

TUGAS JARINGAN KOMPUTER



DISUSUN OLEH:

Nama : Meidi Dwi Hafiz

Nim : 09011281520097

Kelas : SK5C

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

**SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
PALEMBANG 2017**

Lesson 1

Threatscapes Introduction and Overview

I. Threatscapes overview

Tidak ada sebuah perusahaan yang bebas dari serangan luar. Penyerang bisa berasal dari mana saja, misal dari seorang, sekumpulan orang, suatu organisasi, pemerintahan, atau bisa jadi 4 gabungan dari itu semua.

Attacker biasanya memiliki pemikiran yang sangat kreatif dalam melakukan ancaman biasanya ia menggunakan metode seperti berikut :

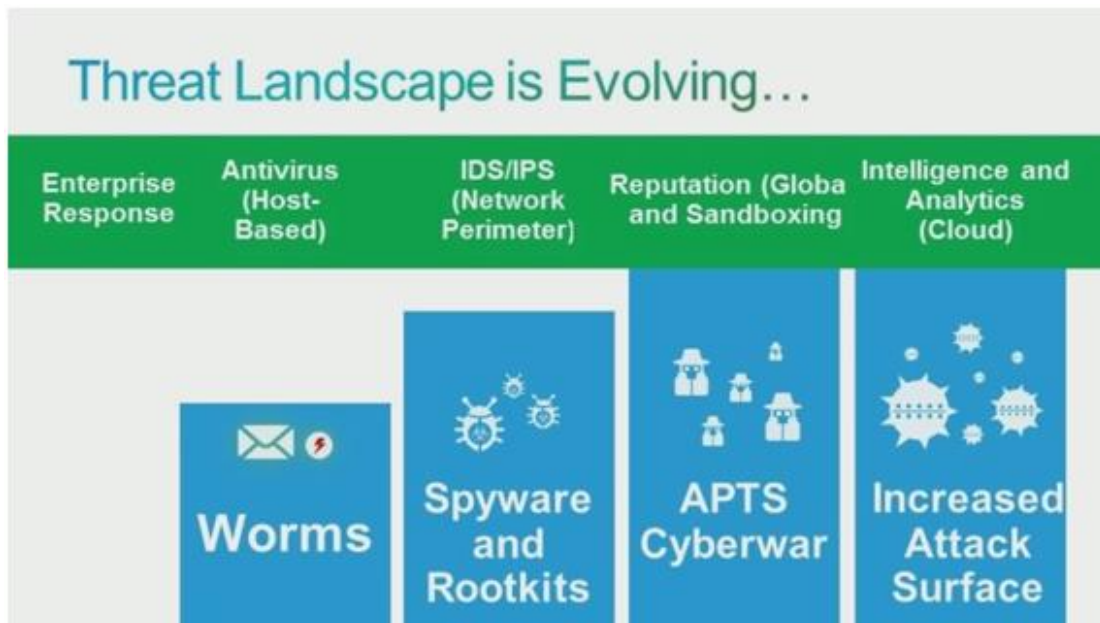
1. Mengkombin konsep Lama dan Baru

Attacker memiliki banyak solusi untuk melakukan ancaman karena ia mengerti semua pengetahuan dalam lingkup cisco, xp ,dan huawei serta juga equipment yang dibutuhkan agar mereka bisa melakukan suatu ancaman.

2. Evolving

Attacker biasanya selalu mengikuti evolusi dalam dunia network yang ada , mereka mengikuti perkembangan dunia network dari hari ke hari , biasanya attacker mengikuti perkembangan network melalui internet.

Beberapa perusahaan besar pun masih terkena ancaman dari para attacker seperti perusahaan Anthem, Ebay, JP Morgan Chase dan sebagainya.



Gambar 1.1 Threat Landscape is Evolving

- **WORMS**

Worm adalah sebuah program komputer berupa malware. Program ini sangat berbahaya yang dapat menyalin sendiri berulang-ulang, pada drive lokal, jaringan, email, atau Internet. Program ini menggunakan jaringan komputer untuk mengirimkan salinan dirinya ke node lainnya (komputer pada jaringan) dan dapat menginfeksi tanpa sepengetahuan pengguna.

