**TUGAS JARINGAN KOMPUTER**



DISUSUN OLEH:

Nama : Juan Alkasar

Nim : 09011281520092

Kelas : SK 5 C

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

**SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**PALEMBANG 2017**

**Tugas menganalisa sebuah video yang salah satunya berjudul**

Threatscapes Introduction and Overview



Threatscapes overview



Pada video yang sudah saya tonton saya mengetahui bahwa Tidak ada perusahan yang bebas atau aman dari serangan luar,hal itu terjadi dikarenakan oleh biasanya disebut attacker.

Attacker biasanya 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

Threat Landscape is Evolving atau



Kita akan membahas satu persatu pada gambar diatas

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.

Berikut ini adalah 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.
4. **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.
4. **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.
2. Aurora ditujukan untuk mencuri data-data sensitif para aktivis HAM Cina mencuat satu tahun sebelumnya.
3. Operation Shady RAT

merupakan kampanye peretasan yang menjadikan 72 jaringan organisasi di seluruh dunia sebagai targetnya termasuk pemerintah Amerika Serikat, pemerintah Inggris, 12 situs pertahanan Amerika Serikat dan banyak perusahaan teknologi lain di seluruh dunia.

Aksi ini merupakan tindakan yang dilakukan secara bertahan dari sebelum tahun 2006 sampai 2010 lalu. Belum ada alasan dan informasi pasti apa yang mendasari dilakukannya Operation Shady RAT.



Gambar diatas merupakan Membuat atau mendapatkan uang dari hacking pada global cybercrime market karena itulah termasuk threat atau ancaman



Gangguan atau virus, worm, trojan horse, sebagian besar rootkit, spyware, adware yang tidak jujur, serta software-software lain yang berbahaya dan tidak diinginkan oleh pengguna PC dan alat penyerang

Dan gangguan Polymorphic adalah kode pemograman yang digunakan oleh program untuk bermutasi sekaligus mempertahankan algoritma asli tetap utuh. Dalam arti katanya, perubahan itu sendiri berjalan sesuai kriteria program asli.



**Ancaman terminology**

**Vulnerability**

akan digunakan oleh hacker sebagai jalan untuk masuk kedalam sistem secara ilegal. Hacker biasanya akan membuat Exploit yang desesuaikan dengan vulnerability yang telah ditemukan nya.

**exploit**

adalah virus conficker, salah satu teknik penyebaran virus conficker ini adalah dengan memanfaatkan local exploit komponen Windows yang digunakan untuk menampilkan thumbnail pada jendela explorer. Kegagalan komponen Windows ini menyebabkan kode virus tereksekusi secara otomatis tanpa perlu korban mengklik file yang bervirus.

**thread**

disini adalah keadaan atau kejadian yang berpotensi menyebabkan kerusakan pada asset.

**risk**
Kemungkinan bahwa ancaman tertentu yang menggunakan serangan spesifik akan memanfaatkan kerentanan tertentu dari suatu asset.