Lesson 2 : Serangan DoS, Spoofing, Serangan Smurf, dan Phishing.

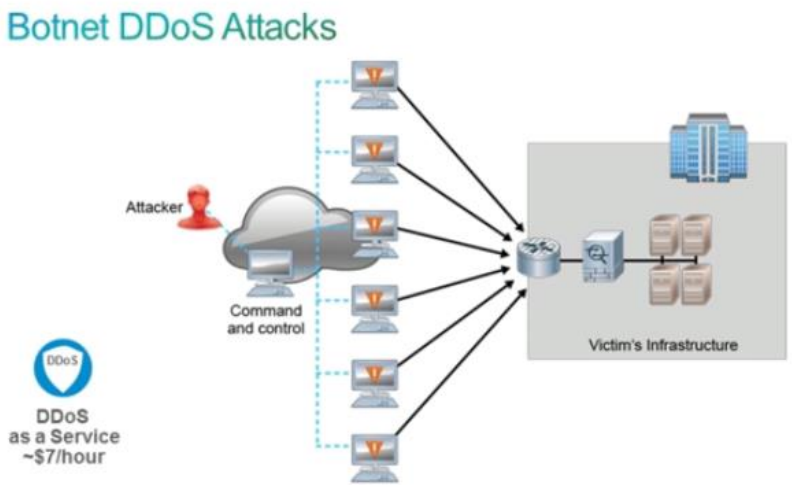
Hasil laporan :

SERANGAN DoS

1. Mencoba membuat komputer atau sumber jaringan yang tidak tersedia untuk penggunaan yang diinginkan.
    - mengkonsumsi semua sumber daya kritis
    - menyebabkan sistem crash
2. Dapat dengan mudah mengganggu operasi bisnis
3. Relatif mudah dilakukan

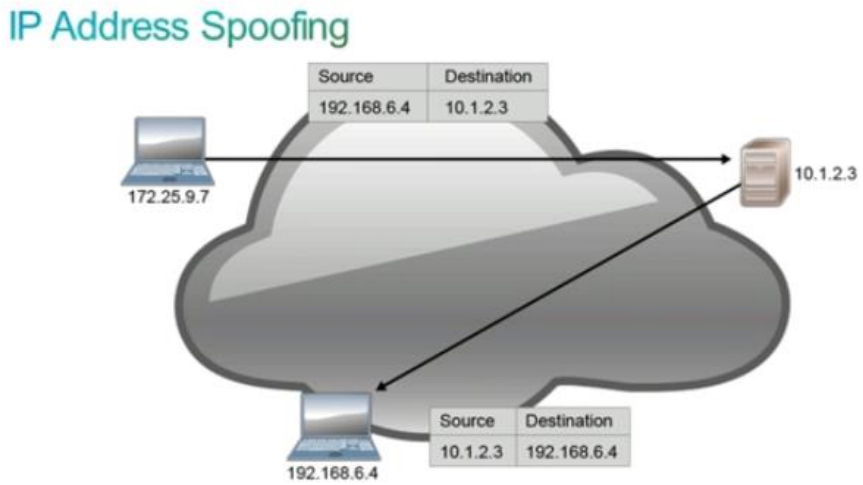
   Contoh :
    - TCP SYN Flood
    - Ping of Death
4. Umumnya bersumber dari satu sistem saja
5. Serangan DoS yang sekaligus memanfaatkan sejumlah besar sistem penyerang
6. Tipikal memanfaatkan botnet
    - kelompok komputer "zombie" yang menjalankan bot
    - mekanisme kontrol master yang mengendalikan zombie

BOTNET SERANGAN DDoS



SPOOFING

Menyuntikkan lalu lintas yang nampaknya bersumber dari sistem selain sistem penyerang itu sendiri. Bukan serangan itu sendiri, ini adalah teknik yang bisa diungkit dalam berbagai jenis serangan.



