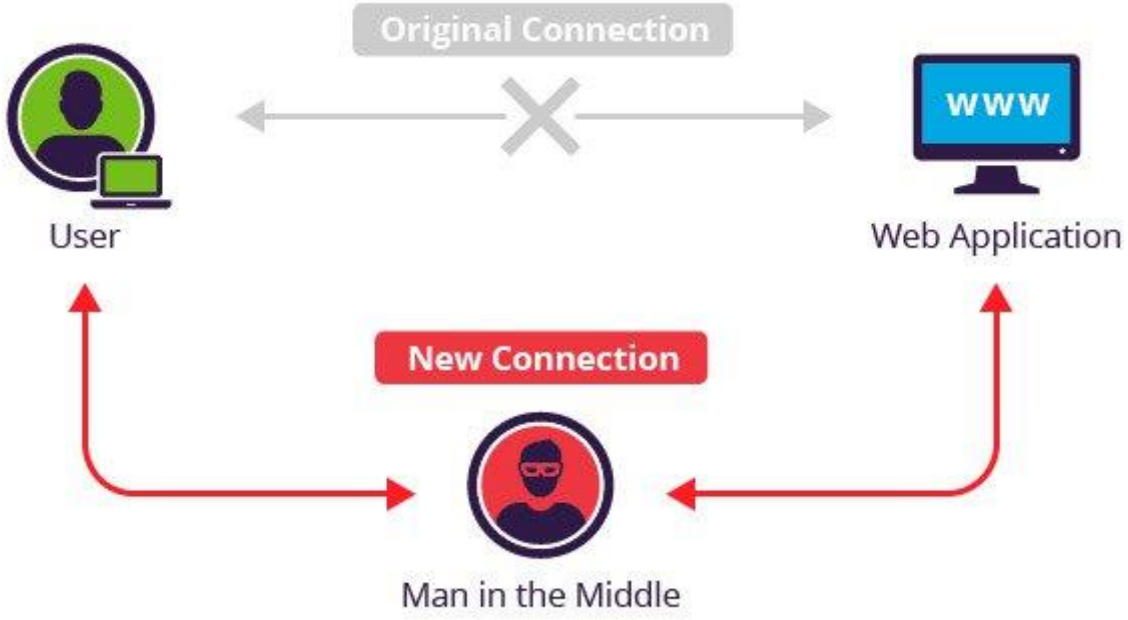
MITM Attack

MITM singkatan dari Man In The Middle. MITM Attack merupakan penyerangan yang dilakukan dengan cara mengalihkan paket yang seharusnya dikirim oleh host 1 untuk host 2 jadi melewati attacker dahulu baru diteruskan ke host 2. Tujuan dari MITM Attack ini adalah mengambil data krusial yang dimiliki oleh host saat host tersebut berkomunikasi dengan host lainnya. Data krusial bias berupa id dan password, PIN bank, data pribadi dan semacamnya.



Sniffer

Sniffing merupakan salah satu metode hacking yang mudah digunakan. Walaupun mudah digunakan sniffing ini bisa sangat berbahaya karena dapat mengambil data-data krusial yang dimiliki host saat berkomunikasi dengan router atau dengan host lainnya. Sampai saat ini, metode sniffing attack masih sulit untuk mendeteksi dan mengatasinya.

Bagaimana penyerang dapat mengambil data-data krusial yang dimiliki host? Yaitu dengan cara melihat lalu lintas paket yang dikirim atau diterima oleh host. Lalu lintas tersebut dapat dilihat oleh penyerang karena paket yang seharusnya langsung diterima oleh lawan bicara host dialihkan melewati penyerang terlebih dahulu baru diteruskan ke lawan bicara host.

Sniffing dapat dilakukan didalam jaringan LAN wireless maupun wireline. Pada wireless, paket disebar kesegala arah jadi sniffer dapat menangkap paket tersebut sebelum diteruskan ke tujuan. Pada wireline, tiap hostnya membutuhkan protokol untuk bisa saling berkomunikasi antara satu sama lain. Sniffer memanfaatkan protokol tersebut untuk mengalihkan paket sebelum sampai ke tujuan.

Walaupun serangan ini mudah untuk dilakukan, kita harus terlebih dahulu tahu di jaringan seperti apa sniffer ini dapat digunakan dan aturan main pada jaringan tersebut.

Ethernet dan Topologi Jaringan

Ethernet merupakan aturan pengiriman data yang ada didalam suatu jaringan salah satu contohnya, bagaimana paket dikirimkan dari komputer ke komputer lainnya.

