NAMA : PASCAL ADHI KURNIA TARIGAN

NIM : 09011281520113

KELAS : SK5C

Laporan Pembelajaran *Lesson 2* : **Attacker Methodology, Malware and Attacker tools**

From : https://learningnetwork.cisco.com/community/learning_center/ccna-security-training-videos

Attacker Methodology, Malware and Attacker tools

Pada pembelajaraan CCNA tentang security training tentang me rivew jenis jenis serangan dalam network dalam pembelajaran yang ke dua yaitu metodologi penyerangan , malware dan tools dalam melakukan penyerangan

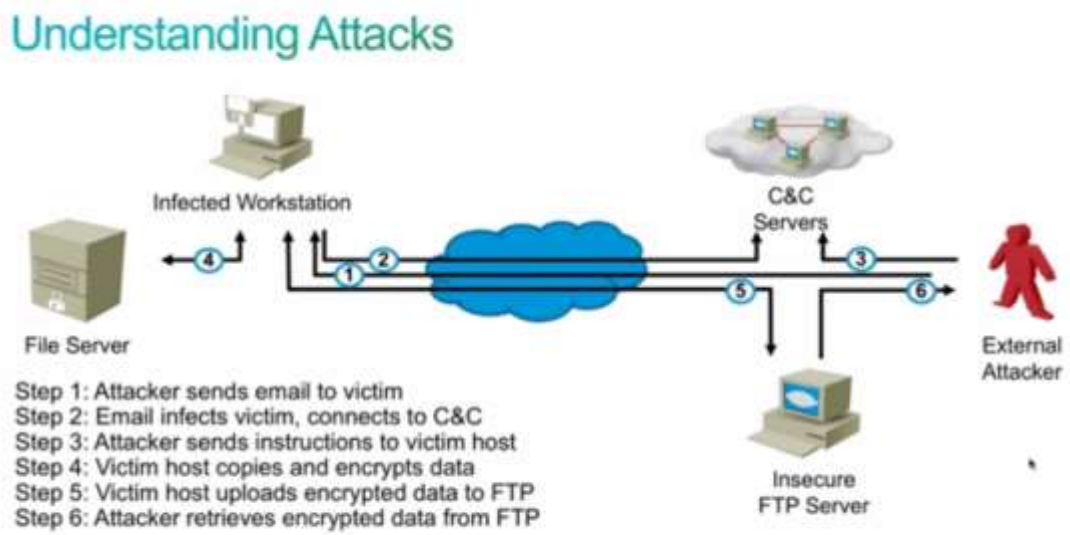
Pada video *lesson 1* membahas tentang evolusi dari penyerangan cyber. Setiap hal yang berhubungan dengan tekhnologi selalu pasti akan berkembang dan berevolusi. Sehingga penyerangan terhadap teknologi juga akan berkembang sehingga para cybercrime juga akan mengembangkannya. Hal tersebut dapat dibuktikan pada

1. Worms yang tren dalam tahun 2000. Worm adalah evolusi dari virus komputer. Sebuah worm dapat menggandakan dirinya dengan memanfaatkan jaringan (LAN/WAN/Internet) tanpa perlu campur tangan dari user itu sendiri. Worm tidak seperti virus komputer biasa, yang menggandakan dirinya dengan cara menyisipkan program dirinya pada program yang ada dalam komputer tersebut, tetapi worm memanfaatkan celah keamanaan yang memang terbuka atau lebih dikenal dengan sebutan vulnerability.
2. Spyware and rootkits tahun 2005. Spyware adalah perangkat lunak yang mengumpulkan dan mengirim informasi tentang pengguna komputer tanpa diketahui oleh si pengguna itu. Rootkit adalah sebuah atau kombinasi dari beberapa program yang dirancang untuk mengambil alih sistem secara fundamental (pada Linux istilahnya akses root sedang pada Ms Windows istilah nya akses Administrator).
3. APTS Cyberwar pada tahun 2010. Persistent Threats bisa disebut dengan APTs. Ancaman keamanan digital ini bekerja dengan mencuri informasi pribadi organisasi maupun perorangan. Misalnya ketika menyerang jejaring sosial, seperti Facebook. APTs bisa mengubah informasi pribadi penggunanya, memanfaatkannya untuk mengambil kepercayaan orang lain serta memindai jaringan yang dimiliki akun yang disusupinya.
4. Increased Attack Surface kemungkinan di kemudian hari. Increased Attack Surface menyatakan bahwa benar benar dapat dikatakan bahwa tidak ada sistem yang aman.

Sebuah organisasi atau anonymous kadang tidak menyukai organisasi kita sehingga mereka menyerang organisasi kita tersebut. Para penyerang sekarang dengan cepat membuat dan membentuk cara untuk membobol atau menyerang dan membuat alat mereka sendiri. Rencana yang banyak kita temui yaitu rencana dalam penyebaran spam. Saat browsing internet banyak sekali spam yang bermunculan dalam situs atau site tertentu. Para penyerang atau atacker juga dapat mendesain malware pada tools yang kita percayai. Hal itu juga membuat para pembobol terus menerus mencari cara untuk gampang menyerang contoh dari DNS dan Protocol.

Pada video *lesson 2* lebih membahas dalam metodologi penyerangan , malware dan tools dalam melakukan penyerangan.

