****

**JARINGAN KOMPUTER**

**NETWORK SECURITY THREATSCAPE – DOS ATTACKS, SPOOFING, SMURF ATTACKS, AND PHISING**

**SUMMARY**

**CYNTHIA CAROLINE**

**09011281520101**

**UNIVERSITAS SRIWIJAYA**

**INDRALAYA**

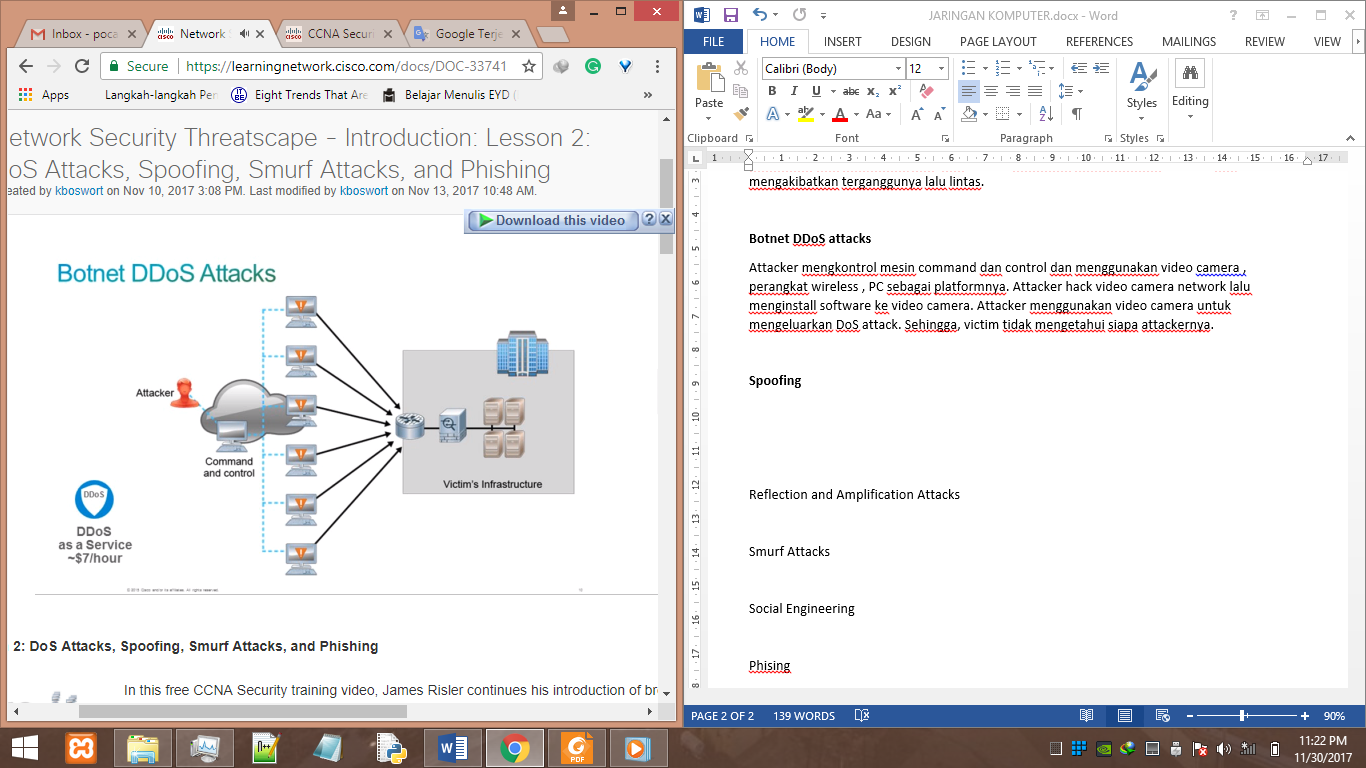
**2017**

DoS attacks (Denial of Service) mencoba untuk membuat komputer atau network tidak bisa digunakan untuk dipakai oleh seluruh sumber kritis dan menyebabkan sistem menjadi gagal. DoS attack sangat mudah menganggu operasi dari sebuah bisnis dan mudah untuk dibuat. DoS attack sering menyerang pada email, website dan sebagainya dan umumnya bersumber dari satu sistem saja. DoS attacks umumnya memanfaatkan botnets dan mengakibatkan terganggunya lalu lintas jaringan.

