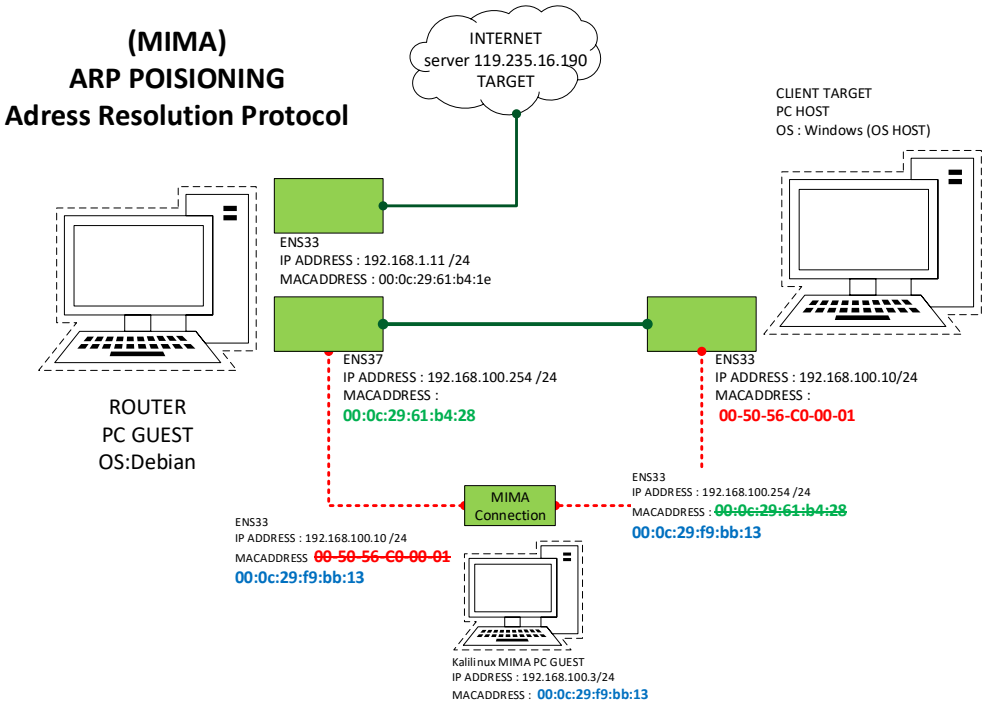
Macam-macam serangan jaringan Komputer

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 perjalan 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 poisioning. Berikut ini skema konsep dari *A man in the middle attack* (MITM)



Gambar 1 Konsep MIMA

Jika Sebuah Komputer menlakukan koneksi dengan komputer lain dalam jaringan, secara otomtis komputer teesebut akan melakukan brodcast dan hasilnya berupa tabel arp yang mencapat alamat fisik jaringangan 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 adress 00-0c-29-f9-bb-13 dan melakukan poisioning 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 adress dari router adalah 00-0c-29-f9-bb-13 . hal tersebut yang menjadikan dirinya berada ditengah koneksi.

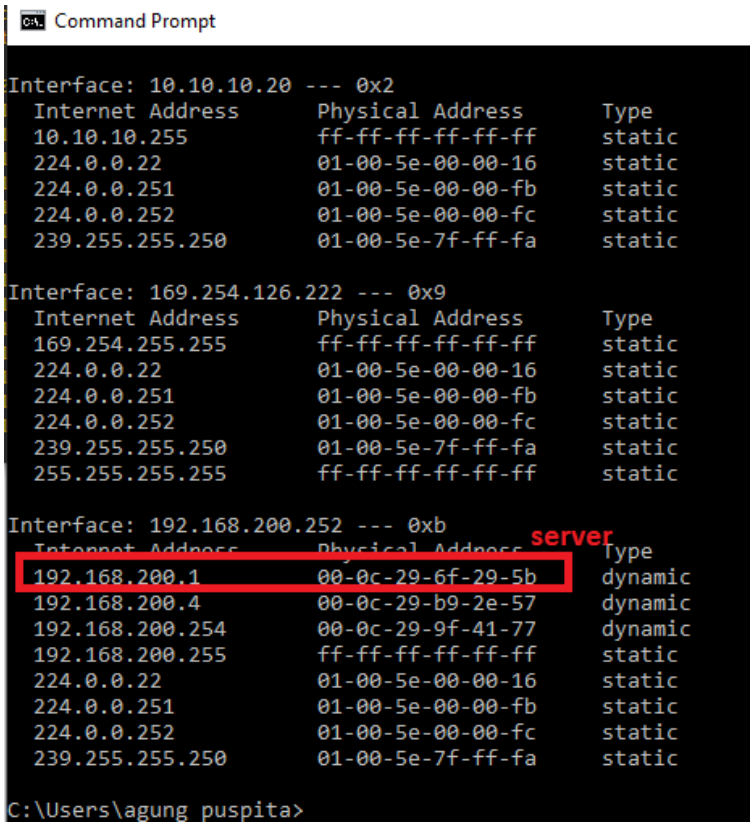
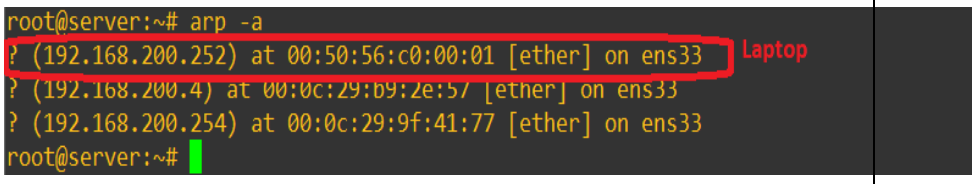
1. Praktek Ujicoba Man In The Midle Attack

