Copyright © September 2023

PERTEMUAN 2
SERANGAN, KONSEP DAN TEKNIK

Bab ini membahas cara para profesional keamanan siber menganalisis apa yang terjadi setelah serangan siber. Ini menjelaskan kerentanan perangkat lunak dan perangkat keras keamanan dan berbagai kategori kerentanan keamanan. Berbagai jenis perangkat lunak berbahaya (dikenal sebagai malware) dan gejala malware dibahas. Berbagai cara penyerang dapat menyusup ke sistem tercakup, serta serangan penolakan layanan. Sebagian besar serangan siber modern dianggap sebagai serangan campuran. Serangan campuran menggunakan beberapa teknik untuk menyusup dan menyerang sistem. Ketika serangan tidak dapat dicegah, adalah tugas profesional keamanan siber untuk mengurangi dampak serangan itu.

1.1. MENGANALISA SERANGAN CYBER

1.1.1. Security Vulnerabilities and Exploit

1. Menemukan Security Vulnerabilities

Security vulnerabilities adalah segala jenis cacat perangkat lunak atau perangkat keras. Setelah mendapatkan pengetahuan tentang kerentanan, pengguna jahat mencoba untuk mengeksploitasinya. Sebuah mengeksploitasi adalah istilah yang digunakan untuk menggambarkan sebuah program yang ditulis untuk mengambil keuntungan dari kerentanan diketahui. Tindakan menggunakan eksploitasi terhadap kerentanan disebut sebagai serangan. Tujuan serangan adalah untuk mendapatkan akses ke sistem, data yang dihostingnya, atau sumber daya tertentu.

Copyright © September 2023

a. Software vulnerabilities

Software vulnerabilities biasanya disebabkan oleh kesalahan dalam sistem operasi atau kode aplikasi, terlepas dari semua upaya yang dilakukan perusahaan untuk menemukan dan menambal kerentanan perangkat lunak, kerentanan baru sering muncul ke permukaan. Microsoft, Apple, dan produsen sistem operasi lainnya merilis tambalan dan pembaruan hampir setiap hari. Pembaruan aplikasi juga umum. Aplikasi seperti browser web, aplikasi seluler, dan server web sering diperbarui oleh perusahaan atau organisasi yang bertanggung jawab atasnya.

Pada tahun 2015, kerentanan utama, yang disebut SYNful Knock, ditemukan di Cisco IOS. Kerentanan ini memungkinkan penyerang untuk mendapatkan kendali atas router tingkat perusahaan, seperti router Cisco 1841, 2811, dan 3825 yang lama. Penyerang kemudian dapat memantau semua komunikasi jaringan dan memiliki kemampuan untuk menginfeksi perangkat jaringan lain. Kerentanan ini diperkenalkan ke dalam sistem ketika versi IOS yang diubah dipasang di router. Untuk menghindari hal ini, selalu verifikasi integritas gambar IOS yang diunduh dan batasi akses fisik peralatan hanya untuk personel yang berwenang.

Tujuan pembaruan perangkat lunak adalah untuk tetap terkini dan menghindari eksploitasi kerentanan. Sementara beberapa perusahaan memiliki tim pengujian penetrasi yang didedikasikan untuk mencari, menemukan, dan menambal kerentanan perangkat lunak sebelum mereka dapat dieksploitasi, peneliti keamanan pihak ketiga juga mengkhususkan diri dalam menemukan kerentanan dalam perangkat lunak.

Project Zero Google adalah contoh yang bagus dari praktik semacam itu. Setelah menemukan sejumlah kerentanan dalam berbagai perangkat lunak yang digunakan oleh

Copyright © September 2023

pengguna akhir, Google membentuk tim permanen yang didedikasikan untuk menemukan kerentanan perangkat lunak. Riset Keamanan Google dapat ditemukan di sini .

b. Hardware vulnerabilities

Hardware vulnerabilities sering kali disebabkan oleh kelemahan desain perangkat keras. Memori RAM misalnya, pada dasarnya adalah kapasitor yang dipasang sangat dekat satu sama lain. Ditemukan bahwa, karena kedekatan, perubahan konstan yang diterapkan pada salah satu kapasitor ini dapat memengaruhi kapasitor tetangga. Berdasarkan cacat desain itu, eksploitasi yang disebut Rowhammer telah dibuat. Dengan berulang kali menulis ulang memori di alamat yang sama, eksploitasi Rowhammer memungkinkan data diambil dari sel memori alamat terdekat, bahkan jika sel tersebut dilindungi.

