

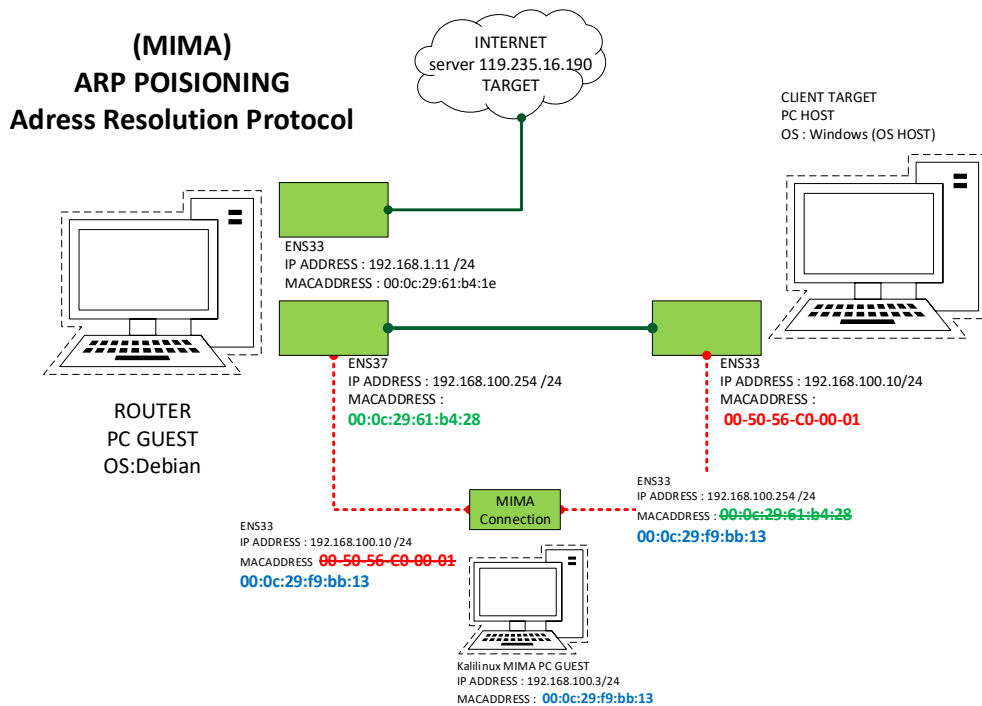
# Macam-macam serangan jaringan Komputer

Beberapa teknik yang dapat digunakan untuk pentest adalah :

## A. MAN IN The Midle Attack

*Man in the middle attack* (MITM) sama seperti menguping. Data dikirim dari titik A (komputer) ke titik B (server/website) dan penyerang bisa mendapatkan data tersebut dalam perjalanan antara poin A ke poin B atau dalam proses transmisi. Penyerang kemudian membuat diprogram untuk menguping pada transmisi, mencegat data yang berharga dan memanen data. Kadang-kadang data tersebut dimodifikasi dalam proses transmisi untuk mencoba untuk mengelabui pengguna akhir untuk membocorkan informasi sensitif, seperti detail *login*. Setelah pengguna tertipu oleh umpan, data dikumpulkan dari pengguna dan data asli kemudian diteruskan ke tujuan tanpa diubah.

Secara Konsep *A man in the middle attack* (MITM) , Memanfaatkan kelemahan dari ARP (Address Resolution Protocol), dimana tabel ARP tersebut akan di racuni, atau sering disebut ARP poisoning. Berikut ini skema konsep dari *A man in the middle attack* (MITM)



Gambar 1 Konsep MIMA

Jika Sebuah Komputer melakukan koneksi dengan komputer lain dalam jaringan, secara otomatis komputer tersebut akan melakukan broadcast dan hasilnya berupa tabel arp yang mencatat alamat fisik jaringan atau mac address. Sebagai contoh Jika Komputer *client* target yang memiliki mac address 00-50-56-c0-00-01 menghubungi router dengan mac address 00-0c-29-61-b4-28. Maka secara otomatis akan mencatat alamat mac dari router kedalam tabel ARP. Begitu pula sebaliknya.

Jika komputer Hacker dengan alamat mac address 00-0c-29-f9-bb-13 dan melakukan poisoning ARP maka komputer hacker akan mengubah dirinya seolah olah berada ditengah koneksi dengan mengatakan pada komputer router bahwa komputer client target adalah menggunakan mac 00-0c-29-f9-bb-13 dan mengatakan pada komputer client target bahwa mac address dari router adalah 00-0c-29-f9-bb-13 . hal tersebut yang menjadikan dirinya berada ditengah koneksi.