Metodologi dalam penyerangan bersumber dari jenisnya penyerangan itu. Metodologi penyerangan itu yaitu teknik dalam hacking (Hacking Techniques) yaitu cara hacker tersendiri dengan skill dan pengetahuan yang dia miliki. Startegi dasar (Basic strategy) yaitu rencana dan pesiapan dan cara apa yang akan dilakukan dalam penyerangan. Kemudian Informasi pubik (Public Information) yaitu informasi yang umum yang bisa didapatkan. Pemetaan Informasi (Map Information) yaitu pengumpulan informasi yang sudah dicari. Dan terakhir adalah tujuan penyerangan (Short-term vs. Long-term attacker goals) dengan 2 tujuan jangka pendek dan dengan jangka panjang yang harus ada sehingga tercapai goal atau sasaran dalam penyarangan.



Gambar diatas adalah metode para hacker akan menyerang dengan 6 steps yang tentunya masih banyak metode lainnya tetapi hal umum yang pasti akan dilakukan hacker tentunya dengan metode diatas.

Malware (Malicious Software) adalah suatu program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer. Malware dapat menginfeksi banyak komputer dengan masuk melalui email, download internet, atau program yang terinfeksi.

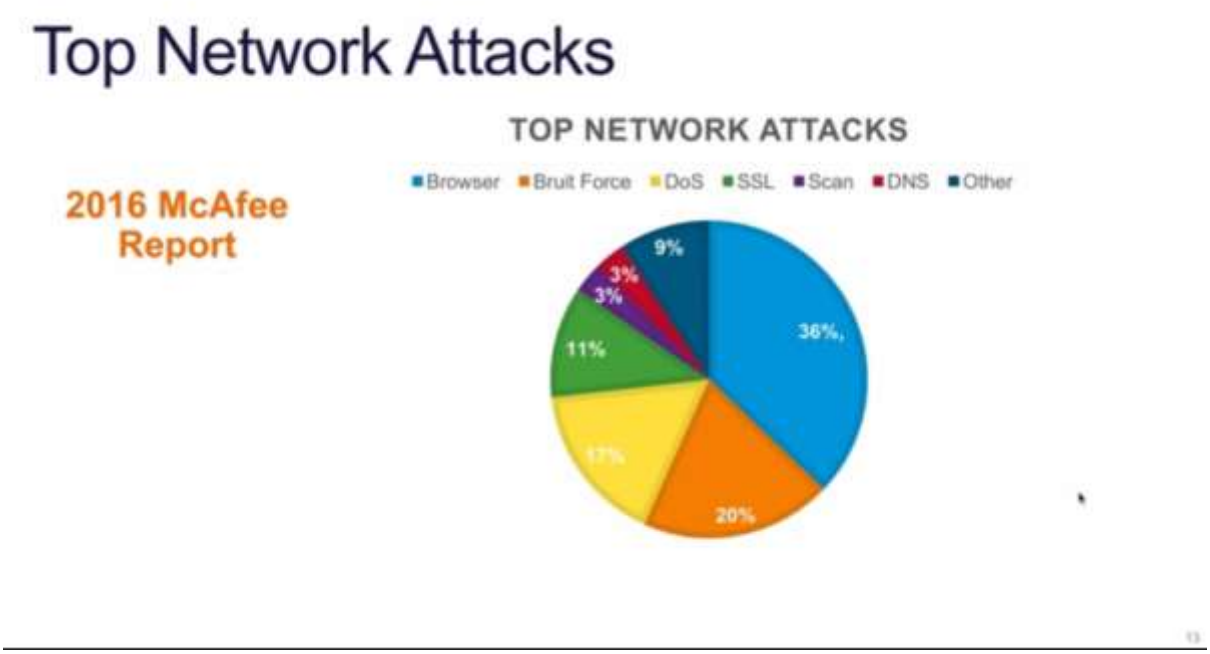
Malware bisa menyebabkan kerusakan pada sistem komputer dan memungkinkan juga terjadi pencurian data / informasi. Hal yang pada umumnya terjadi penyebab malware adalah mendownload software dari tempat ilegal yang disisipan malware. Malware mencakup virus, worm, trojan horse, sebagian besar rootkit, spyware, adware yang tidak jujur, serta software-software lain yang berbahaya dan tidak diinginkan oleh pengguna PC.

Pada website sendiri terkadang bisa terjangkit malware, hal ini bisa terjadi jika pengguna melakukan download theme website secara ilegal, hal itu dapat menyebabkan data dan informasi yang ada di website jebol, terkadang juga bisa menyebabkan server website menjadi down karena aktifitas yang mencurigakan tersebut.

Hal yang harus dilakukan untuk mencegah malware adalah tidak melakukan aktifitas ilegal, sebagai contoh tidak melakukan download resource dan aplikasi di situs yang tidak terverifikasi atau ilegal, hal ini karena biasanya peluang adanya virus malware lebih besar terjangkit pada suatu aplikasi yang diunduh di website tersebut

Tools Attacker yang biasa digunakan hacker yaitu :Backdoors, Downloaders and droppers, Rootkits, Pivots, Keyloggers, Exploits, Payloads

---



Penyerangan network biasanya dari Browser, Bruit Force, DoS, SSL, Scan, DNS dll

Serangan DoS (bahasa Inggris: denial-of-service attacks') adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

Brute Force Attack adalah metode untuk meretas password (password cracking) dengan cara mencoba semua kemungkinan kombinasi yang ada pada “wordlist“. Metode ini dijamin akan berhasil menemukan password yang ingin diretas. Namun, proses untuk meretas password dengan menggunakan metode ini akan memakan banyak waktu.