Kerentanan perangkat keras khusus untuk model perangkat dan umumnya tidak dieksploitasi melalui upaya kompromi acak. Sementara eksploitasi perangkat keras lebih sering terjadi pada serangan yang sangat bertarget, perlindungan malware tradisional dan keamanan fisik adalah perlindungan yang cukup untuk pengguna sehari-hari.

1.1.2. Jenis Security vulnerabilities

1. Kategori Security vulnerabilities

Sebagian besar Security vulnerabilities perangkat lunak termasuk dalam salah satu kategori berikut:

a. Buffer overflow

Kerentanan ini terjadi ketika data ditulis di luar batas buffer. Buffer adalah area memori yang dialokasikan untuk suatu aplikasi. Dengan mengubah data di luar batas

Copyright © September 2023

buffer, aplikasi mengakses memori yang dialokasikan untuk proses lain. Hal ini dapat menyebabkan sistem crash, kompromi data, atau memberikan eskalasi hak istimewa.

b. Non-validated input

Program sering kali bekerja dengan input data. Data yang masuk ke program ini mungkin berisi konten berbahaya, yang dirancang untuk memaksa program berperilaku dengan cara yang tidak diinginkan. Pertimbangkan sebuah program yang menerima gambar untuk diproses. Pengguna jahat dapat membuat file gambar dengan dimensi gambar yang tidak valid. Dimensi yang dibuat dengan jahat dapat memaksa program untuk mengalokasikan buffer dengan ukuran yang salah dan tidak terduga.

c. Race conditions

Kerentanan ini terjadi ketika output dari suatu peristiwa bergantung pada output yang dipesan atau berjangka waktu. Kondisi balapan menjadi sumber kerentanan ketika peristiwa yang dipesan atau diatur waktu yang diperlukan tidak terjadi dalam urutan yang benar atau waktu yang tepat.

d. Weaknesses in security practices

Sistem dan data sensitif dapat dilindungi melalui teknik seperti otentikasi, otorisasi, dan enkripsi. Pengembang tidak boleh mencoba membuat algoritme keamanan mereka sendiri karena kemungkinan akan menimbulkan kerentanan. Sangat disarankan agar pengembang menggunakan pustaka keamanan yang telah dibuat, diuji, dan diverifikasi.

e. Access-control problems

Kontrol akses adalah proses mengontrol siapa yang melakukan apa dan berkisar dari mengelola akses fisik ke peralatan hingga menentukan siapa yang memiliki akses ke

Copyright © September 2023

sumber daya, seperti file, dan apa yang dapat mereka lakukan dengannya, seperti membaca atau mengubah berkas. Banyak kerentanan keamanan diciptakan oleh penggunaan kontrol akses yang tidak tepat.

Hampir semua kontrol akses dan praktik keamanan dapat diatasi jika penyerang memiliki akses fisik ke peralatan target. Misalnya, apa pun yang Anda atur izin filenya, sistem operasi tidak dapat mencegah seseorang melewati sistem operasi dan membaca data langsung dari disk. Untuk melindungi mesin dan data yang dikandungnya, akses fisik harus dibatasi dan teknik enkripsi harus digunakan untuk melindungi data agar tidak dicuri atau rusak.

1.1.3. Jenis Malware dan Gejalanya

1. Jenis Malware

Kependekan dari Malicious Software, malware adalah kode apa pun yang dapat digunakan untuk mencuri data, melewati kontrol akses, atau membahayakan, atau membahayakan sistem. Berikut adalah beberapa jenis malware yang umum: Jenis Malware.

a. Spyware

Malware ini dirancang untuk melacak dan memata-matai pengguna. Spyware sering menyertakan pelacak aktivitas, pengumpulan keystroke, dan pengambilan data. Dalam upaya untuk mengatasi langkah-langkah keamanan, spyware sering memodifikasi pengaturan keamanan. Spyware sering menggabungkan dirinya dengan perangkat lunak yang sah atau dengan kuda Trojan.