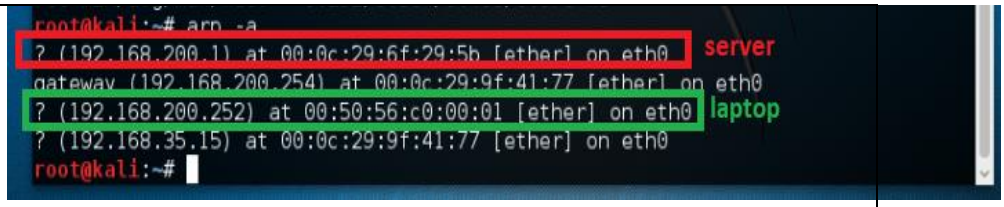
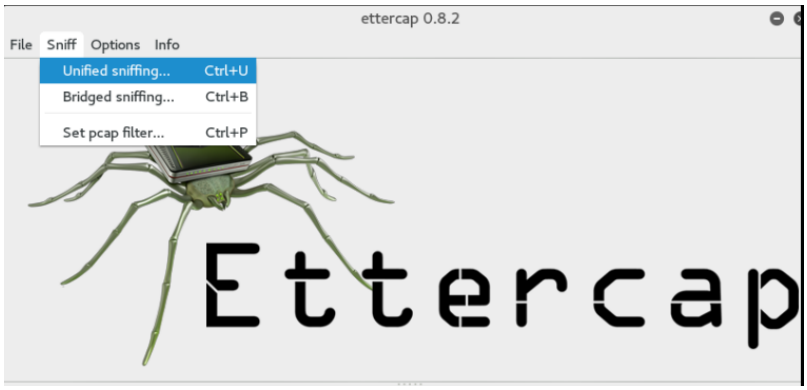
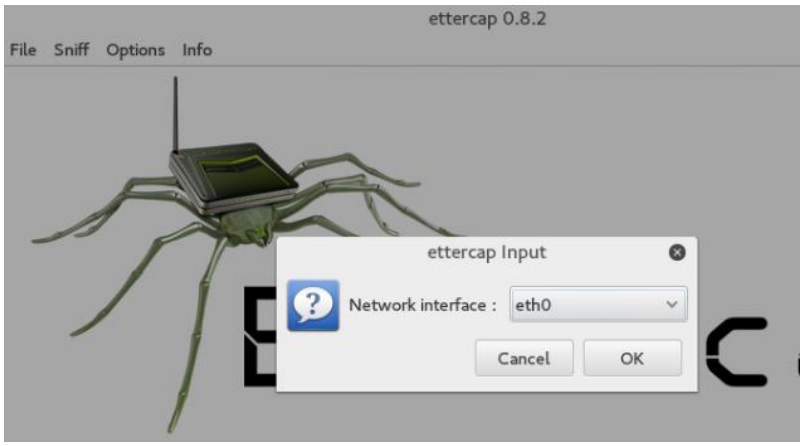
Sekenario Pengujian MIMA pada FTP server dan Web Server