Tujuannya ialah untuk mereproduksi, tidak seperti virus yang mencoba untuk menginfeksi, tapi menyalin kode embed ke dalam file lainnya. Hal ini disebabkan oleh kelemahan keamanan pada komputer target. Worm tidak menginfeksi file atau memodifikasi file melainkan menimbulkan kerugian pada jaringan karena worm akan mengkonsumsi bandwidth jaringan, sehingga mengakibatkan speed Internet lambat.

Jenis worm yang paling umum adalah worm email. Sesuai dengan jenisnya, worm email tidak menulari file lainnya seperti halnya virus tetapi mereka hanya membuat salinan dirinya berulang-ulang. worm email melakukan ini melalui email, dengan mengirimkan diri ke alamat email yang ditemukan pada sistem pengguna yang terinfeksi.

- **Spyware and Rootkits**

Spyware adalah program komputer yang dibuat untuk memata-matai komputer korbannya. Awalnya spyware ini digunakan untuk memata-matai profil pengguna komputer dan penggunaannya dalam menampilkan iklan yang sesuai dengan minat

pengguna komputer tersebut. Sedangkan **Rootkit** adalah kumpulan software yang bertujuan untuk menyembunyikan proses, file dan data sistem yang sedang berjalan dari sebuah sistem operasi tempat dia bernaung.

Rootkit awalnya berupa aplikasi yang tidak berbahaya, tetapi belakangan ini telah banyak digunakan oleh malware yang ditujukan untuk membantu penyusup menjaga aksi mereka yang ke dalam sistem agar tidak terdeteksi. rootkit hadir di beragam sistem operasi seperti, Linux, Solaris dan Microsoft Windows. Rootkit ini sering merubah bagian dari sistem operasi dan juga menginstall dirinya sendiri sebagai driver atau modul kernel.

