LAPORAN JARINGAN KOMPUTER
NETWORK SECURITY THREATSCAPE

Nama : Dyah Citra Soraya

NIM : 09011281520107

Kelas : SK5C

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

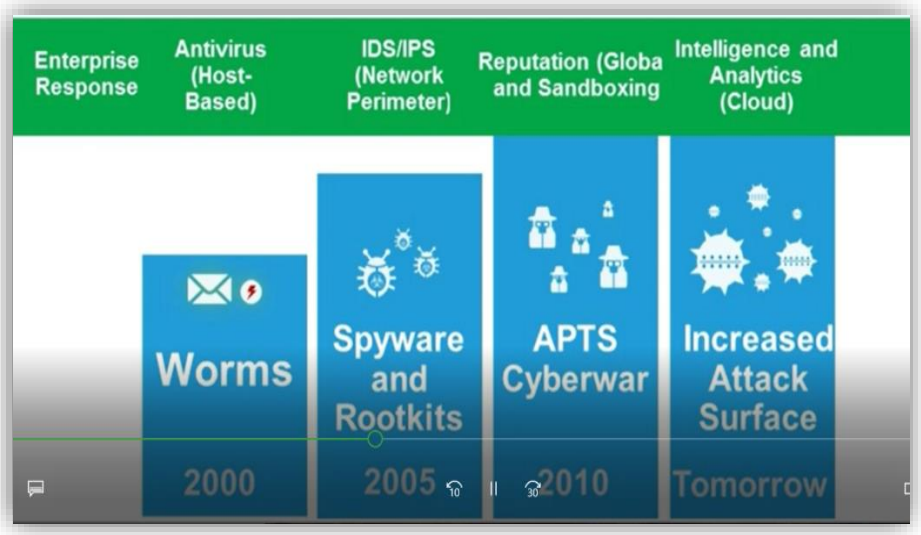
2017

LESSON 1

A. Pengertian Threatscape

Threatscape merupakan beberapa cara yang dikembangkan menjadi perindustrian untuk mengatasi penyerangan – penyerangan yang ada pada jaringan. Yang dimaksud dengan penyerangan (attacker) adalah sebuah penggabungan konsep ancaman pengamanan jaringan dari kosep lama maupun konsep yang baru ataupun (yang sedang dikembangkan). Penyerangan – penyerangan bisa berupa perorangan, kelompok kecil dari hacker, kejahatan yang terorganisir, pemerintahan nasional, ataupun gabungan diatas.

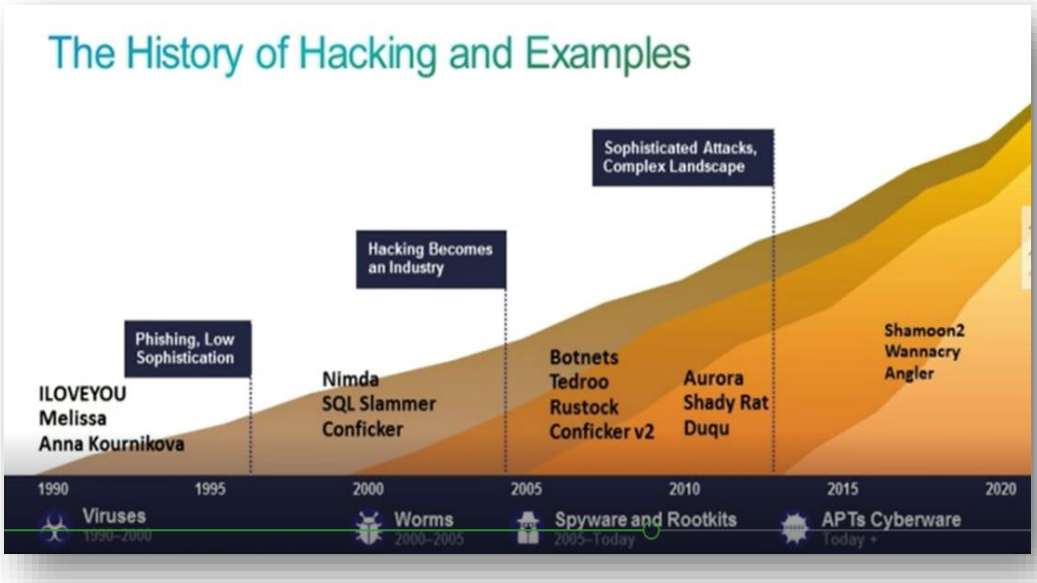
B. Tanggapan Perusahaan Mengenai Attacker yang Ada



- Pada tahun 2000 Penyerangan (Attacker) berupa Worms Threatscapenya adalah Antivirus.
- Pada tahun 2005 Penyerangan (Attacker) berupa spyware dan rootkits Threatscapenya adalah jaringan parameter IDS/IPS.
- Pada tahun 2010 Penyerangan (Attacker) berupa APTS Cyberwar Threatscapenya reputation (global dan sandboxing).
- Dan pada 2011-2020 Penyerangan (Attacker) berupa increased attack surface Threatscapenya adalah cloud (intelligence and analytics).

C. Sejarah dari Hacking dan Contohnya

Penyerangan yang semakin kompleks dan beragam dari tahun ketahun.



D. Bagaimana Perindustrian Hacking Berkesempatan Mendapatkan Uang

Dapat kita lihat dari data diatas bagaimana hacking mampu mendapatkan penghasilan dengan berbagai bentuk sajian seperti (spam, account, keamanan jaringan, info dan data penting) dari berbagai aplikasi ataupun media yang banyak digunakan oleh pengguna internet.

E. Perbedaan Malware dan Attacker Tools

Malware merupakan software yang membuat dokumen pada computer tanpa diketahui oleh pengguna (nama umum dari virus komputer) sedangkan attacker tools adalah hardware yang mampu membuat penyerangan-penyerangan pada computer.

F. Istilah – Istilah pada Threatscape

1. Vulnerability : Salah satu kelemahan yang membahayakan keamanan atau fungsi dari sebuah system.
2. Exploit : Pengguna mesin untuk mempengaruhi sebuah vulnerability yang bertujuan untuk membahayakan sebuah system.
3. Threat : Persoalan atau kejadian yang berpotensi untuk pembuat kerusakan ataupun untuk sebuah asset.
4. Risk : Threat khusus yang berkemungkinan sebagai penyerangan spesifik yang akan mengexploit sebuah vulnerability yang khusus dari sebuah asset.

DAFTAR PUSTAKA

Noname. “CCNA Security Training Videos”. (online) http://learningnetwork.cisco.com/community/learning_center/ccna-security-training-videos. Diakses pada tanggal 29 November 2017.