Jenis-jenis Spoofing :

1. Alamat IP Spoofing

   Serangan teknis yang rumit yang terdiri dari beberapa komponen. Ini adalah eksploitasi keamanan yang bekerja dengan menipu komputer, seolah-olah yang menggunakan komputer tersebut adalah orang lain.
2. Alamat MAC Spoofing

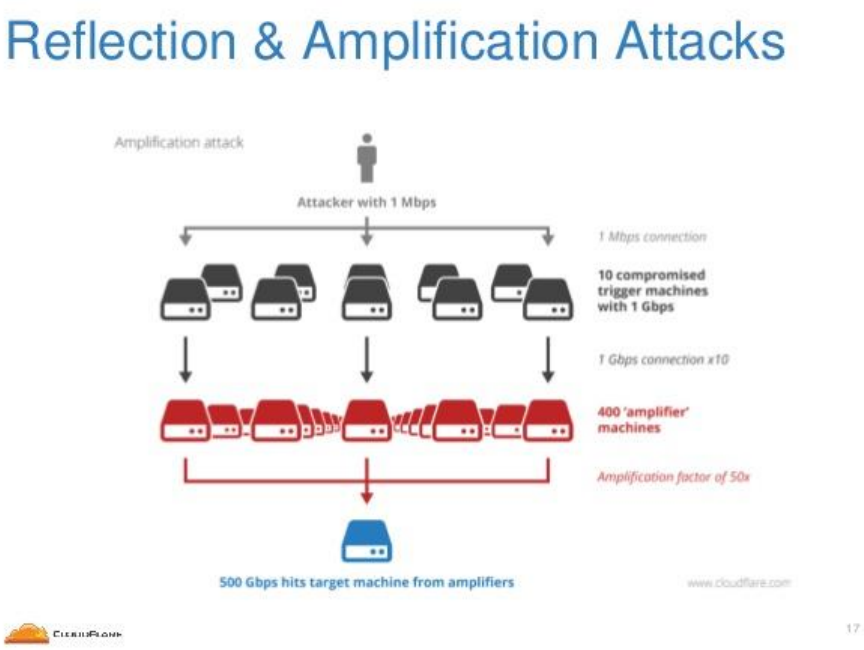
   adalah teknik untuk mengubah alamat Media Access Control (MAC) milik pabrik dari antarmuka jaringan pada perangkat jaringan. Alamat MAC yang dikodekan dengan keras pada pengontrol antarmuka jaringan (NIC) yang tidak dapat diubah.
3. Spoofing aplikasi atau layanan :

   DHCP, DNS, routing protocols, email, dll.

SERANGAN REFLEKSI DAN AMPLIFIKASI

Dalam serangan refleksi, penyerang mengirimkan paket permintaan dengan alamat IP palsu untuk membuat host lain membanjiri korban. Serangan refleksi juga bisa menjadi serangan amplifikasi jika paket permintaan meminta respons yang lebih besar.

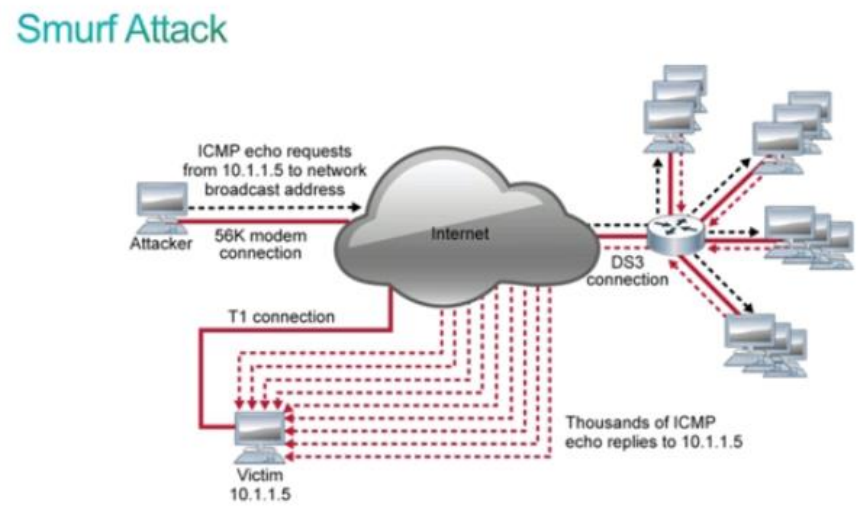
Serangan refleksi menggunakan protokol yang sama di kedua arah. Penyerang tersebut menipu alamat IP korban dan mengirimkan permintaan informasi melalui UDP ke server yang diketahui menanggapi jenis permintaan tersebut.