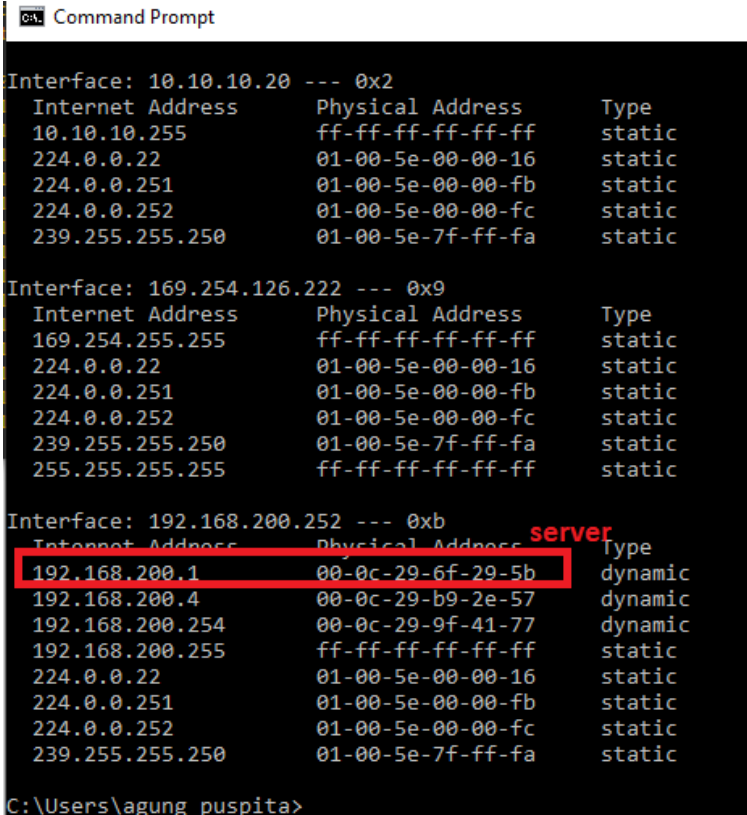
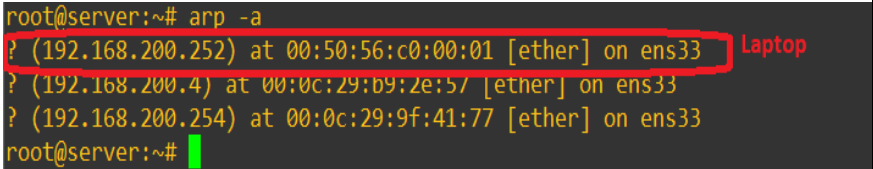
### 1. Praktek Ujicoba Man In The Midle Attack

Skenario Pengujian MIMA pada FTP server dan Web Server

- a. Lakukan koneksi dengan ping dari Laptop client / peserta ke server
- b. Lakukan poisoning terhadap Laptop peserta dan server Linux. Melalui Kalilinux dengan aplikasi ether cap
- c. Laptop peserta melakukan FTP ke server
- d. Lakukan proses Privilege Excalation mencakup kegiatan identifikasi dan password cracking terhadap akun pengguna FTP, dari Komputer Kalilinux
- e. Komputer target mengakses web server pada alamat server 202.180.21.17, dengan url lengkap http:// 202.180.21.17/administrator
- f. Lakukan login dengan username : admin dan password : admin123
- g. Lakukan proses Privilege Excalation mencakup kegiatan identifikasi dan password cracking terhadap akun pengguna web server dari Komputer Kalilinux

### 2. Langkah Kerja

No	Steps	Information
<b>Membuat Koneksi dari Laptop ke server</b>		
1.	Buat koneksi antara komputer	<ol style="list-style-type: none"> <li>1. Ping dari Laptop ke server</li> <li>2. Ping dari server ke laptop</li> <li>3. Ping dari kalilinux ke server</li> </ol>

		4. Ping dari Kalilinux ke laptop
2.	Melihat Tabel ARP sebelum proses poisoning	<p>5. Ketik: <b>arp -a</b> pada laptop melalui <i>command prompt</i> (catat hasil arp berupa <b>ip address</b> dan <b>mac address</b> dari <b>server</b> pada table laporan )</p>  <pre> C:\&gt; Command Prompt  Interface: 10.10.10.20 --- 0x2   Internet Address      Physical Address      Type   10.10.10.255          ff-ff-ff-ff-ff-ff    static   224.0.0.22            01-00-5e-00-00-16    static   224.0.0.251           01-00-5e-00-00-fb    static   224.0.0.252           01-00-5e-00-00-fc    static   239.255.255.250       01-00-5e-7f-ff-fa    static  Interface: 169.254.126.222 --- 0x9   Internet Address      Physical Address      Type   169.254.255.255       ff-ff-ff-ff-ff-ff    static   224.0.0.22            01-00-5e-00-00-16    static   224.0.0.251           01-00-5e-00-00-fb    static   224.0.0.252           01-00-5e-00-00-fc    static   239.255.255.250       01-00-5e-7f-ff-fa    static   255.255.255.255       ff-ff-ff-ff-ff-ff    static  Interface: 192.168.200.252 --- 0xb   Internet Address      Physical Address      Type   192.168.200.1         00-0c-29-6f-29-5b    dynamic   192.168.200.4         00-0c-29-b9-2e-57    dynamic   192.168.200.254       00-0c-29-9f-41-77    dynamic   192.168.200.255       ff-ff-ff-ff-ff-ff    static   224.0.0.22            01-00-5e-00-00-16    static   224.0.0.251           01-00-5e-00-00-fb    static   224.0.0.252           01-00-5e-00-00-fc    static   239.255.255.250       01-00-5e-7f-ff-fa    static  C:\Users\agung_puspita&gt; </pre> <p>6. Ketik: <b>arp -a</b> pada server debian (catat hasil arp berupa <b>ip address</b> dan <b>mac address</b> dari <b>laptop</b> pada table laporan )</p>  <pre> root@server:~# arp -a ? (192.168.200.252) at 00:50:56:c0:00:01 [ether] on ens33 ? (192.168.200.4) at 00:0c:29:b9:2e:57 [ether] on ens33 ? (192.168.200.254) at 00:0c:29:9f:41:77 [ether] on ens33 root@server:~# </pre> <p>7. Ketik <b>arp -a</b> pada Kalilinux (catat hasil arp berupa <b>ip address</b> dan <b>mac address</b> dari <b>laptop dan server</b> pada table laporan )</p>

```

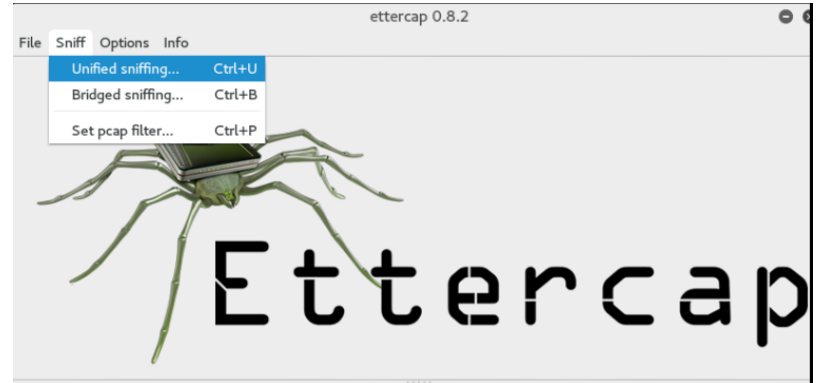
root@kali:~# arp -a
? (192.168.200.1) at 00:0c:29:6f:29:5b [ether] on eth0 server
gateway (192.168.200.254) at 00:0c:29:9f:41:77 [ether] on eth0
? (192.168.200.252) at 00:50:56:c0:00:01 [ether] on eth0 laptop
? (192.168.35.15) at 00:0c:29:9f:41:77 [ether] on eth0
root@kali:~#