Dahulu kabel coaxial masih digunakan untuk menghubungkan antara komputer. Dahulu juga topologi yang digunakan adalah topologi bus. Topologi ini memungkinkan paket yang dikirimkan perlu melewati setiap komputer yang terhubung baru sampai pada router. Topologi seperti ini sangat mudah untuk di-sniffing.

Sekarang kegunaan kabel coaxial digantikan oleh kabel UTP. Dan topologi bus sudah mulai digantikan oleh topologi lainnya seperti ring ataupun star. Topologi ini membutuhkan perangkat tambahan, yaitu hub atau switch. Secara bentuk hub dan switch tidak dapat dibedakan karena bentuk yang sama persis. Tetapi cara berkerjanya sangat berbeda.

Hub

Hub merupakan perangkat yang digunakan untuk menghubungkan dua atau lebih komputer agar bisa didalam satu jaringan. Hub itu sendiri dibagi menjadi dua, yaitu : Passive Hub dan Active Hub. Perbedaannya ada dibagaimana hub itu berkerja. Passive Hub tidak membutuhkan listrik dikarenakan hub ini hanya meneruskan paket dari komputer ke komputer lain. Active Hub membutuhkan listrik karena Active Hub akan meneruskan paket ke semua komputer yang terhubung.

Misalnya Komputer-1 ingin mengirim paket ke Komputer-2, maka paket tersebut akan dibroadcast oleh hub ke semua komputer yang terhubung. Lalu apa yang dilakukan oleh Komputer-3 dan Komputer-4 bila menerima paket itu? Komputer-3 dan Komputer-4 akan mengabaikannya karena paket tersebut tidak ditujukan pada dia. Maka dari itu sniffer dapat dengan mudah mengambil paket tersebut tanpa harus menyerang Komputer-1.

Switch

Walaupun bentuk yang sama persis dengan hub, switch memiliki cara kerja yang berbeda dengan hub. Pada hub, semua paket yang melewatikan akan dibroadcast ke

semua komputer yang terhubung dengannya. Tetapi tidak pada switch. Switch memiliki memori yang berfungsi untuk menyimpan alamat MAC komputer yang terhubung dengannya. Memori ini dinamakan *Content Addressable Memory*.

Pada switch, host yang ingin berkomunikasi akan membroadcast IP dan MAC host itu sendiri berserta IP tujuan. Lalu tujuan membalas broadcast tersebut dengan MACnya. Setelah itu switch akan menyimpan alamat IP dan MAC host yang terhubung. Switch setelah itu menghubungkan host yang akan berkomunikasi tersebut tanpa menghubungkan dengan host lainnya.

Karena jalur khusus yang dibentuk oleh switch ini, host lain tidak dapat mendengarkan pesan-pesan yang dikirimkan oleh host yang terhubung dengan jalur khusus itu. Disinilah sniffing tidak dapat langsung digunakan lagi.

RAM Switch

RAM Switch merupakan tempat penyimpanan MAC Address yang telah disimpan oleh switch. RAM Switch memiliki kapasitas sesuai dengan yang diinfokan pada switch tersebut.

Enkapsulasi dan Dekapsulasi

Enkapsulasi dan dekapsulasi merupakan serangkaian proses dalam pengiriman paket antara host yang berkomunikasi. Enkapsulasi dan dekapsulasi dapat dianalogikan dengan pengiriman surat. Surat tidak diantar begitu saja kepada penerimanya. Tetapi surat dibungkus terlebih dahulu dengan amplop, direkatkan dengan lem agar tidak bisa dibuka, diberikan alamat pengiriman diamplop surat itu, lalu amplop tersebut dimasukan kedalam kotak pos.

Pegawai pos akan mengambil amplop tersebut, melihat alamat dan mengirimkan amplop ke alamat yang dituju. Lalu penerima menerima amplop, membuka amplop untuk melihat surat didalamnya. Proses pembungkusan dan pengiriman amplop ini bisa disebut dengan enkapsulasi dan dekapsulasi. Proses ini memudahkan pengiriman paket dari satu tempat ke tempat lain. Karena proses ini, banyak sekali data yang terbaca didalam sniffer. Data-data ini sebagian besar merupakan data tambahan dari data utama yang dikirimkan.