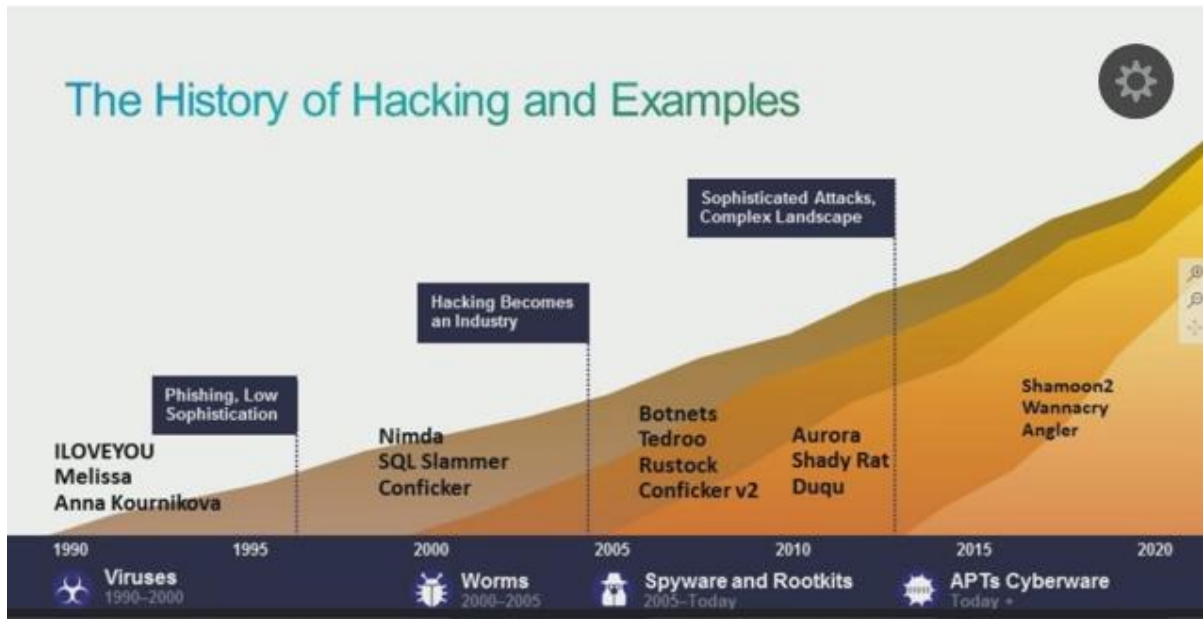
- **APTS Cyberwar**

Aktivitas yang terjadi pada perang cyber ini pada umumnya adalah kegiatan hacking dan anti-hacking yang dilakukan secara 'resmi' oleh negara. Tujuannya mulai dari mencuri data hingga melumpuhkan sistem yang dimiliki oleh negara musuh. Dengan terhubungnya seluruh dunia melalui jaringan internet, Amerika, China, Rusia, Iran, Korea Utara, Korea Selatan, Jepang dan banyak lagi negara eropa dan timur tengah, setiap hari terlibat dalam kegiatan cyber war ini.

Cyber war sendiri bermacam-macam. Mulai dari yang non teknis seperti penyebaran propaganda melalui media sosial, dalam bentuk gambar-gambar maupun artikel atau kegiatan bully mem-bully. Hingga yang luar biasa canggih seperti penyebaran virus stuxnet yang dirilis oleh Israel dengan target melumpuhkan reaktor nuklir Iran, atau peristiwa 'pembajakan' drone Amerika oleh Iran beberapa waktu lalu.

- **Increase Attack Surface**

Internet of Things (IoT) menyebabkan meningkatnya Attack Surface , Attack Surface ialah serangan yang dilakukan attacker yang tertuju pada jumlah total kerentanan pada perangkat komputasi atau jaringan tertentu yang mengakibatkan dapat diakses oleh peretas.



Gambar 1.2 Sejarah hacking dan contohnya

3 Contoh Hacking beserta contoh :

1. Phishing, Low Sophistication

Contoh: pada virus computer ILOVEYOU, Melissa , dan Anna Kournikova

a. ILOVEYOU

Sering disebut Love Bug atau Love Letter, adalah worm komputer yang menyerang puluhan juta komputer pribadi Windows pada dan setelah 5 Mei 2000 di waktu setempat di Filipina ketika mulai menyebar sebagai pesan email dengan subjek line "ILOVEYOU" dan lampiran "LOVE-LETTER-FOR-YOU.txt.vbs".

Ekstensi file yang terakhir ('vbs', jenis file yang diinterpretasikan) paling sering disembunyikan secara default pada komputer Windows pada saat itu (karena ini merupakan ekstensi untuk tipe file yang dikenal oleh Windows), menyebabkan pengguna yang tidak sadar untuk memikirkannya adalah file teks biasa. Membuka attachment mengaktifkan script Visual Basic. Cacing itu merusak mesin lokal, menimpa jenis file acak (termasuk file Office, file gambar, dan file audio; namun setelah menimpa file MP3, virus tersebut akan menyembunyikan file tersebut), dan mengirim salinan dirinya ke semua alamat di Windows Address Book yang digunakan oleh Microsoft Outlook. Sebaliknya, virus Melissa hanya mengirim salinan ke 500 kontak pertama. Hal ini membuatnya menyebar jauh lebih cepat daripada worm email lainnya sebelumnya.

b. Melissa

Melissa adalah virus makro yang menyebar cepat yang didistribusikan sebagai lampiran e-mail yang, ketika dibuka, menonaktifkan sejumlah pengamanan di Word 97 atau Word 2000, dan jika pengguna memiliki program e-mail Microsoft Outlook, menyebabkan virus menjadi kebencian kepada 50 orang pertama di setiap buku alamat pengguna. Meskipun tidak menghancurkan file atau sumber daya lainnya, Melissa berpotensi untuk menonaktifkan server surat perusahaan dan lainnya karena riak distribusi e-mail menjadi gelombang yang jauh lebih besar. Pada hari Jumat, tanggal 26 Maret 1999, Melissa menyebabkan Microsoft Corporation menutup e-mail yang masuk. Intel dan perusahaan lain juga melaporkan akan terpengaruh. Tim Tanggap Darurat Komputer U. S. yang didanai oleh Pertahanan (CERT) mengeluarkan peringatan tentang virus tersebut dan mengembangkan sebuah perbaikan.

