Vicko Bhayyu / 09011181520036

Jaringan Komputer SK5C

Sumber : <https://learningnetwork.cisco.com/docs/DOC-33768>

Judul yang diambil : **Lesson 2: Attacker Methodology, Malware and Attacker tools**

**Metodologi yang akan dipakai oleh penyerang :**

* **Teknik hacking**
* **Strategi dasar**
* **Informasi public**
* **Informasi map**
* **Tujuan jangka pendek atau jangka panjang**

**Urutan serangan klasik yakni**

* **Menyelidiki**
* **Menembus**
* **Bersikeras**
* **Memperbanyak**
* **Melumpuhkan**

**Pemahaman tentang serangan**

1. **Step 1 : Penyerang mengirim email ke korban**
2. **Step 2 : Email akan menginfeksi korban, dan menghubungkan ke C&C**
3. **Step 3 : Penyerang mengirimkan instruksi ke host korban**
4. **Step 4 : Host korban akan mengcopy dan enkripsi data**
5. **Step 5 : Host korban mengupload data terenkripsi ke FTP**
6. **Step 6 : Penyerang menerima data terenkripsi dari FTP**

**Toolset dari attacker yakni**

* **Backdoors**
* **Downloaders and droppers**
* **Rootkits**
* **Pivots**
* **Keyloggers**
* **Exploits**
* **Payloads**

**Serangan network teratas berdasarkan laporan McAfee 2016**

1. **Browser**
2. **Brute Force**
3. **DoS**
4. **SSL**
5. **Scan**
6. **DNS**
7. **Lain-lain**

**Lalu ada juga serangan sniffer, sniffer adalah aplikasi yang dapat mencapture paket network, atau untuk menganalisa protocol network., jika paket network tidak terenkripsi, data pada paket network akan dapat dibaca dengan menggunakan sniffer.**

**Serangan aplikasi dengan menggunakan :**

1. **Cross Scripting : injeksi client-side code untuk menyerang dimana penyerang dapat mengeksekusi script berbahaya ke dalam website atau aplikasi web.**
2. **Broken Authentication and Session Management : umumnya otentikasi menggunakan token kriptografi atau biometric, dan session management diurus oleh akun administrator sistem. Penyerang akan menyerang kedua hal tersebut.**
3. **Trojan Horse : Perangkat Lunak berbahaya yang dapat merusak sebuah sistem atau jaringan**
4. **Active X**
5. **Java**
6. **HTML**

**Anatomi dari serangan**

**Dengan model artichoke**

**Setiap daun menyediakan proteksi layer namun juga sebagai jalan untuk menyerang dan tidak dibutuhkan setiap daun untuk dibuang untuk mencapai jantung artichoke**

**Dengan urutan :**

1. **Password**
2. **Client-side attacks**
3. **Databases**
4. **Web applications**
5. **Buffer overflows**
6. **Network devices**