Tipe-tipe Sniffing

Dari ilmu-ilmu diatas, kita dapat mengetahui bagaimana antara host bisa berkomunikasi, bagaimana cara hub dan switch berkerja, broadcast ARP dan sebagainya. Dilihat dari bagaimana cara hub dan switch berkerja, dapat diketahui bahwa perlu cara sniffing yang berbeda tergantung dengan jaringan yang terpasang. Berikut merupakan tipe-tipe sniffing pada umumnya :

1. Passive Sniffing
   Merupakan cara sniffing yang paling mudah dan paling simple. Cara ini dapat digunakan bila jaringan tersebut menggunakan hub. Dengan memanfaatkan cara kerja hub, penyerang hanya perlu duduk diam sambil mengambil semua data yang lewat didalam jaringan tersebut.
2. Active Sniffing
   Aktifitas sniffing hanya dapat dilakukan bila penyerang mendapatkan akses diantara host yang saling berkomunikasi. Dibeberapa jaringan, untuk mendapatkan akses ini bisa terbilang sulit misalnya didalam jaringan tersebut menggunakan switch. Karena switch dapat membentuk jalur khusus untuk komunikasi antara host, penyerang perlu mengakali bagaimana penyerang bisa berada didalam jalur khusus itu.

   Dinamakan Active Sniffing karena penyerang perlu melakukan beberapa hal untuk bisa mendapatkan paket-paket yang melewati jaringan tersebut.

Protokol yang biasa dimanfaatkan

Beberapa protokol yang biasa kita gunakan dalam kehidupan sehari-hari bisa menjadi celah penyerang untuk mengambil data-data kita lewat sniffing. Data ini bisa dilihat secara clear text / teks murni bila data yang dikirimkan tidak melalui enkripsi (pengacakan data). Jadi data seperti email, password, pin dan data-data krusial bisa dilihat secara langsung oleh penyerang. Bila saat pengiriman dilakukan enkripsi terlebih dahulu, maka paket-paket yang masuk kedalam komputer penyerang terlihat seperti tumpukan tulisan tidak bermakna.

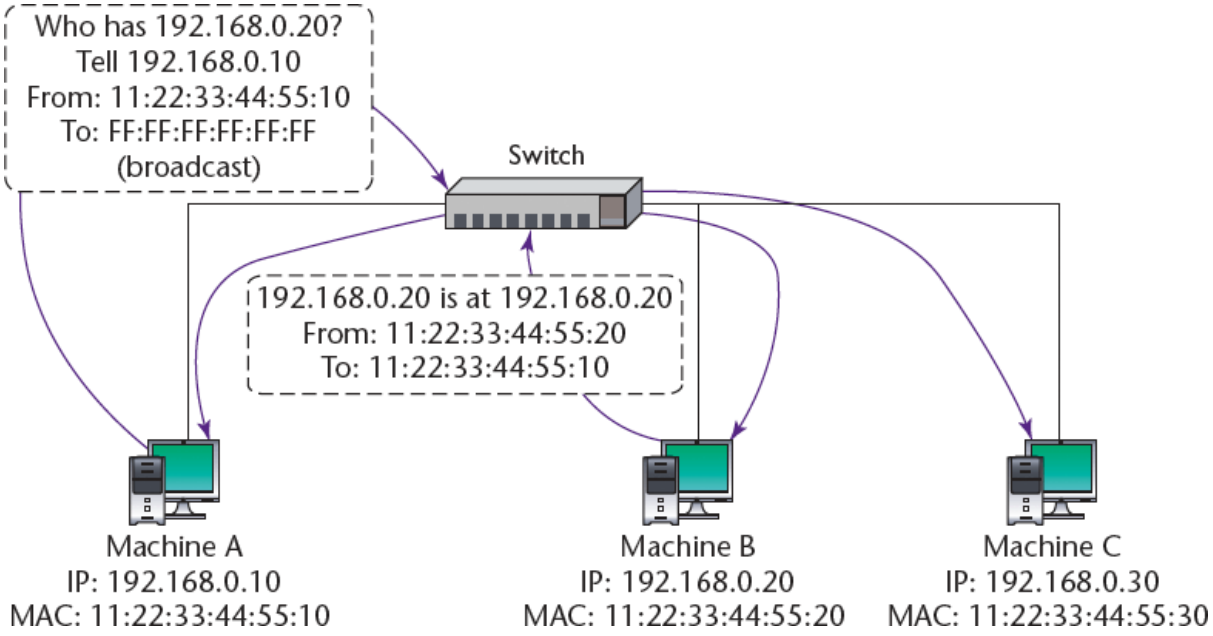
Berikut merupakan protokol yang biasa dimanfaatkan oleh penyerang :