c. Anna Kournikova

Anna Kournikova VBS.SST virus komputer, yang dikenal secara informal sebagai "Anna," adalah worm virus yang menggunakan Visual Basic untuk menginfeksi sistem Windows saat pengguna tanpa disadari membuka surat elektronik dengan lampiran yang tampaknya merupakan gambar grafis bahasa Rusia. bintang tenis Anna Kournikova. Namun, saat file dibuka, ekstensi kode klandestin memungkinkan worm tersebut untuk menyalin dirinya ke direktori Windows dan kemudian mengirim file tersebut sebagai lampiran ke semua alamat yang tercantum di buku alamat e-mail Microsoft Outlook Anda.

2. Hacking Becomes an Industry

Contoh pada virus computer Nimda, SQL Slammer , conficker.

a. Nimda

Pertama kali muncul pada tanggal 18 September 2001, Nimda adalah virus komputer yang menyebabkan kemunduran lalu lintas saat beriak di Internet, menyebar melalui empat metode yang berbeda, menginfeksi komputer yang berisi server Web Microsoft, Internet Information Server (IIS), dan pengguna komputer yang membuka Lampiran email. Seperti sejumlah virus pendahulu, muatan Nimda tampaknya merupakan kemunduran lalu lintas - yaitu, tampaknya tidak

menghancurkan file atau menyebabkan kerusakan selain waktu yang cukup lama yang mungkin hilang akibat melambatnya atau hilangnya lalu lintas yang dikenal sebagai penyangkalan - pelayanan dan pemulihan sistem yang terinfeksi. Dengan serangan multi-cabangnya, Nimda nampaknya merupakan virus yang paling bermasalah dari jenisnya yang belum muncul. Namanya (mundur untuk "admin") ternyata mengacu pada file "admin.dll" yang, ketika dijalankan, terus menyebarkan virus.

b. SQL Slammer

SQL Slammer adalah worm yang menargetkan unpatched Microsoft SQL 2000 servers. Worm ini menyebar antar server, meningkatkan lalu lintas pada port UDP 1434 dan menyebabkan lalu lintas jaringan berat yang dapat memperlambat kinerja jaringan dan menyebabkan penolakan layanan. SQL slammer tidak membawa muatan yang merusak. Meski namanya, itu tidak menggunakan bahasa SQL. Home PC umumnya tidak terpengaruh oleh worm ini. Karena tetap berada dalam memori sistem, mudah untuk menghapusnya.

c. Conficker

Conficker (juga disebut Downup, Downandup dan Kido) adalah worm yang muncul pada Oktober 2008.[1] Conficker menyerang Windows dan paling banyak ditemui dalam Windows XP. Microsoft merilis patch untuk menghentikan worm ini pada tanggal 15 Oktober 2008.[2] Heinz Heise memperkirakan Conficker telah menginfeksi 2.5 juta PC pada 15 Januari 2009,[3] sementara The Guardian memperkirakan 3.5 juta PC terinfeksi.[4] Pada 16 Januari 2009, worm ini telah menginfeksi hampir 9 juta PC,[5] menjadikannya salah satu infeksi yang paling cepat menyebar dalam waktu singkat.