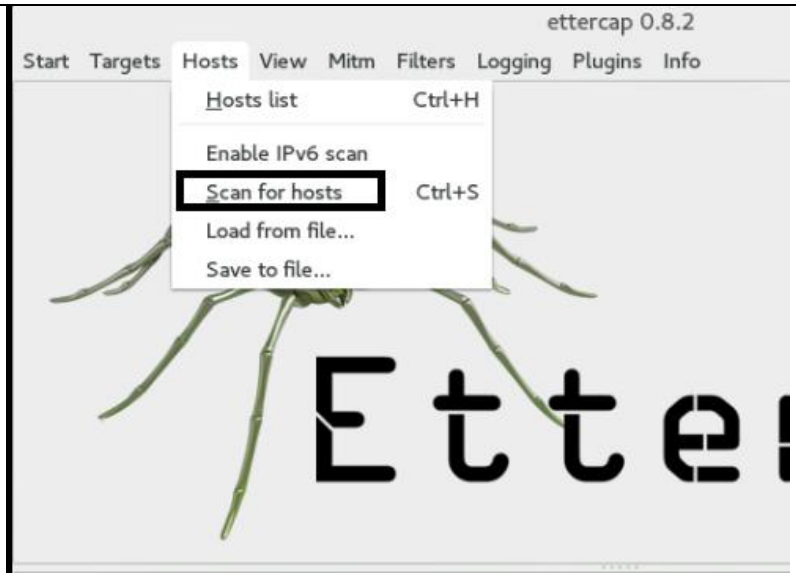
a. Lakukan koneksi dengan ping dari Laptop client / peserta ke server
b. Lakukan poisioning terhadap Laptop peserta dan server Linux. Melalui Kalilinux dengan aplikasi ether cap
c. Laptop peserta melakukan FTP ke server
d. Lakukan proses Privilege Excalation mencakup kegiatan identifikasi dan password 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

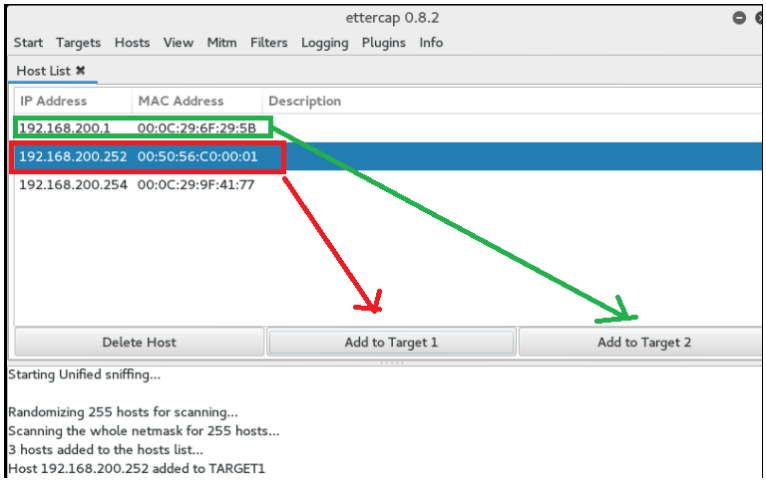
No	Steps	Information
Membuat Koneksi dari Laptop ke server		
1.	Buat koneksi antara komputer	1. Ping dari Laptop ke server 2. Ping dari server ke laptop 3. Ping dari kalilinux ke server

		4. Ping dari Kalilinux ke laptop
2.	Melihat Tabel ARP sebelum proses poisioning	5. Ketik: ***arp –a*** pada laptop melalui *command prompt* (catat hasil arp berupa **ip address** dan **mac address** dari **server** pada table laporan)  6. Ketik: **arp –a** pada server debian (catat hasil arp berupa **ip address** dan **mac address** dari **laptop** pada table laporan)  7. Ketik arp –a pada Kalilinux (catat hasil arp berupa **ip address** dan **mac address** dari **laptop dan server** pada table laporan)