b. Adware

Perangkat lunak yang didukung iklan dirancang untuk mengirimkan iklan secara otomatis. Adware sering diinstal dengan beberapa versi perangkat lunak. Beberapa

Copyright © September 2023

adware dirancang untuk hanya mengirimkan iklan tetapi juga umum untuk adware datang dengan spyware.

c. Bot

Dari kata robot, bot adalah malware yang dirancang untuk melakukan tindakan secara otomatis, biasanya online. Sementara kebanyakan bot tidak berbahaya, salah satu peningkatan penggunaan bot berbahaya adalah botnet. Beberapa komputer terinfeksi bot yang diprogram untuk diam-diam menunggu perintah yang diberikan oleh penyerang.

d. Ransomware

Malware ini dirancang untuk menahan sistem komputer atau data yang dikandungnya hingga pembayaran dilakukan. Ransomware biasanya bekerja dengan mengenkripsi data di komputer dengan kunci yang tidak diketahui pengguna. Beberapa versi ransomware lain dapat memanfaatkan kerentanan sistem tertentu untuk mengunci sistem. Ransomware disebarkan oleh file yang diunduh atau beberapa kerentanan perangkat lunak.

e. Scareware

Ini adalah jenis malware yang dirancang untuk membujuk pengguna agar mengambil tindakan tertentu berdasarkan rasa takut. Scareware memalsukan jendela pop-up yang menyerupai jendela dialog sistem operasi. Jendela-jendela ini menyampaikan pesan palsu yang menyatakan bahwa sistem berisiko atau membutuhkan eksekusi program tertentu untuk kembali ke operasi normal. Pada kenyataannya, tidak ada masalah yang dinilai atau

Copyright © September 2023

terdeteksi dan jika pengguna setuju dan menghapus program yang disebutkan untuk dijalankan, sistemnya akan terinfeksi malware.

f. Rootkit

Malware ini dirancang untuk memodifikasi sistem operasi untuk membuat pintu belakang. Penyerang kemudian menggunakan pintu belakang untuk mengakses komputer dari jarak jauh. Kebanyakan rootkit memanfaatkan kerentanan perangkat lunak untuk melakukan eskalasi hak istimewa dan memodifikasi file sistem. Rootkit juga umum untuk memodifikasi forensik sistem dan alat pemantauan, membuatnya sangat sulit untuk dideteksi. Seringkali, komputer yang terinfeksi rootkit harus dihapus dan diinstal ulang.

g. Virus

Virus adalah kode executable berbahaya yang dilampirkan ke file executable lainnya, seringkali program yang sah. Sebagian besar virus memerlukan aktivasi pengguna akhir dan dapat diaktifkan pada waktu atau tanggal tertentu. Virus bisa tidak berbahaya dan hanya menampilkan gambar atau bisa merusak, seperti yang mengubah atau menghapus data. Virus juga dapat diprogram untuk bermutasi untuk menghindari deteksi. Sebagian besar virus sekarang disebarkan oleh drive USB, disk optik, jaringan berbagi, atau email.

h. Trojan horse

Trojan adalah malware yang melakukan operasi jahat dengan kedok operasi yang diinginkan. Kode berbahaya ini mengeksploitasi hak istimewa pengguna yang menjalankannya. Seringkali, Trojan ditemukan di file gambar, file audio, atau game. Trojan horse berbeda dari virus karena mengikat dirinya ke file yang tidak dapat dieksekusi.

i. Worms

Copyright © September 2023

Worms adalah kode berbahaya yang mereplikasi dirinya sendiri dengan mengeksploitasi kerentanan secara independen dalam jaringan. Worm biasanya memperlambat jaringan. Sedangkan virus membutuhkan program host untuk berjalan, worm dapat berjalan dengan sendirinya. Selain infeksi awal, mereka tidak lagi memerlukan partisipasi pengguna. Setelah host terinfeksi, worm dapat menyebar dengan sangat cepat melalui jaringan. Cacing memiliki pola yang serupa. Mereka semua memiliki kerentanan yang memungkinkan, cara untuk menyebarkan diri mereka sendiri, dan semuanya mengandung muatan.