**Botnet DDoS attacks**

Attacker mengkontrol mesin command dan control dan menggunakan video camera , perangkat wireless , PC sebagai platformnya. Mekanisme hack video cameranya adalah

1. Attacker hack video camera network
2. Menginstall software ke video camera, dan memanfaatkan sumber daya korban.
3. Attacker menggunakan video camera untuk mengeluarkan DoS attack. Sehingga, victim tidak mengetahui siapa attackernya.



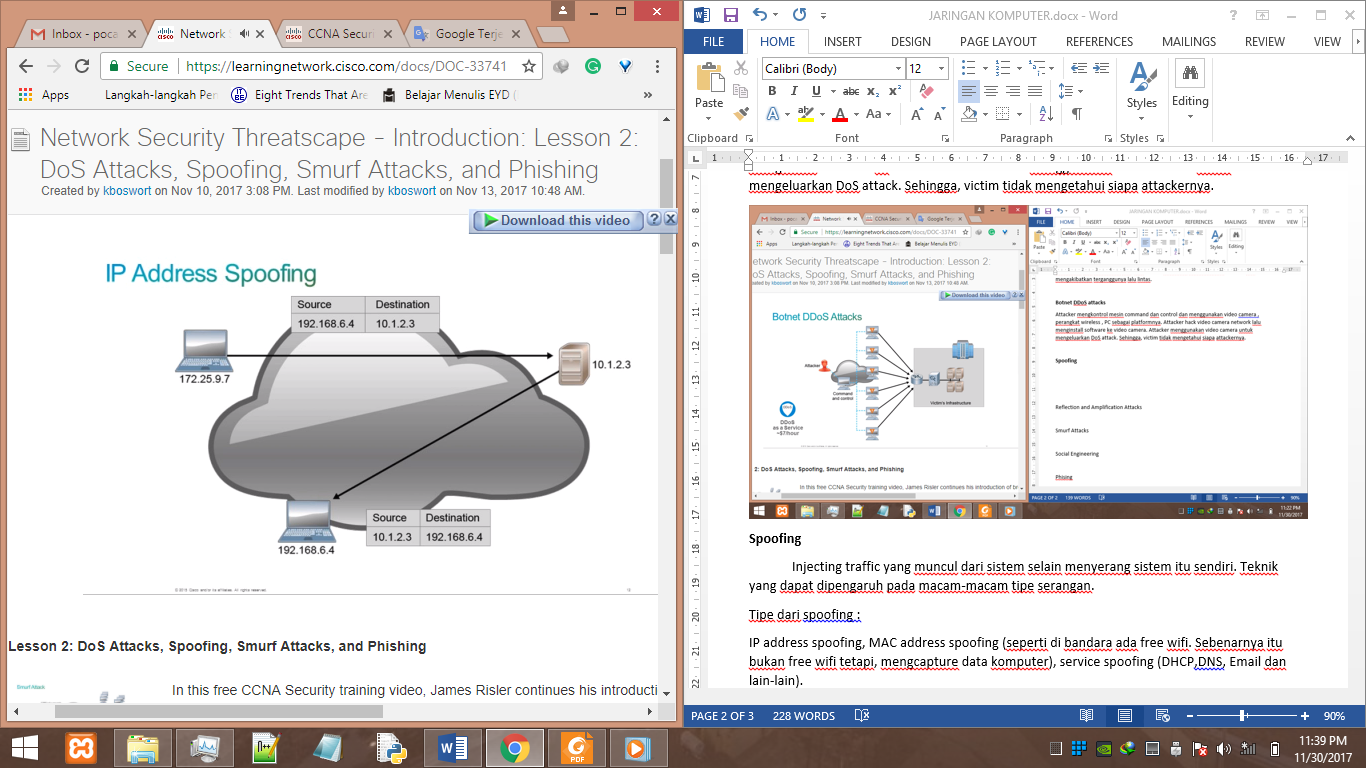
**Spoofing**

Spoofing inject traffic yang muncul untuk menjadi sumber dari sebuah sistem bukan berarti, spoofing menyerang dirinya sendiri melainkan, teknik ini dipengaruh pada macam-macam tipe serangan.

Tipe dari spoofing :

IP address spoofing, MAC address spoofing (seperti di bandara ada free wifi ilegal. Sebenarnya itu bukan free wifi tetapi, mengcapture data komputer kita), service spoofing (DHCP,DNS, Email dan lain-lain).

Contoh IP Spoofing lainnya, pada IP sumber attacker memalsukan alamat IP-nya dengan menggunakan VPN. Lalu, mengirim packet ke IP tujuan dengan alamat IP tujuan kembali yang berbeda dengan yang asli sehingga, IP sumber korban terbanjiri packet melalui IP tujuan.