```

3. Melakukan Man In Midle Attack melalui Kalilinux

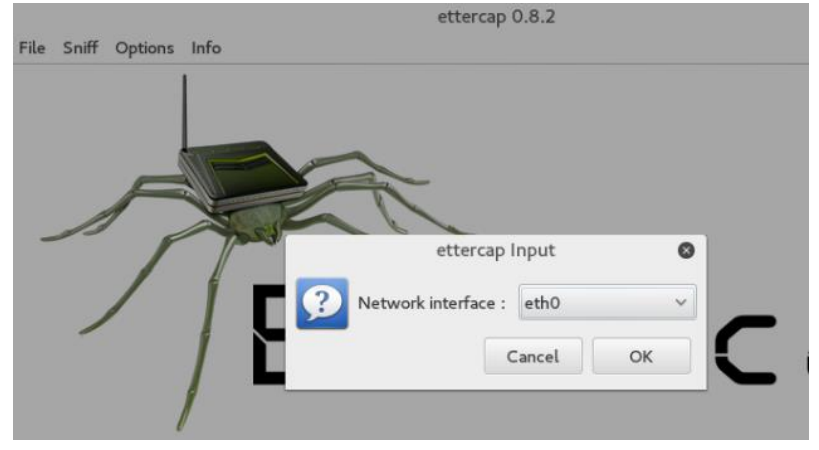
1. Pada kalilinux, pilih *application>sniffing&spoofing>ettercap-gui*
2. Pada ethercap pilih tab menu :

*Sniff>unifield sniffing..*



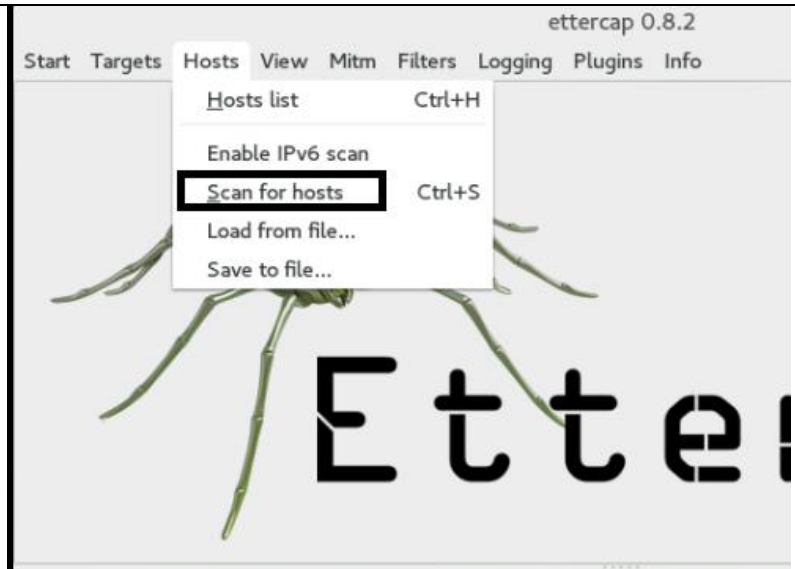
3. .pada ethercap input, pilih interface:

