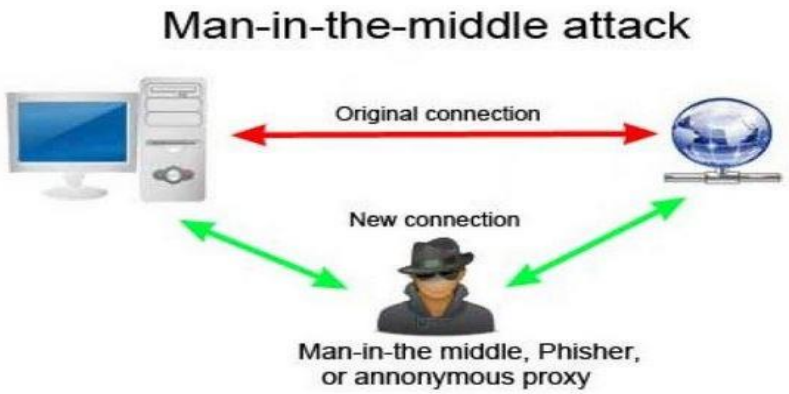
NAMA : M. NIZAL
NIM : 09011181419025

ANALISA HOLE CVE (COMMON VULNERABILITIES AND EXPOSURES)

Pada tugas sebelumnya tentang CVE (Common Vulnerabilities and Exposures) yang membahas tentang hole di website www.pusri.co.id dimana hole pada website ini merupakan serangan **Man In The Middle Attack,** Hole ini termasuk dalam **Buffer Overflow**. Dimana Buffer Overlfow adalah salah satu metode yang digunakan oleh penyerang untuk mengeksploitasi sebuah sistem komputer yang memiliki kelemahan (vulnerability) pada salah satu layanan yang digunakan oleh sistem tersebut. Sebuah aplikasi dapat di-buffer-overflow karena memang aplikasi tersebut tidak memiliki kontrol data yang baik dan biasanya ini tidak di sadari oleh si pembuat program tersebut. Seorang hacker dapat memperoleh hak akses terhadap sistem tersebut hanya dengan memanfaatkan kelemahan dari suatu aplikasi yang ada di sistem komputer target, tentu hal yang berkaitan erat dengan akses yang dimiliki oleh aplikasi tersebut.serangan ini merupakan jenis serangan dengan menyadap lalu lintas jaringan antara client dan server, serangan dilakukan dengan menggunakan tool cain cable, dimana tool ini dapat menyadap lalu lintas jaringan dengan memanfaatkan ARP (Address Resolution Protocol), penyerang meracuni ARP cache antara dua perangkat yang berkomunikasi dengan alamat MAC kedua perangkat.

Setelah cache ARP berhasil diracuni, masing-masing perangkat korban yang berkomunikasi mengirimkan paket ke penyerang, seingga penyerang seolah - olah berada di antara client dan server yang berkomunikasi. Seperti pada proses login attacker yang berhasil masuk meracuni cache ARP dapat memantau lalu lintas jaringan antara client dan server, sehingga saat proses login client mengirimkan data pada server maka attacker dapat menangkap data tersebut sehingga didapat username dan password untuk masuk pada aplikasi web server.



NAMA : M. NIZAL
NIM : 09011181419025

Penyerang harus mampu mencegat semua pesan terjadi antara kedua korban dan menyuntikkan yang baru, misalnya, seorang penyerang dalam jangkaun penerimaan terenskripsi Wi-Fi jalur akses nirkabel, dapat menyisipkan dirinya sebagai seorang Man-In-The-Middle. Konsep dasar serangan ini secara umum adalah penyerang berada ditengah – tengah atau di antara dua komputer yang sedang berkomunikasi, sehingga secara teknis memungkinkan penyerang untuk melihat, mengubah dan mengontrol data yang dikirim antar dua komputer tersebut, namun rute paket yang dikirimkan atau ditunjukkan kepada host lain harus melalui mesin penyerang.

Teknik Man In The Middle

Ada berbagai teknik dan istilah dalam serangan Man in the middle, Antara lain adalah :

1. **Sniffer**

   Sniffer yang juga dikenal sebagai **Network Analyzer** atau **Ethernet Sniffer** ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak – balik ada jaringan, aplikasi ini menangkap tiap – tiap paket dan kadang – kadang menguraikan isi dari RFC (Request For Comments atau spesifikasi yang lain.
2. **Spoofing**

   Spoofing adalah situasi dimana seseorang berhasil menyamar sebagai user dengan memalsukan data dengan demikian mendapatkan keuntungan tidak sah.
3. **Interception**

   Interception merupakan ancaman terhadap secrecy, dimana orang yang tidak berhak namun berhasil mendapatkan akses informasi dari dalam sistem komputer.
4. **Modification**

   Modification merupakan ancaman terhadap intergrity dimana orang yang tidak berhak dapat mengakses maupun merubah suatu informasi.
5. **Fabrication**

   Fabrication adalah teknik menambahkan objek atau informasi palsu pada informasi yang asli, sehingga data atau informasi berubah.