**TUGAS JARINGAN KOMPUTER**

**Network Security Threatscape - Introduction: Lesson 2: DoS Attacks, Spoofing, Smurf Attacks, and Phishing**



DISUSUN OLEH:

Nama : M. Afria Alim Saputra

Nim : 09011281520100

Kelas : SK5C

Dosen Pengampuh : Deris Stiawan, M.T., Ph.D

**SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**PALEMBANG 2017**

**Lesson 2: DoS Attacks, Spoofing, Smurf Attacks, and Phishing**

**DoS (Denial of Servie) Attacks**

Denial service attack adalah sebuah serangan untuk membuat komputer atau server di dalam jaringan tidak bisa bekerja dengan baik dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer sampai komputer tersebut tidak bisa menjalankan fungsinya dengan benar. Contohnya adalah web ketika terkena DoS Attack, web tersebut akan mengalami website tidak bisa diakses, adanya sistem yang crash, adanya spam yang meningkat, dll. DoS Attack dapat dengan mudahnya mengganggu operasi bisnis dan dengan mudahnya dapat dilakukan.

DDoS singkatan dari Distributed Denial of Service. Penyerang dapat memerintah dan mengendalikan suatu mesin yang memiliki serangkaian bot. Bot dikendalikan oleh mesin yang menunggu perintah.



**Spoofing**

Spoofing adalah teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer dengan berpura-pura menjadi Host. Dengan spoofing Penyerang dapat langsung memasuki sistem dari dalam sehingga sistem dapat dimanipulasi.

Ada 3 jenis spoofing, yaitu :

1. IP address spoofing
2. MAC address spoofing
3. Aplikasi atau layanan spoofing : DHCP, DNS, routing protocol, Email, dll.

**IP Address Spoofing**

IP address spoofing adalah teknik untuk menyembunyikan source ip address sehingga asal dari paket network tidak dapat dilacak ataupun untuk mengelabui komputer tujuan. IP asli penyerang adalah 172.25.9.7 yang menggunakan IP palsu yaitu 192.168.6.4 dengan tujuan 10.1.2.3. server 10.1.2.3 akan mengirim balasan ke komputer yang memiliki IP 192.168.6.4 sehingga IP penyerang tidak terlacak.



**Reflection dan Amplification Attacks**

Reflection Attacks : penyerang mengirimkan paket permintaan dengan alamat IP palsu untuk membuat data menumpuk pada host lain.

Amplification Attacks : penyerang mengirimkan paket request yang kecil untuk mendapatkan reply yang besar.

**Smurf Attacks**

Smurf Attacks merupakan salah satu jenis serangan Denial of Service yang mengeksploitasi protokol Internet Control Message Protocol. Si penyerang akan memulai serangan dengan membuat paket-paket "ICMP echo request" dengan alamat IP sumber yang berisi alamat IP host target yang akan diserang yaitu 10.1.1.5. Paket-paket tersebut pun akan dikirimkan secara broadcast ke jaringan di mana komputer target berada, dan host-host lainnya yang menerima paket yang bersangkutan akan mengirimkan balasan dari "ICMP echo request" ("ICMP echo reply") kepada komputer target, seolah-olah komputer target merupakan komputer yang mengirimkan ICMP echo request tersebut.

Smurf attacks dapat digagalkan dengan konfigurasi router yang benar, akan tetapi banyak orang-orang yang tidak mengerti apa itu smurf attacks yang menyebabkan ketidaktahuan untuk menanggulangi smurf attacks.



**Social Engineering**

Social engineering adalah tehnik untuk mendapatkan informasi /hak akses dengan cara menipu korban nya dengan halus dan tanpa dia sadari. Contoh dari social engineering adalah :

* Penipuan lewat telepom
* Pishing
* Tailgating
* "Kehilangan" kunci memori USB (Salting)
* Visual hacking (shoulder surfing)

**Phising**

Phising merupakan tehnik untuk mendapatkan informasi Data pribadi atau akun dari korban dengan cara menulis email yang seolah-olah berasal dari website resmi. Contoh :

BIG-bank.com mengirimi Anda email, yang meminta Anda menyetel ulang kata sandi Anda,

* pada saat melihat link yang terkirim terlihat bahwa link tersebut benar.
	+ Memanipulasi karakter agar tampil sebagai URL yang sah.
	+ Sesuatu dikompres dalam link.
	+ Yang membawa Anda ke situs web yang terlihat sama.
	+ Pengguna lengah akan tautan Phishing yang membawa mereka ke HTTP dan bukan HTTPS.
* Hal kecil yang terlihat adalah indikator yang menandakan anda telah kena pengelabuan.



**Evolution of Phishing**

* Spear phishing: Phishing yang menargetkan individu atau kelompok.
* Whaling: Phishing yang menargetkan individu atau kelompok yang berstatus tinggi (CFO).
* Pharming: Mengumpan korban dengan mengorbankan DNS.
* Lubang penyiraman: Serangan yang memanfaatkan server web yang terganggu untuk menargetkan kelompok yang dipilih.
* Vishing: Phishing yang menggunakan suara dan sistem telepon sebagai media bukan email.
* Smishing: Phishing yang menggunakan SMS texting sebagai media bukan email.