1. Telnet : Protokol yang digunakan untuk meremote sebuah komputer.
2. HTTP : *Hypertext Transfer Protocol* merupakan protokol yang digunakan di internet pada umumnya. Protokol ini sangat mudah untuk di-sniffing karena langsung memperlihatkan secara clear text paket yang dilewatkan.
3. SMTP : *Simple Mail Transfer Protocol* merupakan protokol yang digunakan untuk pengiriman email. Sampai sekarang SMTP masih umum digunakan untuk pengiriman email.
4. POP : *Post Office Protocol* merupakan protokol yang digunakan untuk menerima email. POP juga masih umum digunakan saat ini.

5. IMAP : *Internet Message Access Protocol* adalah protokol yang digunakan pada penerima email. Mirip dengan POP, bedanya adalah IMAP biasa digunakan pada perangkat mobile.
6. NNTP : *Network News Transfer Protocol* adalah protokol yang digunakan untuk menggunakan Usenet.
7. FTP : *File Transfer Protocol* merupakan protokol yang digunakan untuk pengiriman file dari host ke host lain.

ARP

ARP atau disebut juga sebagai Address Resolution Protocol adalah protokol yang bertugas untuk untuk mencocokan IP Address dengan MAC address host yang terhubung didalam jaringan switch. ARP ini digunakan saat host melakukan broadcast IP Address berserta MAC Addressnya ke jaringan yang dia terhubung. Proses ini berguna agar host yang terhubung dapat saling berkomunikasi didalam jaringan switch tersebut.



Network Viewer Tools

Network Viewer Tools, adalah program yang digunakan untuk melihat ada berapa perangkat yang terhubung didalam sebuah jaringan. Hal ini dilakukan agar penyerang tahu alamat IP yang digunakan oleh korbannya.

DHCP

DHCP (Dynamic Host Configuration Protocol) adalah layanan yang digunakan untuk memberikan IP secara otomatis kepada komputer yang memintanya. DHCP Server adalah komputer yang memberikan IP secara otomatis tersebut. Dan DHCP Client adalah yang meminta IP kepada DHCP Server. Didalam DHCP ini ada layanan Leasing Periode, dimana jika client tidak memperbaharui permintaan IP lagi maka akan dicabut IPnya oleh DHCP Server.

HTTP

HTTP, atau kependekan dari Hypertext Transfer Procotol merupakan sekumpulan aturan dalam pengiriman paket-paket data yang bisa berupa gambar, suara, video, atau data multimedia lainnya pada WWW (World Wide Web). Protokol ini akan secara tidak langsung digunakan saat user membuka web browser.

HTTPS

Hypertext Transfer Protocol merupakan kepanjang dari HTTPS, dimana HTTPS ini bentuk adaptasi dari HTTP. Apa yang membuat HTTPS dan HTTP berbeda? Pada HTTP semua data yang dikirimkan melalui protocol tersebut tidak dienkripsi terlebih dahulu. Jadi saat paket tersebut disniffing maka akan terlihat secara langsung apa isi paket tersebut.

Karena ancaraman keamanan jaringan inilah HTTPS dibentuk. Dengan menggunakan HTTPS, paket-paket yang akan dikiriman acak terlebih dahulu. Bagaimana sistem pengacakan ini? Komputer pengguna dengan komputer server akan melakukan perjanjian penggunaan suatu kode dimana kode ini digunakan untuk mengacak paket yang akan mau dikirim.

SSL/TLS

SSL (Secure Socket Layer) atau sekarang yang lebih sering disebut dengan TLS (Transport Layer Security) adalah protokol yang berfungsi untuk mengenkripsi data yang dilewatkan didalam jaringan komputer. SSL/TLS ini sering sekali digunakan baik pada website, email, faxing, instant message ataupun telepon dengan IP. SSL/TLS ini digunakan diberbagai macam tempat dengan tujuan agar paket-paket data yang dikirimkan terjaga dari pihak luar. Kedua protokol ini digunakan untuk menjaga privasi serta integritas data.

Cara kerja SSL/TLS :
Saat user membuka browser dan halaman yang menggunakan HTTPS, maka browser akan bertanya pada server versi SSLnya dan algoritma yang digunakan. Lalu server akan memberi versi SSL/TLS dan algoritmanya serta sertifikat keaslian SSL/TLS tersebut. Browser user akan memverifikasi sertifikat itu dengan data yang ada didalam browser, apakah sudah dipercaya oleh CA (Certificate Authorities) dan tidak habis masa berlakunya.

