**TUGAS JARKOM**



DISUSUN OLEH:

Nama : Therio Anggara

Nim : 09011281520112

Kelas : SK 5C

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

**SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**PALEMBANG 2017**

Threatscapes Introduction and Overview



Threatscapes overview

Kesimpulan dari video yang ada ialah tidak ada satupun yang aman dari kejahatan cyber,perusahaan-perusahaan besar pun masih rentan akan serangan-serangan dari pihak yang tidak bertanggung jawab

Attacker biasanya berasal dari :

1. Seorang individu
2. Sekumpulan atau team hacker dalam skala kecil
3. Organisasi criminal
4. Pemerintahan
5. Gabungan

Attacker biasanya memiliki pemikiran yang sangat kreatif dalam melakukan ancaman

* metode yang biasa digunakan
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



1. **Worms**

Istilah worm diambil dari bahasa inggris yang berarti cacing, dalam hal ini kita lebih tepat menyebutnya sebagai cacing komputer. Penamaan worm atau cacing untuk program ini memang merujuk kepada kemampuannya untuk mengganggu sistem komputer. Adapun **pengertian worm adalah** sebuah program yang mempunyai ukuran kecil yang mampu untuk berjalam pada sebuah sistem operasi komputer ataupun sistem jaringan komputer, program worm mempunyai kemampuan untuk mengembangbiakan dirinya sendiri pada kedua sistem tersebut..

1. **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.

**Rootkit**  adalah suatu software yang dirancang khusus untuk memanipulasi sistem operasi secara langsung ke hardware.

Menurut spesialis antivirus Anvie Anzav, RootKit yang memiliki akses yang lebih tinggi daripada administrator, sama seperti sistem operasi. "Awalnya RootKit diciptakan untuk membantu administrator mengembalikan password yang hilang tapi justru disalahgunakan untuk merusak, membuat virus, bahkan membuat bom

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**
5. 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.
6. 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.
7. **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



**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.