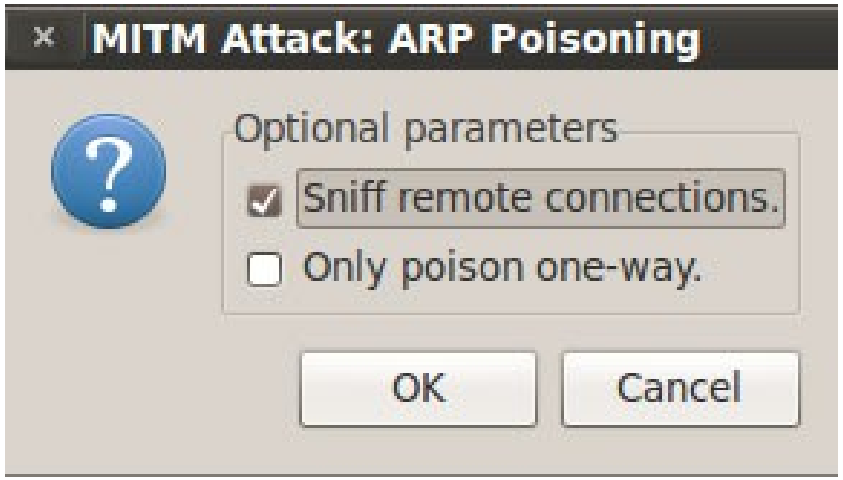


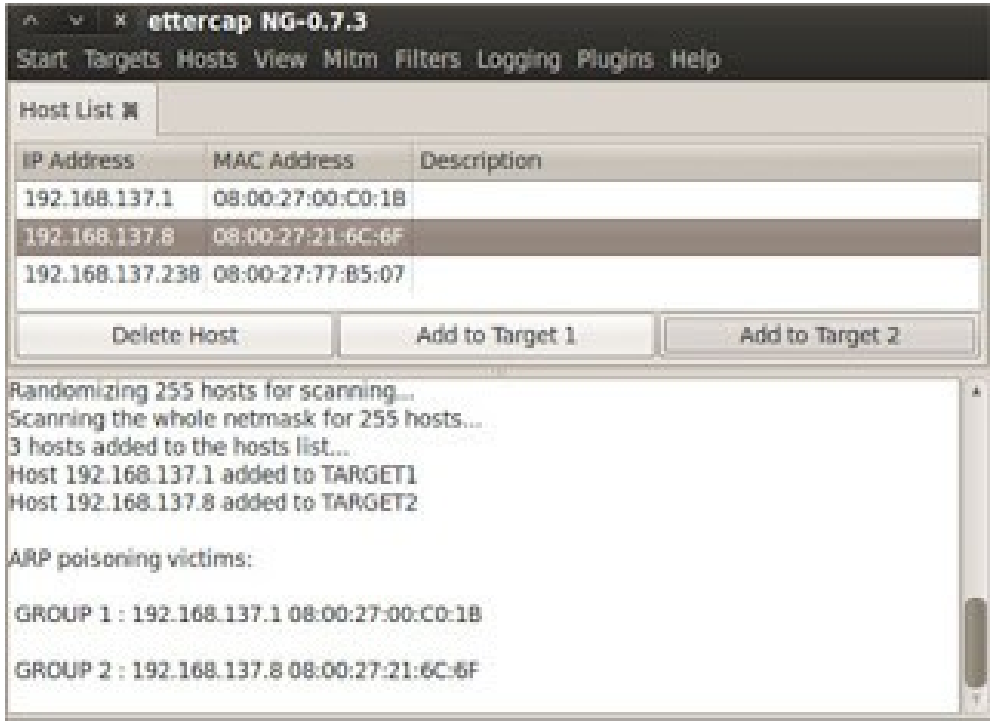
Mengaktifkan Plugin DNS Spoofing

pada menu aplikasi Ettercap, Plugins -> Manage Plugins -> DNS Spoof (klik 2 kali, sehingga muncul report 'DNS Spoofing Activating dns_spoof plugin...')