Dalam sebuah serangan amplifikasi, penyerang mengirimkan paket permintaan palsu untuk mendapatkan jawaban yang besar. Refleksi dan serangan amplifikasi sulit dilacak karena sebenarnya sumber serangannya tersembunyi.

Serangan amplifikasi menghasilkan volume paket yang tinggi untuk membanjiri situs target tanpa memberi tahu perantara, dengan mengembalikan balasan besar ke permintaan kecil. Pertahanan dasar melawan serangan ini menghalangi paket sumber-sumber palsu.

SMURF ATTACK



Smurf attack adalah sebuah serangan yang dibangun dengan menggunakan pemalsuan terhadap paket-paket ICMP echo request, yakni sebuah jenis paket yang digunakan oleh utilitas troubleshooting jaringan. Si penyerang akan memulai serangan dengan membuat paket-paket "ICMP echo request" dengan alamat IP sumber berisi alamat IP host target yang akan diserang (berarti alamat telah dipalsukan atau telah terjadi address spoofing).

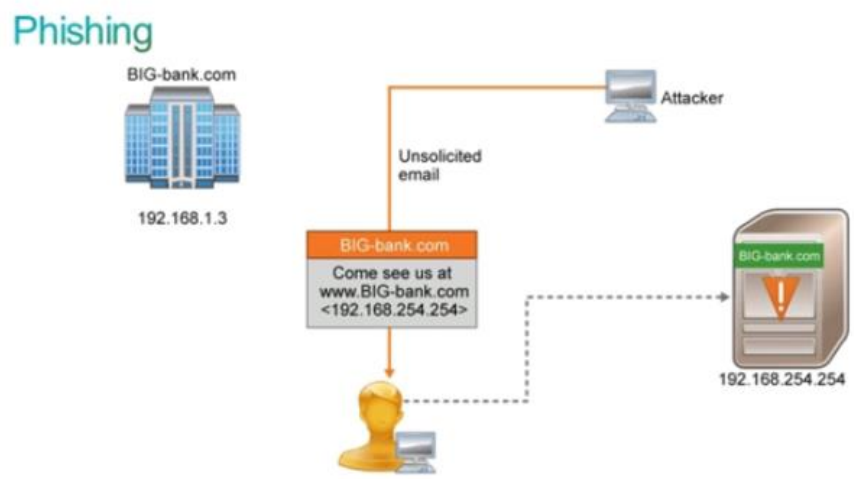
REKAYASA SOSIAL

Memanipulasi orang dan memanfaatkan perilaku yang diharapkan.

Contoh rekayasa sosial :

1. Penipuan telepon
2. Phishing
3. Tailgating
4. "Lost" kunci memori USB (salting)
5. Hacking visual (tepian surfing)

EVOLUSI PHISHING



1. Phishing tombak : phishing yang menargetkan individu atau kelompok
2. Whaling : phishing yang menargetkan individu atau kelompok dengan profil tinggi (CFOs)
3. Pharming : memikat atau membujuk korban dengan mengorbankan DNS
4. Watering Hole : serangan yang merusak server web yang terganggu untuk menargetkan kelompok pilihan
5. Vishing : phishing yang menggunakan suara dan sistem telepon sebagai media pengganti Email
6. Smishing : phishing yang menggunakan teks SMS sebagai media pengganti Email