**Reflection and Amplification Attacks**

Attacker mengirim permintaan paket dengan alamat IP yang d*ispoofing* untuk mendapatkan host lainnya untuk membanjiri komputer korban. Berbeda dengan *amplification attack*, attacker mengirim permintaan paket palsu yang berukuran kecil untuk memperoleh balasan yang besar.

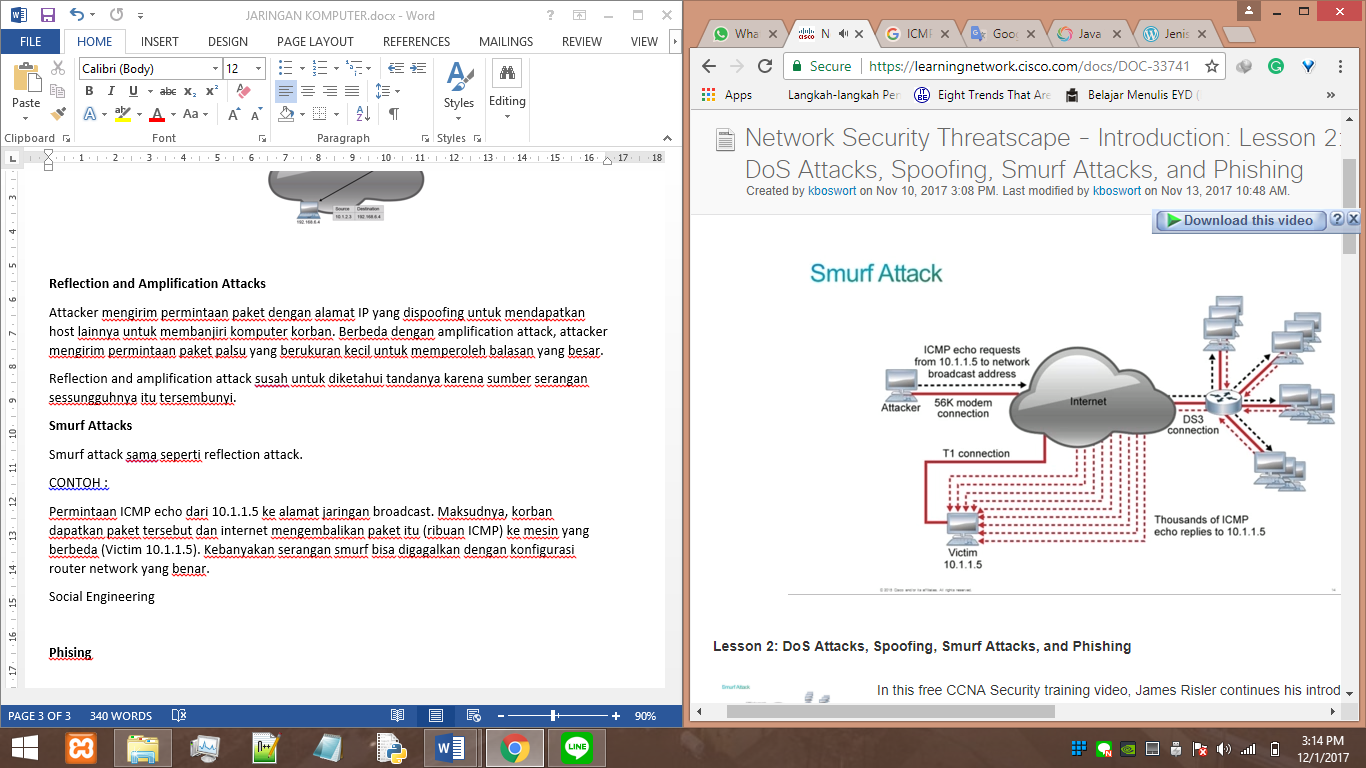
*Reflection and amplification attack* susah untuk diketahui tandanya karena sumber serangan sesungguhnya itu tersembunyi.

**Smurf Attacks**

Smurf attack sama seperti *reflection attack.*

**CONTOH** :

Permintaan ICMP echo dari 10.1.1.5 ke alamat jaringan broadcast. Maksudnya, korban dapatkan paket tersebut dan internet mengembalikan paket itu (ribuan ICMP) ke mesin yang berbeda (*Victim IP* : 10.1.1.5). Kebanyakan serangan smurf bisa digagalkan dengan konfigurasi router network yang benar.