ARP Spoofing

Melakukan ARP Spoofing dengan memilih menu **Mitm -> ARP poisoning**, sehingga akan muncul kotak dialog seperti gambar di bawah, kemudian centang pilihan **"Sniff remote connections",** lalu klik tombol Ok. Maka aplikasi ettercap akan melakukan ARP Spoofing pada komputer target.





Mengaktifkan IP Forward

Lakukan set nilai Ip_forwarding menjadi 1 dengan cara mengetikkan sintaks berikut pada terminal:

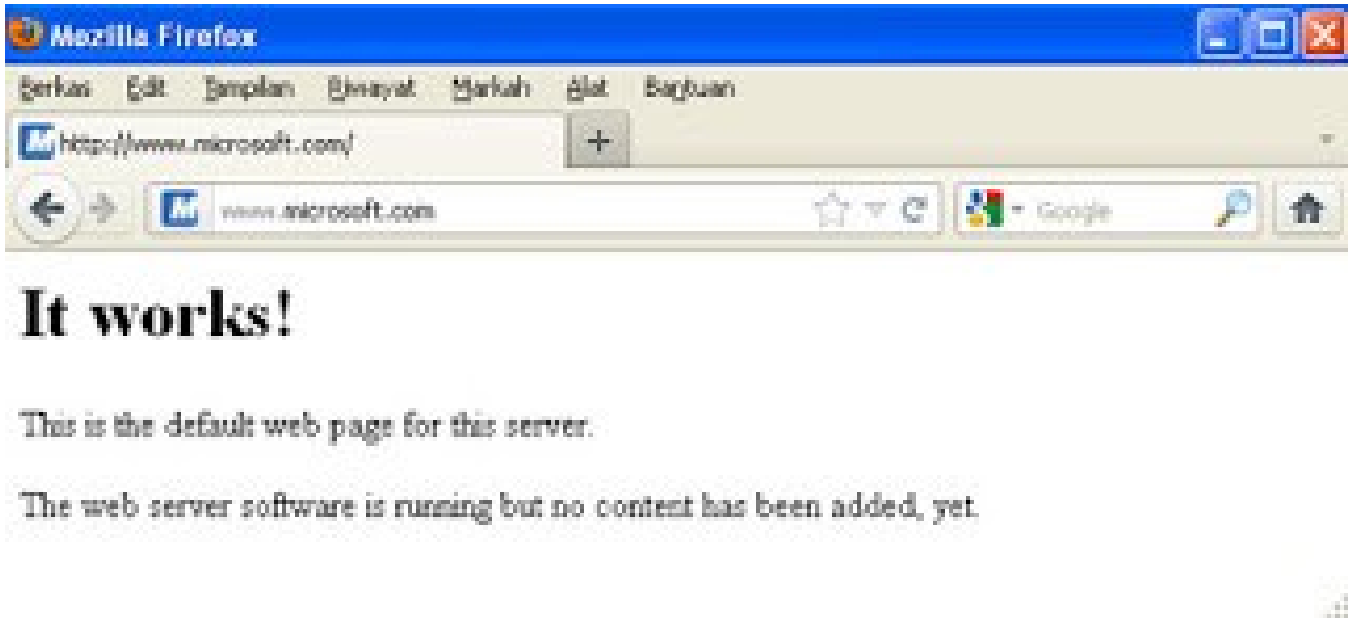
Hal ini bertujuan untuk melakukan forwarding paket dari host ke gateway.

```
1root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Start Sniffing

Memilih menu ***Start -> Start Sniffing***

Coba ketikkan alamat www.detik.com di browser komputer target, dan lihat apa yang terjadi



Ping Target / Host

Mencoba lakukan ping ke www.microsoft.com dari komputer target:

Ping detik.com

TERIMA KASIH