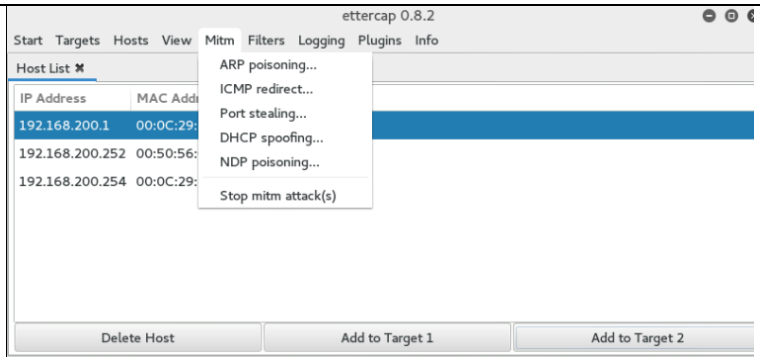
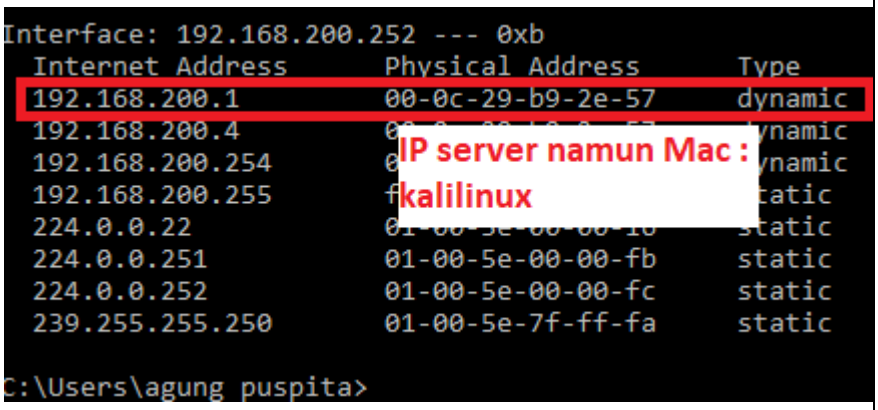
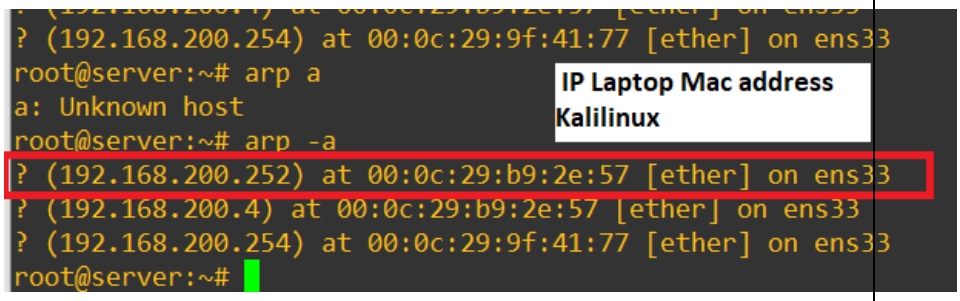
		
3.	Melakukan Man In Midle Attack melalui Kalilinux	1. Pada kalilinux, pilih *application>sniffing&spoofing>ettercag-gui* 2. Pada ethercap pilih tab menu : *Sniff>unifield sniffing..*  3. .pada etthercap input, pilih interface: *eth0*  4. Pilih tab menu host: *Scan for host*

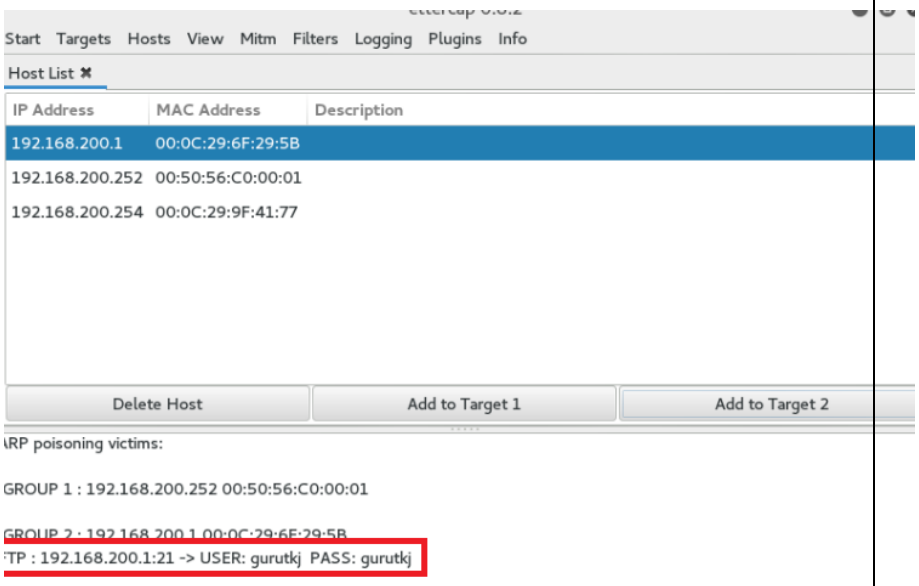


5. Pada **host list,** terdapat 2 alamat ip dan mac address hasil scan
   a) Klik untuk pilih ip computer target dan klik add to target 1 (memasukan laptop kedalam target1.)
   b) Klik untuk pilih ip server dan klik add to target 2 (memasukan pc router kedalam target2)