**Phising**

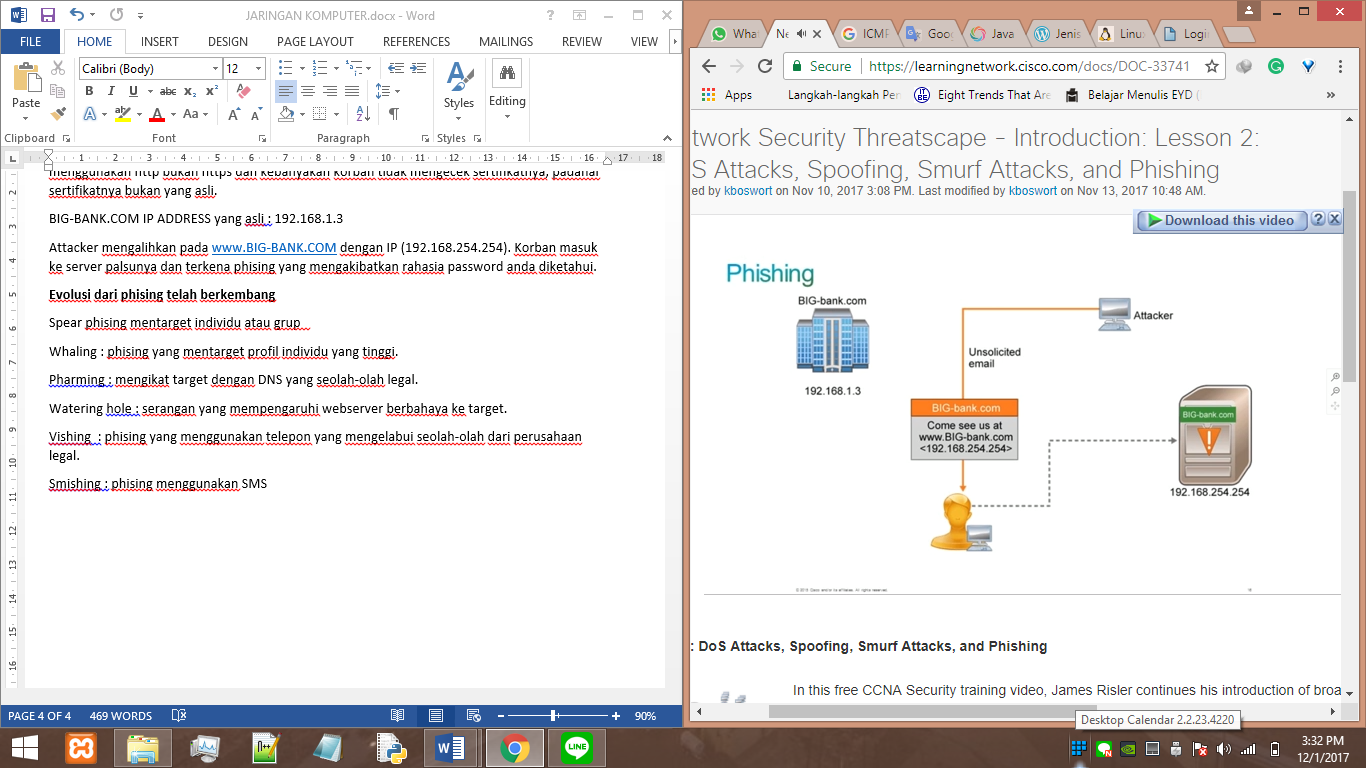
Salah satu contoh dari social engineering.

**Contoh** :

Link bank yang seolah-olah legal mengirim pesan ke email korban dan beralibi bahwa akun anda perlu direset passwordnya. Linknya terlihat legal tetapi, BIGBANK.COM palsu menggunakan http bukan https dan kebanyakan korban tidak mengecek sertifikatnya, padahal sertifikatnya bukan yang asli.

BIG-BANK.COM IP ADDRESS yang asli : 192.168.1.3

Attacker mengalihkan pada [www.BIG-BANK.COM](http://www.BIG-BANK.COM) dengan IP (192.168.254.254). Korban masuk ke server palsunya dan terkena phising yang mengakibatkan rahasia password anda diketahui.



**Evolusi dari phising telah berkembang**

Spear phising mentarget individu atau grup

Whaling : phising yang mentarget profil individu yang tinggi.

Pharming : mengikat target dengan DNS yang seolah-olah legal.

Watering hole : serangan yang mempengaruhi webserver berbahaya ke target.

Vishing : phising yang menggunakan telepon yang mengelabui seolah-olah dari perusahaan legal.

Smishing : phising menggunakan SMS