3. Sophisticated Attacks, Complex Landscape

Contoh: pada virus computer , Duqu

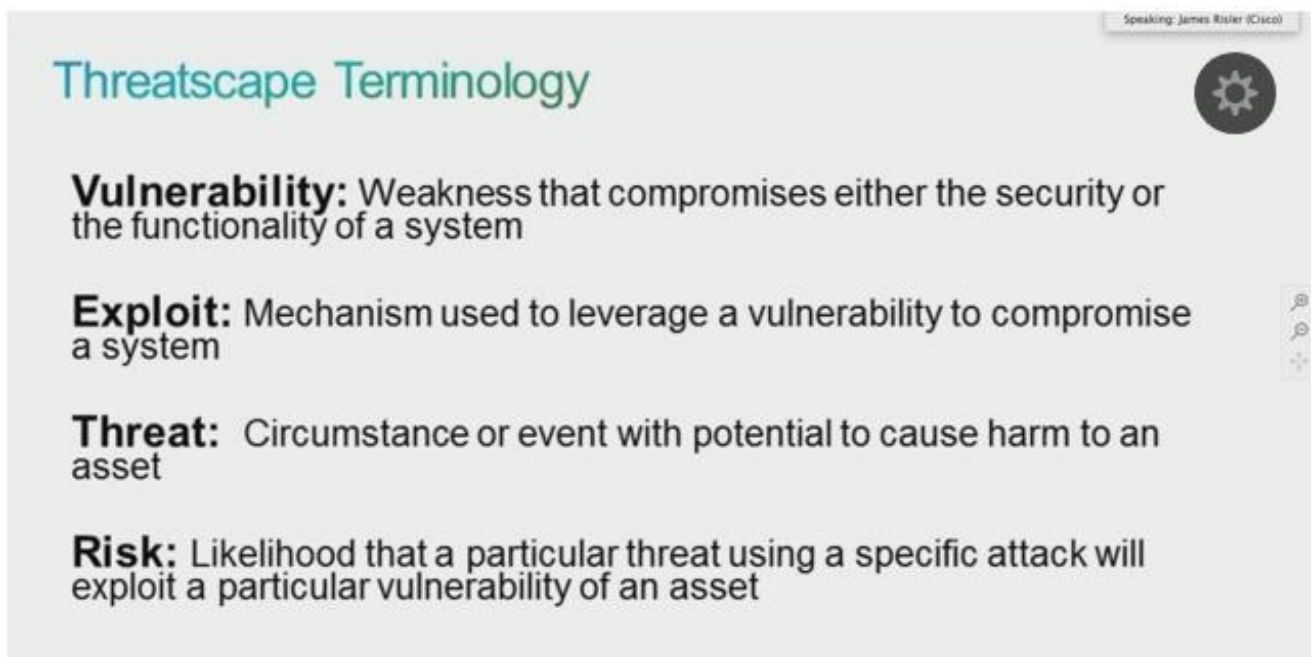
a. Duqu

Duqu adalah kumpulan malware komputer yang ditemukan pada tanggal 1 September 2011, yang diduga terkait dengan worm Stuxnet dan telah dibuat oleh Unit 8200. [1] Laboratorium Kriptografi dan Keamanan Sistem (Laboratorium

CrySyS) [2] Universitas Teknologi dan Ekonomi Budapest di Hungaria menemukan ancaman tersebut, menganalisis malware tersebut, dan menulis sebuah laporan setebal 60 halaman [3] yang menamai ancaman Duqu [4]. Duqu mendapat namanya dari awalan "~ DQ" yang diberikannya ke nama file yang dibuatnya.

Malware and attacker tools :

1. Backdoors
2. Downloaders and droopers
3. Rootkits
4. Pivots
5. Keylogger
6. Exploits
7. Payload



The image is a screenshot of a presentation slide titled "Threatscape Terminology". The slide is light gray with a dark gray header area. In the top right corner of the header, it says "Speaking: James Risler (Cisco)" next to a gear icon. The main content of the slide lists four definitions:

- Vulnerability:** Weakness that compromises either the security or the functionality of a system
- Exploit:** Mechanism used to leverage a vulnerability to compromise a system
- Threat:** Circumstance or event with potential to cause harm to an asset
- Risk:** Likelihood that a particular threat using a specific attack will exploit a particular vulnerability of an asset

Threatscape Terminology

Cara hacker industri memonetisasi suatu kesempatan



Referensi :

[https://learningnetwork.cisco.com/community/learning_center/ccna-security-training-videos.](https://learningnetwork.cisco.com/community/learning_center/ccna-security-training-videos)