6. Pilih tab menu mitm >ARP Poisioning

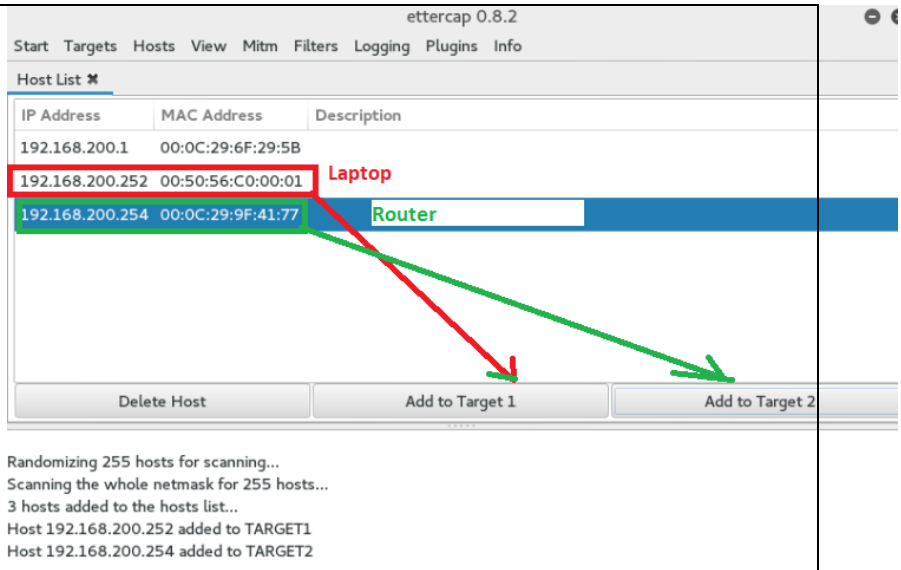
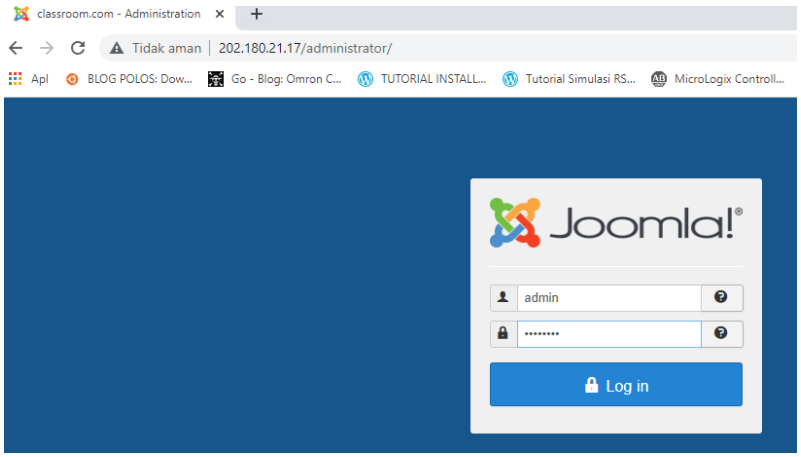
		 7. Pada optimal parameter pilih Beri tanda check pada “sniff remote connection”
4.	Melihat Tabel ARP setelah proses poisioning	1. Ketik: ***arp –a*** pada laptop melalui *command prompt* (catat hasil arp berupa **ip address** dan **mac address** dari **server** pada table laporan)  2. Ketik: **arp –a** pada server debian (catat hasil arp berupa **ip address** dan **mac address** dari **laptop** pada table laporan)  3. Ketik arp –a pada Kalilinux