*eth0*

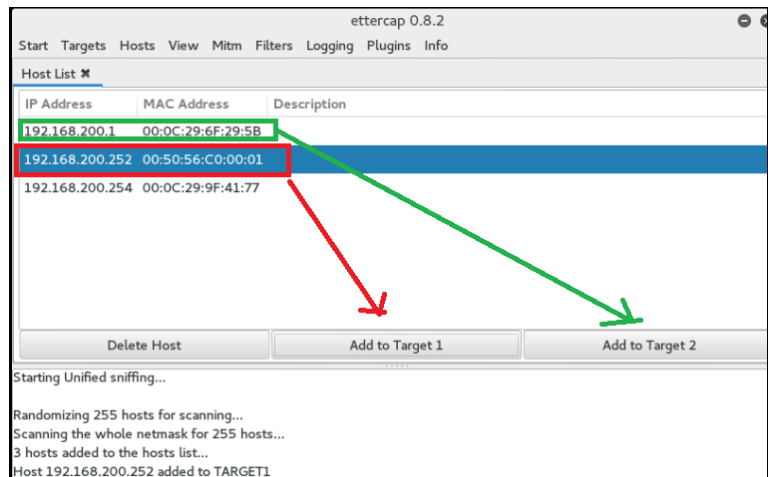


4. Pilih tab menu host:

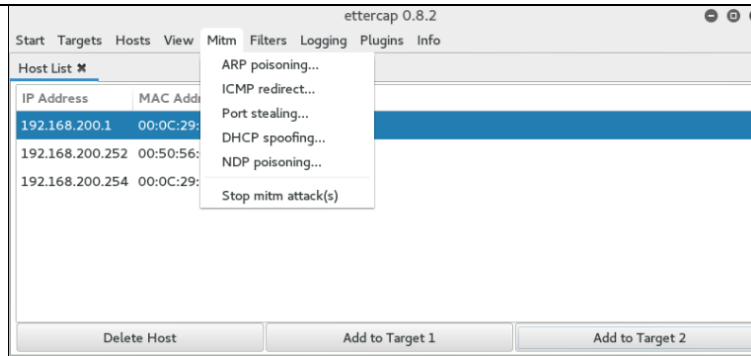
*Scan for host*



5. Pada **host list**, terdapat 2 alamat ip dan mac address hasil scan
  - a) Klik untuk pilih ip computer target dan klik add to target 1  
(memasukan laptop kedalam target1.)
  - b) Klik untuk pilih ip server dan klik add to target 2  
(memasukan pc router kedalam target2)



6. Pilih tab menu mitm >ARP Poisoning



7. Pada optimal parameter pilih  
Beri tanda check pada “sniff remote connection”

4. Melihat Tabel ARP setelah proses poisoning

1. Ketik: **arp -a** pada laptop melalui *command prompt* (catat hasil arp berupa **ip address** dan **mac address** dari server pada table laporan )

```
Interface: 192.168.200.252 --- 0xb
Internet Address      Physical Address      Type
192.168.200.1         00-0c-29-b9-2e-57    dynamic
192.168.200.4         00-0c-29-b9-2e-57    dynamic
192.168.200.254       00-0c-29-9f-41-77    dynamic
192.168.200.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-10    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
C:\Users\agung puspita>
```

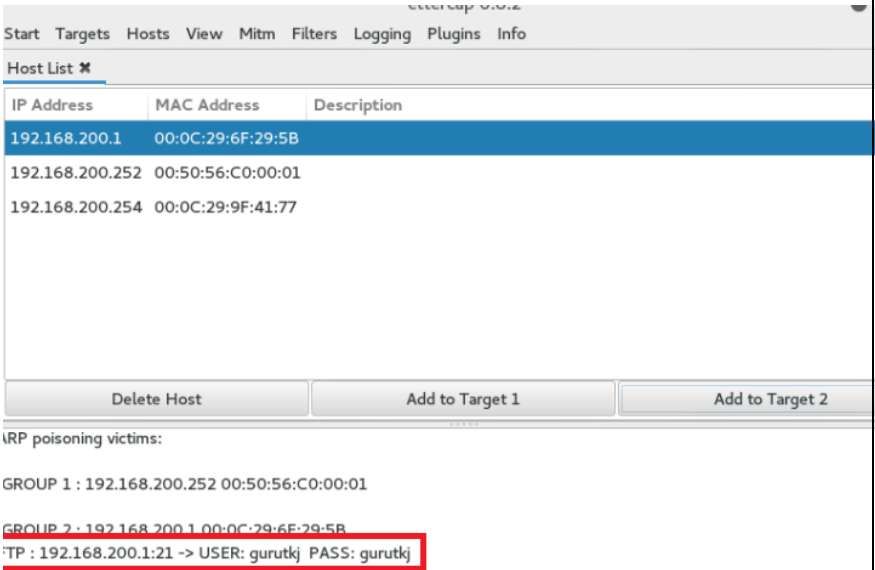
**IP server namun Mac : kalilinux**

2. Ketik: **arp -a** pada server debian (catat hasil arp berupa **ip address** dan **mac address** dari laptop pada table laporan )

```
? (192.168.200.4) at 00:0c:29:b9:2e:57 [ether] on ens33
? (192.168.200.254) at 00:0c:29:9f:41:77 [ether] on ens33
root@server:~# arp a
a: Unknown host
root@server:~# arp -a
? (192.168.200.252) at 00:0c:29:b9:2e:57 [ether] on ens33
? (192.168.200.4) at 00:0c:29:b9:2e:57 [ether] on ens33
? (192.168.200.254) at 00:0c:29:9f:41:77 [ether] on ens33
root@server:~#
```