Jika valid sertifikatnya, maka browser membuat one-time key pada sesi ini, dimana kunci ini akan mengenkripsi server public key dan mengirim ke server. Server mendekripsi kuncinya lalu menggunakan kunci tersebut bersamaan dengan algoritma yang dijanjikan.

Jadi, apa sih bedanya SSL dan TLS? Dari segi cara kerja, SSL dan TLS hampir mirip. Bedanya adalah TLS dapat menutupi beberapa kekurangan yang dimiliki SSL, karena itu TLS lebih baik keamanannya ketimbang SSL.

HSTS

HTTP Strict Transport Security (HSTS), adalah sebuah kebijakan yang digunakan oleh website untuk menjaga paket data yang dikirimkan oleh user ke server. HSTS ini memaksa user untuk mengakses website menggunakan https, bukan menggunakan http. Karena user dipaksa menggunakan https, sudah pasti paket data yang dikirimkan terenkripsi.

HSTS ini juga dapat menangkal serangan protocol downgrade attack dan cookies hijacking dimana serangan ini membuat user yang awalnya mengakses website dengan https menjadi menggunakan http.

Passive Sniffing

Setelah mengetahui host yang terhubung didalam jaringan, penyerang akan melakukan aksi berikutnya untuk mendapatkan paket si korban. Salah satu perangkat lunak yang sering digunakan adalah wireshark.

Wireshark

Wireshark merupakan perangkat lunak yang paling sering digunakan untuk melakukan sniffing pada jaringan. Bukan hanya gratis, tetapi wireshark ini juga mudah dalam penggunaannya. Wireshark bisa digunakan sniffing pada jaringan. Sniffing adalah

mengambil semua paket yang melewati penyerang, termasuk password ataupun pin dari host lain.

Wireshark akan menampilkan semua interface yang tersedia didalam komputer anda. Interface ini dapat dilihat deskripsi, alamat ip dan jumlah paket yang melewatinya.

Pada saat wireshark menangkap paket yang melewatinya, akan muncul halaman berikutnya yang menampilkan paket data yang melewatinya, terjemahan paket yang dipilih, paket data dalam bentuk hexadecimal, dan paket data dalam bentuk ASCII.

Banyaknya paket yang masuk kedalam wireshark akan menyulitkan pengguna dalam melihat paket tersebut. Untungnya wireshark memiliki fitur dimana paket-paket yang masuk dapat menjadi satu dengan cara memilih “Follow TCP Stream“. Semua data yang berhubungan dengan paket yang dipilih akan disatukan dan ditampilkan dalam window baru. Data-data ini ditampilkan dalam bentuk ASCII agar pengguna dapat dengan mudah membaca paket-paket tersebut. Disinilah paket username, password ataupun pin yang tidak dienkripsi dapat dibaca dengan mudah.

Untuk menghindari pembacaan paket-paket ini, dapat dilakukan oleh server website itu sendiri. Server website perlu menmbahkan fitur HTTPS (Hypertext Transfer Protocol Secure) agar paket-paket yang dikirimkan oleh host ke server dienkripsi jadi akan sulit dibaca oleh penyerang karena paket yang dienkripsi akan terlihat seperti paket-paket acak yang tidak ada artinya.

Cara menggunakan Wireshark :

1. Nyalakan aplikasi Wireshark.
2. Pilih interface mana yang akan disniffing.
3. Paket yang melewati wireshark akan langsung tertangkap.