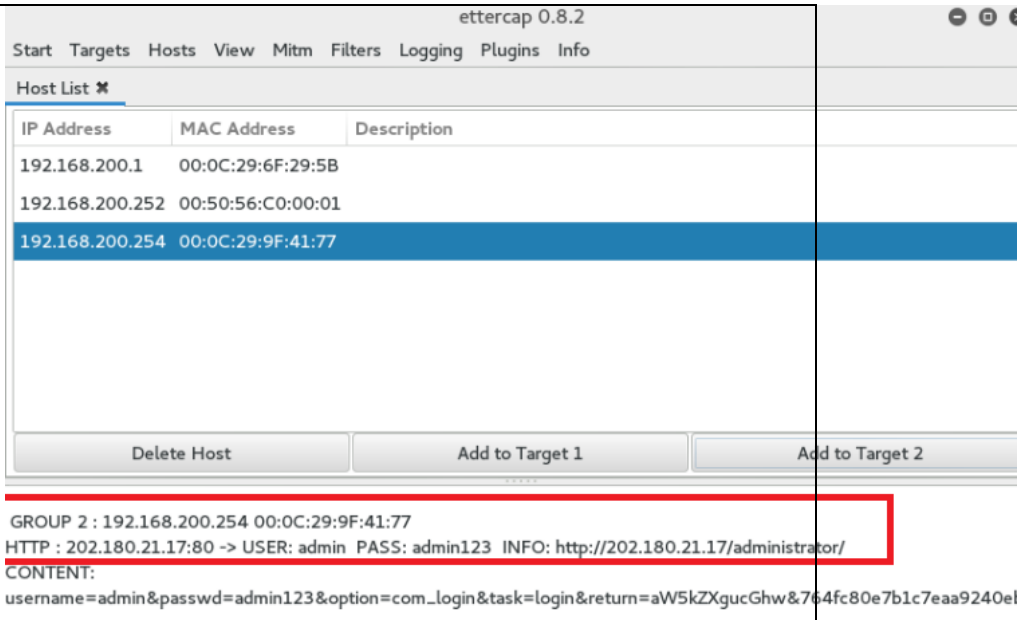
		(catat hasil arp berupa **ip address** dan **mac address** dari **laptop dan pc server** pada table laporan)
5.	Pengujian password FTP	Dari laptop , coba lakukan FTP ke router melalui perintah pada command. Pada contoh yg diberikan *C:\Users\agung puspita>ftp 192.168.xx.2* *Connected to 192.168.xx.2.* *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>* (printscreen /capture hasilnya dan lampirkan pada table laporan)
6.	Pada Komputer Kalilinux	Lihat pada ethercap username password FTP yang terekam (capture gambar dan lampirkan pada table laporan) 

Man In The Middle Attack Melihat Password Web Server

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

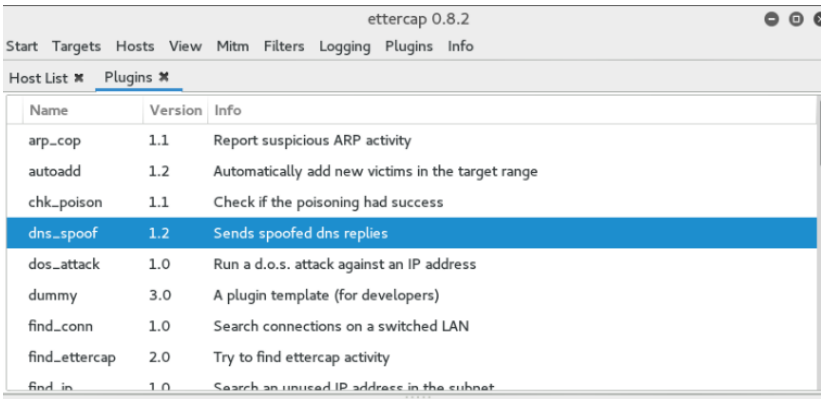
coba kali ini disediakan sebuah halaman web dengan alamat url : *http://202.180.21.17/administrator*, gunakan username : admin dan password admin 23

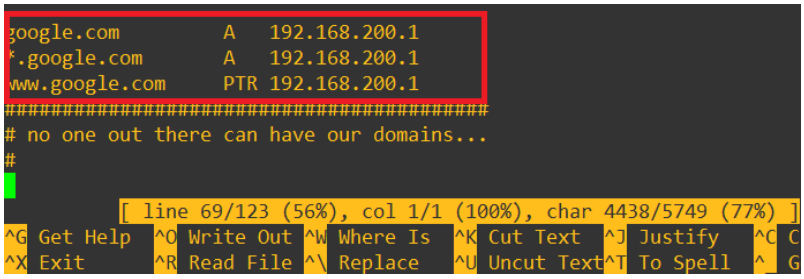
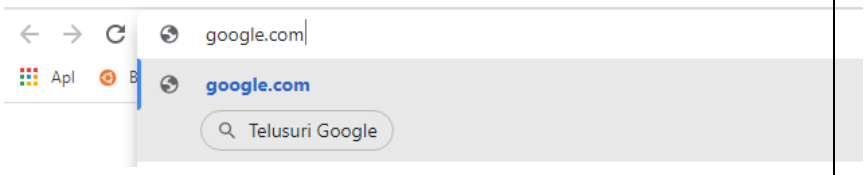
7.	Lakukan langkah yang sama untuk poisioning Laptop Pengguna dan Router ens34 (internal network)	
8.	Pengujian password Web Server/HTTP server	1. Dari PC host , coba akses http server 119.235.16.190, dengan url lengkap ***http:// http://202.180.21.17/administrator*** 2. Masukan **username : admin** dan **password : admin123** (Capture dan lampirkan pada table laporan) 
9.	Pada Komputer Kalilinux	Lihat pada ethercap username password web server yang terekam