**IP Laptop Mac address Kalilinux**

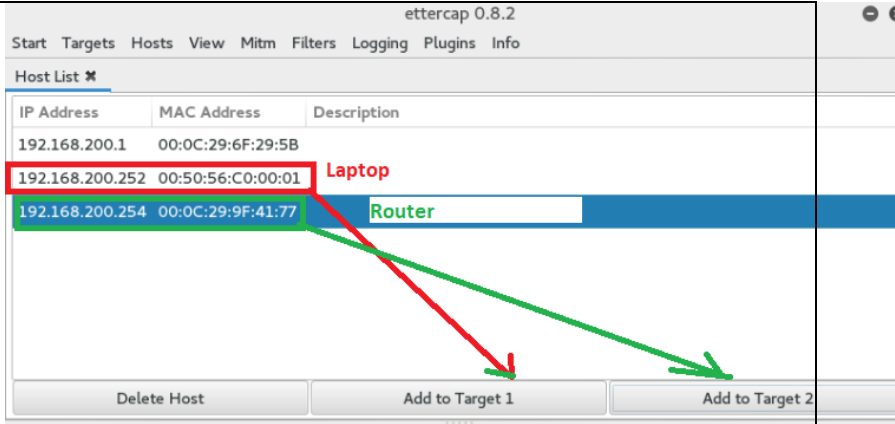
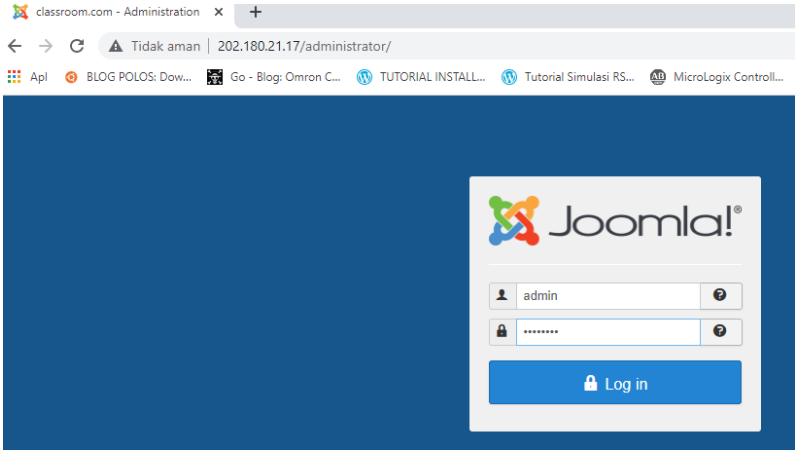
3. Ketik arp -a pada Kalilinux

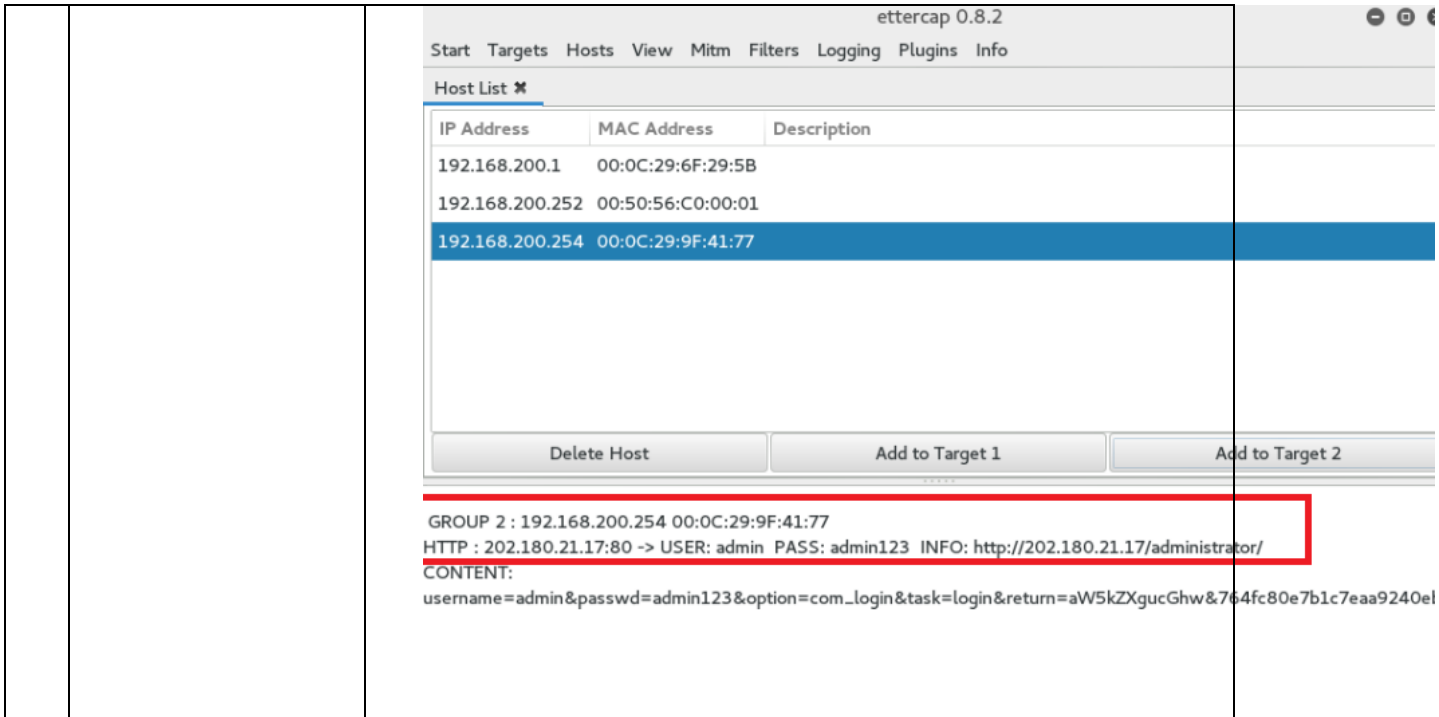
		(catat hasil arp berupa <b>ip address</b> dan <b>mac address</b> dari <b>laptop dan pc server</b> pada table laporan )												
5.	Pengujian password FTP	<p>Dari laptop , coba lakukan FTP ke router melalui perintah pada command. Pada contoh yg diberikan</p> <pre>C:\Users\agung puspita&gt;ftp 192.168.xx.2 Connected to 192.168.xx.2. 220 ProFTPD Server (Debian) [::ffff:192.168.xx.2] 200 UTF8 set to on User (192.168.xx.2:(none)): gurutkj 331 Password required for gurutkj Password: (masukan password contoh guru123) 230 User guru logged in ftp&gt;</pre> <p>(printsreen /capture hasilnya dan lampirkan pada table laporan)</p>												
6.	Pada Komputer Kalilinux	<p>Lihat pada ethercap username password FTP yang terekam (capture gambar dan lampirkan pada table laporan)</p>  <p>The screenshot shows the ethercap interface with a 'Host List' table containing the following data:</p> <table border="1"> <thead> <tr> <th>IP Address</th> <th>MAC Address</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>192.168.200.1</td> <td>00:0C:29:6F:29:5B</td> <td></td> </tr> <tr> <td>192.168.200.252</td> <td>00:50:56:C0:00:01</td> <td></td> </tr> <tr> <td>192.168.200.254</td> <td>00:0C:29:9F:41:77</td> <td></td> </tr> </tbody> </table> <p>Below the table, there are buttons for 'Delete Host', 'Add to Target 1', and 'Add to Target 2'. Underneath, the 'ARP poisoning victims' section lists:</p> <ul style="list-style-type: none"> <li>GROUP 1 : 192.168.200.252 00:50:56:C0:00:01</li> <li>GROUP 2 : 192.168.200.1 00:0C:29:6E:29:5B</li> </ul> <p>A red box highlights the following line: TP : 192.168.200.1:21 -&gt; USER: gurutkj PASS: gurutkj</p>	IP Address	MAC Address	Description	192.168.200.1	00:0C:29:6F:29:5B		192.168.200.252	00:50:56:C0:00:01		192.168.200.254	00:0C:29:9F:41:77	
IP Address	MAC Address	Description												
192.168.200.1	00:0C:29:6F:29:5B													
192.168.200.252	00:50:56:C0:00:01													
192.168.200.254	00:0C:29:9F:41:77													

