**Laporan Rangkuman**

**Jaringan Komputer**

**Rangkuman Lesson Cisco**



Disusun Oleh :

 Nama : M Rasyid Darmawan

 NIM : 09011281520108

 Kelas : SK5C

 Dosen Pengampu : Deris Setiawan, M.T

UNIVERSITAS SRIWIJAYA

SISTEM KOMPUTER

2017

**Threatscapes Introduction and Overview**

**Threatscapes overview**

Tidak ada perusahan yang bebas dari serangan luar dari attacker dan hacker

Attacker bisa berasal dari :

1. Seorang individual
2. Sekumpulan atau beberapa team hacker yang berskala kecil
3. Organisasi criminal
4. Pemerintahan
5. Gabungan dari 4 di atas

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

1. Melakukan kombinasi terhadap konsep yang lama dengan yang 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 ancaman(attack)

1. 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

Masalahnya

 Perusahaan besar-besar pun masih terkena ancaman dari para attacker seperti perusahaan

1. Anthem
2. Target
3. Ebay
4. Home depot
5. JP Morgan Chase

Padahal perusahaan-perusahaan besar di atas sudah mengeluarkan uang sangat banyak sekitar beberapa juta dolar untuk meningkatkan keamanan networknya tetapi masih juga terkena hack dari para attacker.

**Threat Landscape is Evolving**



1. Worms

Worm adalah sebuah program komputer salah satu [malware](http://en.wikipedia.org/wiki/Malware). Program ini berbahaya yang dapat menyalinan sendiri berulang-ulang, pada drive lokal, jaringan, email, atau [Internet](http://en.wikipedia.org/wiki/Internet). Program ini menggunakan jaringan komputer untuk mengirimkan salinan dirinya ke node lainnya (komputer pada jaringan) dan dapat menginfeksi tanpa sepengetahuan pengguna.  tujuan utama Worm adalah 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 bandwith 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.

1. Spyware and Rootkits

[Spyware](https://www.maxmanroe.com/perbedaan-malware-virus-trojan-spyware-dan-worm.html) adalah program komputer yang dibuat untuk memata-matai komputer korbannya. Awalnya [spyware](https://www.maxmanroe.com/perbedaan-malware-virus-trojan-spyware-dan-worm.html) ini digunakan untuk memata-matai profil pengguna komputer dan penggunaannya dalam menampilkan iklan yang sesuai dengan minat pengguna komputer tersebut.

**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.

1. 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.

1. 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.

**Sejarah Hacking dan contohya**



Bisa kita lihat pada gambar di atas ada 3 macam hack

1. Phishing, Low Sophistication

Contohnya pada virus computer ILOVEYOU, Melissa , Anna Kournikova

* 1. ILOVEYOU, kadang-kadang disebut sebagai 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.
	2. 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.
	3. 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.
1. Hacking Becomes an Industry

Contohnya pada virus computer Nimda, SQL Slammer , conficker

* 1. 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.
	2. 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.
	3. 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.
1. Sophisticated Attacks, Complex Landscape

Contohnya pada virus computer , Duqu

* 1. 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

**Gambar ini menjelaskan bahwa itu adalah penghasilan yang di dapat oleh para hacker industri jika sukses menyelesaikan pekerjaannya**



Terdapat 11 Bidang tempat yaitu :

1. Social Security

Jaminan sosial adalah salah satu bentuk perlindungan sosial yang diselenggarakan oleh negara guna menjamin warganegaranya untuk memenuhi kebutuhan hidup dasar yang layak, sebagaimana dalam deklarasi PBB tentang HAM tahun 1948 dan konvensi ILO No.102 tahun 1952. Hacker hanya mendapatkan penghasilan $1 per orang.

1. DDoS as a Service

Serangan DoS (bahasa Inggris: denial-of-service attacks') adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut. Hacker mendpatkan $7 per jam.

1. Medical Report

Rekam Medis adalah hasil perekaman yang berupa keterangan mengenai hasil pengobatan pasien, sedangkan rekam kesehatan yaitu hasil perekaman yang berupa keterangan mengenai kesehatan pasien, Hacker bisa mendapatkan >$50.

1. Credit Card Data

Data Credit Card seseorang, hacker bisa mendapatkan $0,25 - $60 tergantung data siapa yang ingin dicuri

1. Bank ACC Info

Info Bank seseorang seperti saldo , nomor rekening , pembukuan dan lain2, Hacker bisa mendapatkan penghasilan yang sangat besar >$1000 tergantung dari tipe akun dan isinya

1. Mobile Malware

Malware untuk mengattack handphone seseorang , bisa menghasilkan $150 dalam satu kali pekerjaan

1. Spam Email

Menyepam email seseorang sehingga tidak bisa dibuka , penghasilannya $50 – $500k / email

1. Exploits

Exploit adalah sebuah kode yang menyerang keamanan komputer secara spesifik. Exploit banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari kelemahan (vulnerability) pada komputer tujuan. Penghasilannya $100k - $300k

1. Malware Development

 Penghasilan yang di dapatkan hacker sangat besar mencapai $250.

1. Facebook ACC

 Melakukan Hack akun Facebook dengan penghasilan $1/15 teman yang ada di dalam akun tersebut

1. Global Cybercrime Market

Kejahatan dunia maya (Inggris: cybercrime) adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/carding, confidence fraud, penipuan identitas, pornografi anak, dll. Ini merupakan bidang yang menghasilkan penghasilan paling besar bagi seorang besar angkanya menyentuh $450B - $1T

**Peralatan dan Malware yang digunakan Oleh Attacker**



1. Backdoors

Backdoor atau "pintu belakang", dalam keamanan sistem komputer, merujuk kepada mekanisme yang dapat digunakan untuk mengakses sistem, aplikasi, atau jaringan, selain dari mekanisme yang umum digunakan (melalui proses logon atau proses autentikasi lainnya).

1. Downloaders and droppers

A Trojan that contains malicious or potentially unwanted software, which the Trojan places and installs on the host computer.

1. Rootkits

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.

1. Pivots
2. Keyloggers

Keylogger adalah sebuah program yang dibuat untuk merekam pengentrian data melalui keyboard dan memasukanya ke dalam log (catatan). Tapi seiring berkembang versi dan tipenya, kini keylogger pun bisa merekam aktifitas mouse, clipboard,web browser dan visual surveillance (gambar hasil capture otomatis layar monitor). Keylogger terbagi dalam dua jenis, yaitu jenis hardware dan software.

1. Exploits

Exploit adalah sebuah kode yang menyerang keamanan komputer secara spesifik. Exploit banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari kelemahan (vulnerability) pada komputer tujuan.

1. Payloads

Payload : Efek yang ditimbulkan oleh serangan virus. Dalam beberapa kasus, dapat juga dipakai untuk menyebut virus yang berkaitan dengan dropper

**Threatscape Terminology**



* Vulnerability
	+ Suatu kelemahan yang dapat membahayakan keamanan atau fungsionalitas suatu system.
* Exploit
	+ Mekanisme yang digunakan untuk memanfaatkan kerentanan terhadap sebuah system.
* Threat
	+ Keadaan atau kejadian yang berpotensi membahayakan asset.
* Risk
	+ Kemungkinan bahwa ancaman tertentu yang menggunakan serangan tertentu akan memanfaatkan kerentanan tertentu dari asset.