B. DNS Spofing

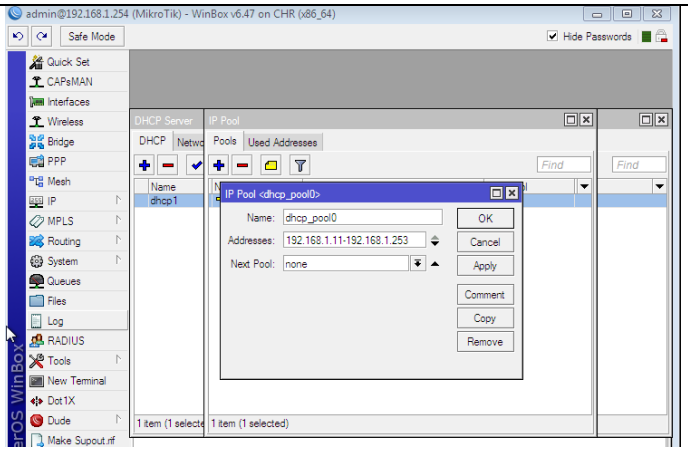
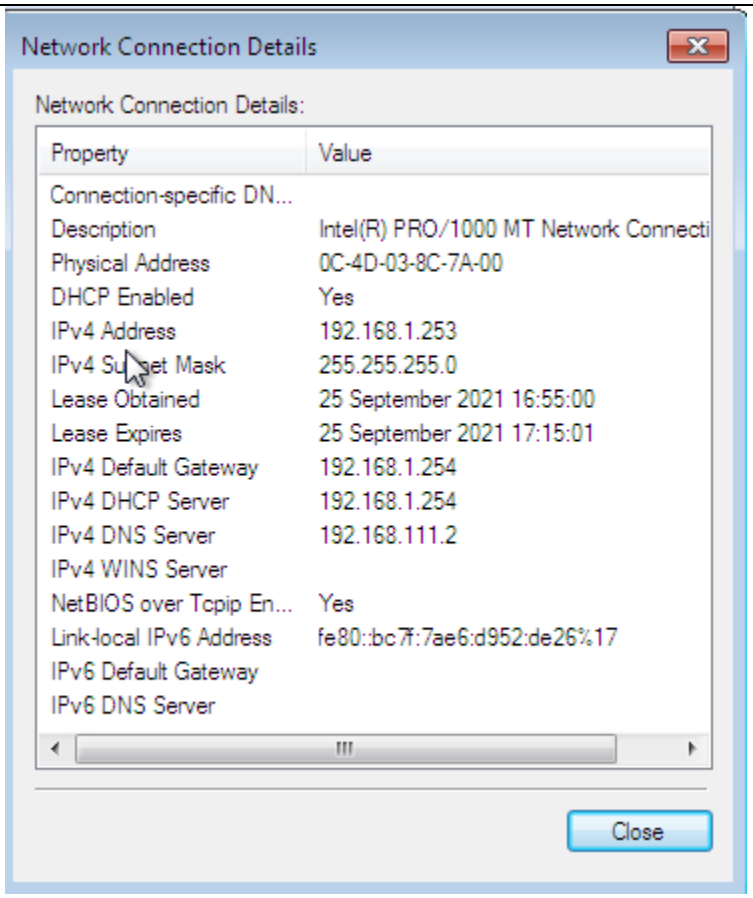
Masih Menggunakan ARP Poisioning, DNS Spofing digunakan untuk mengalihkan nama DNS, kedalam sebuah alamat IP address atau DNS dari sebuah halaman web palsu, sehingga tanpa disadari pengguna akan memasukan username dan account pada sebuah situs dengan alamat DNS yang telah disediakan. Untuk Ujicoba kali 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