### Man In The Middle Attack Melihat Password Web Server

Untuk menguji MIMA, terhadap pengguna yang mengakses situs web diluar (internet/external network), maka ARP poisoning dilakukan terhadap Laptop pengguna dan Router. Untuk uji

coba kali ini disediakan sebuah halaman web dengan alamat url : <http://202.180.21.17/administrator>, gunakan username : admin dan password admin 23

<p>7. Lakukan langkah yang sama untuk poisoning Laptop Pengguna dan Router ens34 (internal network)</p>	 <p>Randomizing 255 hosts for scanning... Scanning the whole netmask for 255 hosts... 3 hosts added to the hosts list... Host 192.168.200.252 added to TARGET1 Host 192.168.200.254 added to TARGET2</p>
<p>8. Pengujian password Web Server/HTTP server</p>	<p>1. Dari PC host , coba akses http server 119.235.16.190, dengan url lengkap <a href="http://202.180.21.17/administrator">http://202.180.21.17/administrator</a></p> <p>2. Masukkan <b>username : admin</b> dan <b>password : admin123</b> (Capture dan lampirkan pada table laporan)</p> 
<p>9. Pada Komputer Kalilinux</p>	<p>Lihat pada ethercap username password web server yang terekam</p>



## B. DNS Spofing

Masih Menggunakan ARP Poisoning, DNS Spofing digunakan untuk mengalihkan nama DNS, kedalam sebuah alamat IP address atau DNS dari sebuah halaman web palsu, sehingga tanpa disadari pengguna akan memasukan username dan account pada sebuah situs dengan alamat DNS yang telah disediakan. Untuk Ujicoba kali ini kita akan mencoba untuk mengalihkan DNS lapto pengguna yang memangil google kealamat situs web dalam jaringan lokal kita yang berada dalam server lokal kita