Active Sniffing

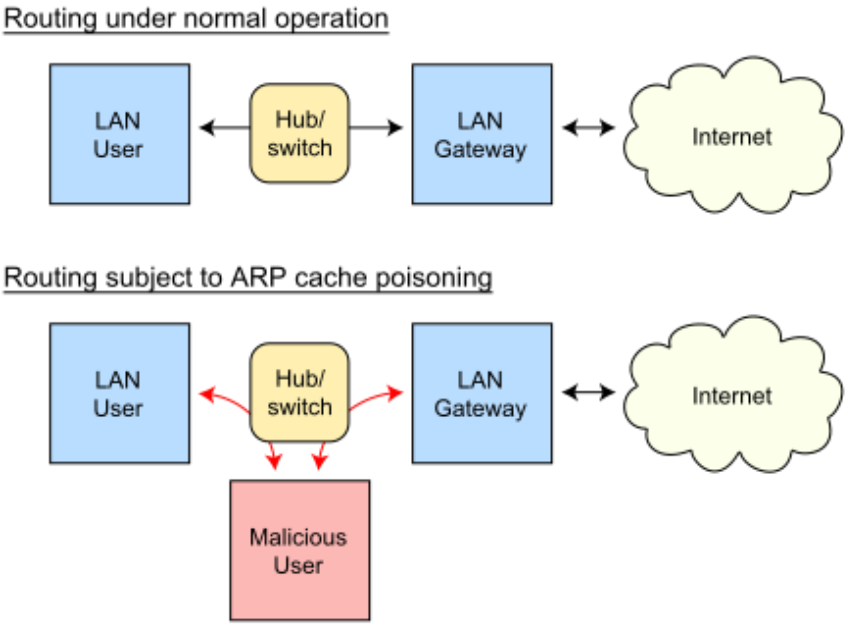
Tidak mungkin semua jaringan akan selalu menggunakan perangkat hub. Karena itu dibuat teknik lain yaitu Active Sniffing. Untuk melakukan active sniffing ini, orang pada umumnya menggunakan Ettercap.

ARP Spoofing

ARP Spoofing adalah teknik penyerangan MITM dimana penyerang mengelabui switch dengan cara mengubah MAC Address korban menjadi MAC Address penyerang. Bagaimana ini bisa dilakukan? Dengan memanfaatkan ARP. Penyerang akan membroadcast ARP

dimana ARP itu digunakan untuk mengubah MAC address penyerang menyerupai MAC address router. Karena MAC Addressnya telah serupai, maka tiap paket yang harusnya dikirimkan ke router jadi melewati penyerang terlebih dahulu.

Begitu juga pada router, penyerang akan mengirimkan paket ARP agar MAC address penyerang dapat menyerupai MAC address korban. Dengan ini semua paket dari korban ke router ataupun router ke korban akan melewati computer penyerang terlebih

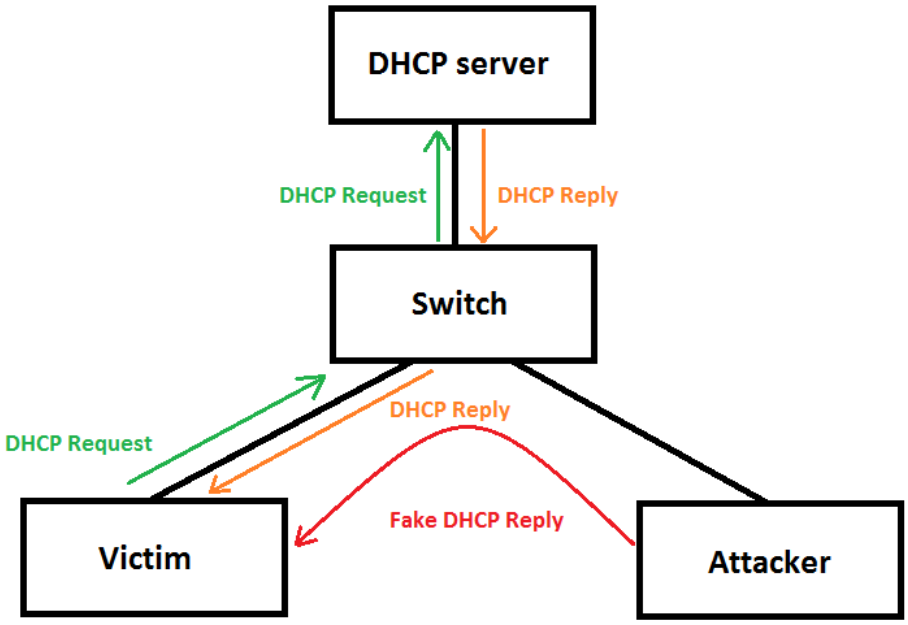


dahulu.

DHCP Spoofing

DCHP Spoofing adalah salah satu teknik MITM dimana penyerang bertindak sebagai DHCP Server palsu. Korban yang terhubung dengan DHCP Server palsu ini akan terbaca semua datanya karena paket-paket ini dikirimkan melewati penyerang terlebih dahulu

lalu penyerang melanjutkannya kepada DHCP Server asli.



Ettercap

Ettercap merupakan sebuah aplikasi open source yang biasa digunakan untuk melakukan teknik spoofing. Ettercap memiliki beberapa teknik penyadapan, yaitu : ARP Poisoning, DHCP Spoofing, ICMP Redirect, Port Stealing, dan NDP Poisoning.