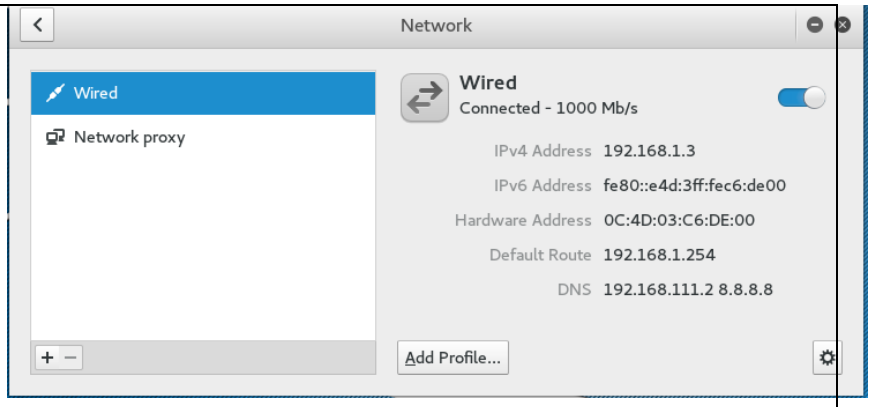
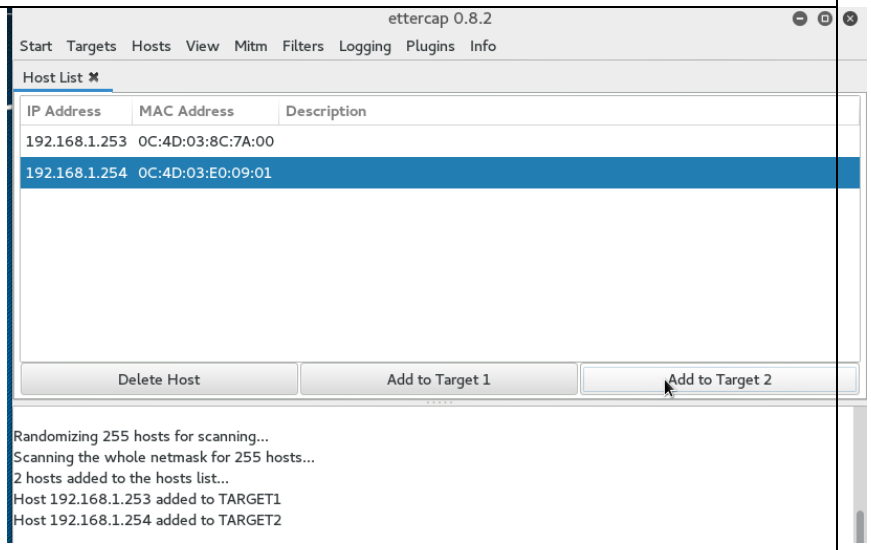
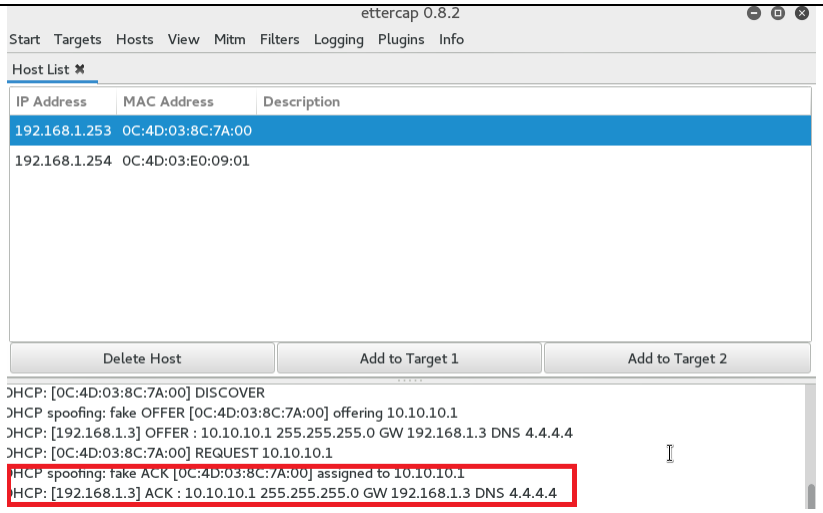
10.	Masih dalam proses meracuni (poisioning Router dan Laptop)	Pilih menu plugin pada ethercap
		2x cklik pada DNS Spoofing sampai muncul tanda * 

11.	Konfigurasi file etter.dns	• nano /etc/ettercap/etter.dns • untuk contoh cari isi text dengan nama google.com, dengan cara ctr+w dan ketik google • ubah menjadi google.com A 192.168.200.1 *.google.com A 192.168.200.1 www.google.com PTR 192.168.200.1 
12.	Dari Laptop Pengguna , gunakan browser untuk membuka google.com	Cek browser access google.com  Hasil dari alamat google.com 

C. DHCP spoofing

Ettercap, banyak memiliki fungsi exploite dalam jaringan selain ARP poisioning ,MIMA, DNS Spoofing terdapat juga jenis serangan yaitu DHCP, spoofing, dimana Etercap 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.	Tampikan menggunakan winbox ip pool	
14.	Tampilkan IP laptop pengguna	

15.	Tampilkan ip address kalilinux	
16.	Masih menggunakan ettercap , lakukan poisioning 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 etthercap user terlihar renew ip address	

19.	Pada Laptop Pengguna