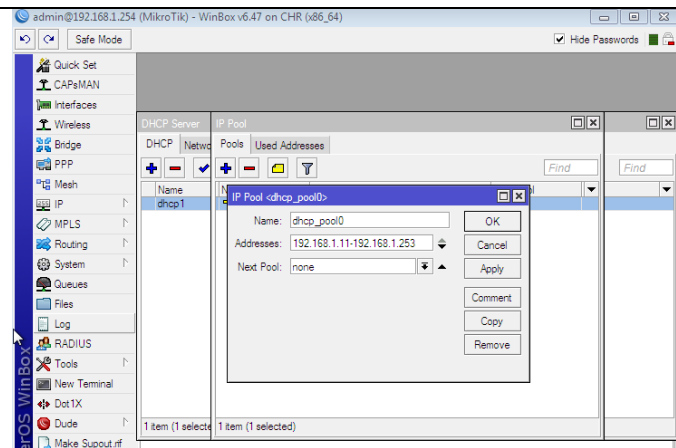
10.	Masih dalam proses meracuni (poisoning Router dan Laptop)	<p>Pilih menu plugin pada ettercap</p> <p>2x cklik pada DNS Spoofing sampai muncul tanda *</p> <p>ettercap 0.8.2</p> <p>Start Targets Hosts View Mitm Filters Logging Plugins Info</p> <p>Host List ✖      Plugins ✖</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Version</th> <th>Info</th> </tr> </thead> <tbody> <tr> <td>arp_cop</td> <td>1.1</td> <td>Report suspicious ARP activity</td> </tr> <tr> <td>autoadd</td> <td>1.2</td> <td>Automatically add new victims in the target range</td> </tr> <tr> <td>chk_poison</td> <td>1.1</td> <td>Check if the poisoning had success</td> </tr> <tr style="background-color: #0070C0; color: white;"> <td>dns_spoof</td> <td>1.2</td> <td>Sends spoofed dns replies</td> </tr> <tr> <td>dos_attack</td> <td>1.0</td> <td>Run a d.o.s. attack against an IP address</td> </tr> <tr> <td>dummy</td> <td>3.0</td> <td>A plugin template (for developers)</td> </tr> <tr> <td>find_conn</td> <td>1.0</td> <td>Search connections on a switched LAN</td> </tr> <tr> <td>find_ettercap</td> <td>2.0</td> <td>Try to find ettercap activity</td> </tr> <tr> <td>find_in</td> <td>1.0</td> <td>Search an unused IP address in the subnet</td> </tr> </tbody> </table>	Name	Version	Info	arp_cop	1.1	Report suspicious ARP activity	autoadd	1.2	Automatically add new victims in the target range	chk_poison	1.1	Check if the poisoning had success	dns_spoof	1.2	Sends spoofed dns replies	dos_attack	1.0	Run a d.o.s. attack against an IP address	dummy	3.0	A plugin template (for developers)	find_conn	1.0	Search connections on a switched LAN	find_ettercap	2.0	Try to find ettercap activity	find_in	1.0	Search an unused IP address in the subnet
Name	Version	Info																														
arp_cop	1.1	Report suspicious ARP activity																														
autoadd	1.2	Automatically add new victims in the target range																														
chk_poison	1.1	Check if the poisoning had success																														
dns_spoof	1.2	Sends spoofed dns replies																														
dos_attack	1.0	Run a d.o.s. attack against an IP address																														
dummy	3.0	A plugin template (for developers)																														
find_conn	1.0	Search connections on a switched LAN																														
find_ettercap	2.0	Try to find ettercap activity																														
find_in	1.0	Search an unused IP address in the subnet																														

11.	Konfigurasi file etter.dns	<ul style="list-style-type: none"> <li>• nano /etc/ettercap/etter.dns</li> <li>• untuk contoh cari isi text dengan nama google.com, dengan cara ctr+w dan ketik google</li> <li>• ubah menjadi  <pre>google.com      A  192.168.200.1 *.google.com    A  192.168.200.1 www.google.com  PTR 192.168.200.1</pre> </li> </ul> 
12.	Dari Laptop Pengguna , gunakan browser untuk membuka google.com	<p>Cek browser access google.com</p>  <p>Hasil dari alamat google.com</p>  <p><b>Halaman web server dari server.debian</b></p>

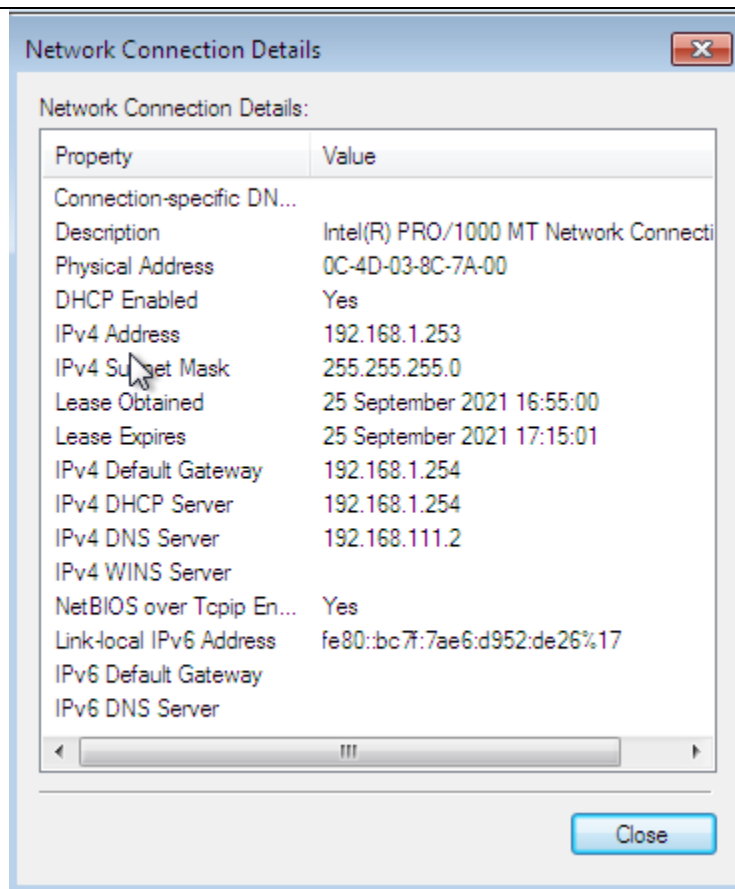
### C. DHCP spoofing

Ettercap, banyak memiliki fungsi exploite dalam jaringan selain ARP poisoning ,MIMA, DNS Spoofing terdapat juga jenis serangan yaitu DHCP, spoofing, dimana Ettercap akan memberikan alamat DHCP palsu kepada komputer client dalam hal ini adalah laptop pengguna, sehingga dapat melumpuhkan koneksi jaringan karena tidak mendapatkan layanan DHCP server.

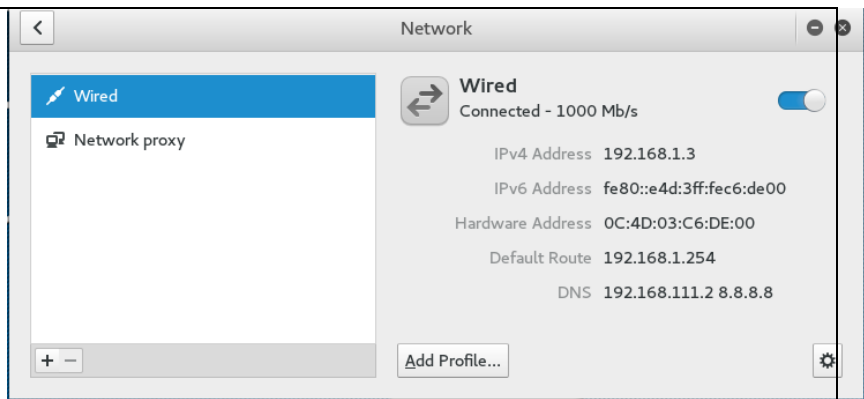
13. Tampilkan menggunakan winbox ip pool



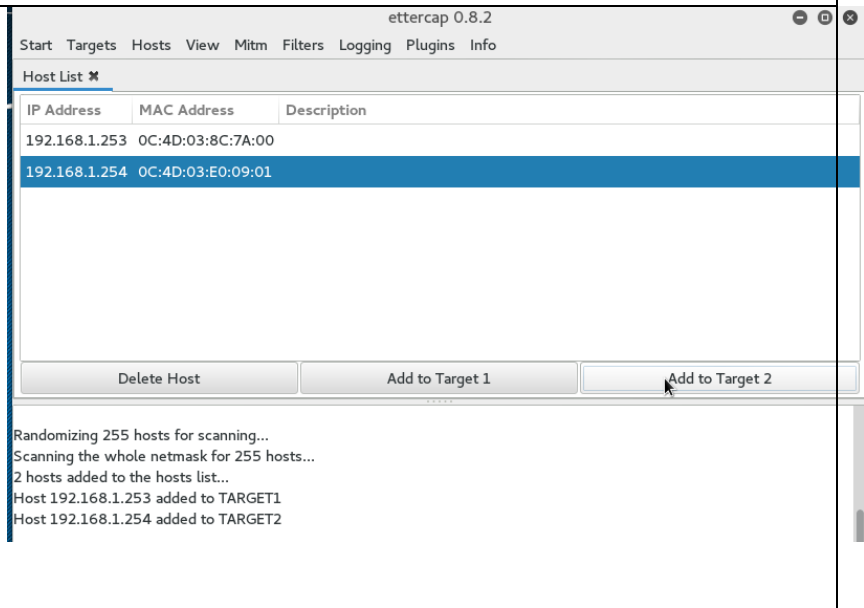
14. Tampilkan IP laptop pengguna



15. Tampilkan ip address kalilinux



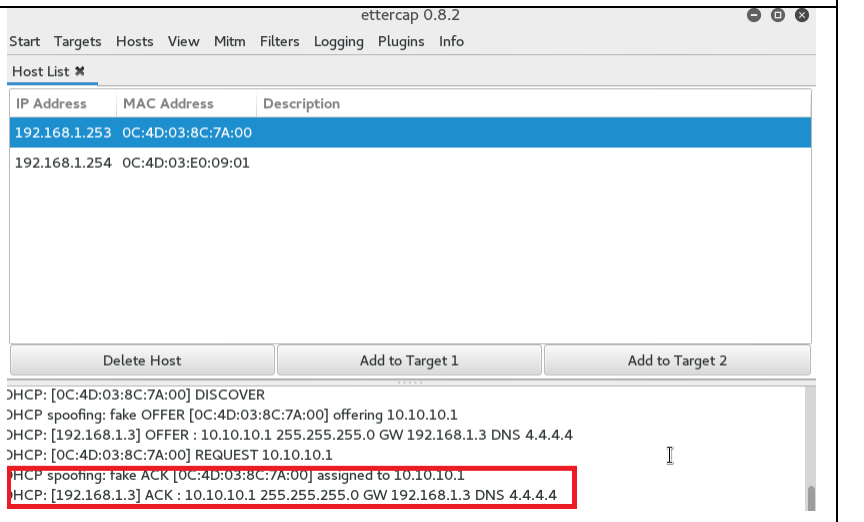
16. Masih menggunakan ettercap, lakukan poisoning terhadap router dan laptop pengguna



17. Pada menu MITM pilih DHCP Spoofing dan isi dhcp pool yang diinginkan

Contoh :  
Ip pool : 10.10.10.1-10.10.10.254  
Netmask : 255.255.255.0  
Dns : 4.4.4.4

18. Hasil pada ettercap user terlihat renew ip address



19. Pada Laptop  
Pengguna