Worms bertanggung jawab atas beberapa serangan paling dahsyat di Internet. Seperti yang ditunjukkan pada Gambar 1, pada tahun 2001 worm Code Red telah menginfeksi 658 server. Dalam 19 jam, worm telah menginfeksi lebih dari 300.000 server seperti yang ditunjukkan pada Gambar 2.

j. Man-In-The-Middle (MitM)

MitM memungkinkan penyerang untuk mengambil kendali atas perangkat tanpa sepengetahuan pengguna. Dengan tingkat akses itu, penyerang dapat mencegat dan menangkap informasi pengguna sebelum menyampaikannya ke tujuan yang diinginkan. Serangan MitM banyak digunakan untuk mencuri informasi keuangan. Banyak malware dan teknik yang ada untuk memberi penyerang kemampuan MitM.

k. Man-In-The-Mobile (MitMo)

Variasi dari man-in-middle, MitMo adalah jenis serangan yang digunakan untuk mengambil kendali atas perangkat seluler. Saat terinfeksi, perangkat seluler dapat diinstruksikan untuk mengekstrak informasi sensitif pengguna dan mengirimkannya ke penyerang. ZeuS, contoh eksploitasi dengan kemampuan MitMo, memungkinkan

Copyright © September 2023

penyerang secara diam-diam menangkap pesan SMS verifikasi 2 langkah yang dikirim ke pengguna.

2. Gejala Malware

Terlepas dari jenis malware yang menginfeksi sistem, berikut adalah gejala malware yang umum:

- Ada peningkatan penggunaan CPU.
- Ada penurunan kecepatan komputer.
- Komputer sering macet atau macet.
- Ada penurunan kecepatan browsing Web.
- Ada masalah yang tidak dapat dijelaskan dengan koneksi jaringan.
- File dimodifikasi.
- File dihapus.
- Ada file, program, atau ikon desktop yang tidak dikenal.
- Ada proses yang tidak diketahui berjalan.
- Program dimatikan atau dikonfigurasi ulang sendiri.
- Email sedang dikirim tanpa sepengetahuan atau persetujuan pengguna.

1.1.4. Metode Infiltrasi

1. Social Engineering

Copyright © September 2023

Social engineering atau Rekayasa sosial adalah serangan akses yang mencoba memanipulasi individu untuk melakukan tindakan atau membocorkan informasi rahasia. Insinyur sosial sering mengandalkan kesediaan orang untuk membantu tetapi juga memangsa kelemahan orang. Misalnya, penyerang dapat menghubungi karyawan yang berwenang dengan masalah mendesak yang memerlukan akses jaringan segera. Penyerang dapat menarik pengalihan karyawan, meminta otoritas menggunakan teknik menjatuhkan nama, atau menarik keserakahan karyawan.

Ini adalah beberapa jenis serangan rekayasa sosial:

a. Pretexting

   Ini adalah saat penyerang memanggil seseorang dan berbohong kepada mereka dalam upaya untuk mendapatkan akses ke data. Contohnya melibatkan penyerang yang berpura-pura membutuhkan data pribadi atau keuangan untuk mengonfirmasi identitas penerima.

b. Tailgating

   Ini adalah saat penyerang dengan cepat mengikuti orang yang berwenang ke lokasi yang aman.

c. Something for Something (Quid pro quo)

   Ini adalah saat penyerang meminta informasi pribadi dari suatu pihak dengan imbalan sesuatu, seperti hadiah gratis.

2. Wi-Fi Password Cracking

Wi-Fi password cracking adalah proses menemukan kata sandi yang digunakan untuk melindungi jaringan nirkabel. Berikut adalah beberapa teknik yang digunakan dalam cracking password:

a. Social engineering

Penyerang memanipulasi orang yang mengetahui kata sandi untuk memberikannya.

b. Brute-force attacks

Penyerang mencoba beberapa kemungkinan kata sandi dalam upaya untuk menebak kata sandi. Jika kata sandi adalah angka 4 digit, misalnya, penyerang harus mencoba setiap dari 10.000 kombinasi. Serangan brute force biasanya melibatkan file daftar kata. Ini adalah file teks yang berisi daftar kata yang diambil dari kamus. Sebuah program kemudian mencoba setiap kata dan kombinasi umum. Karena serangan brute force membutuhkan waktu, kata sandi yang rumit membutuhkan waktu lebih lama untuk ditebak. Beberapa alat brute force password termasuk Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, dan Medusa.

c. Network sniffin

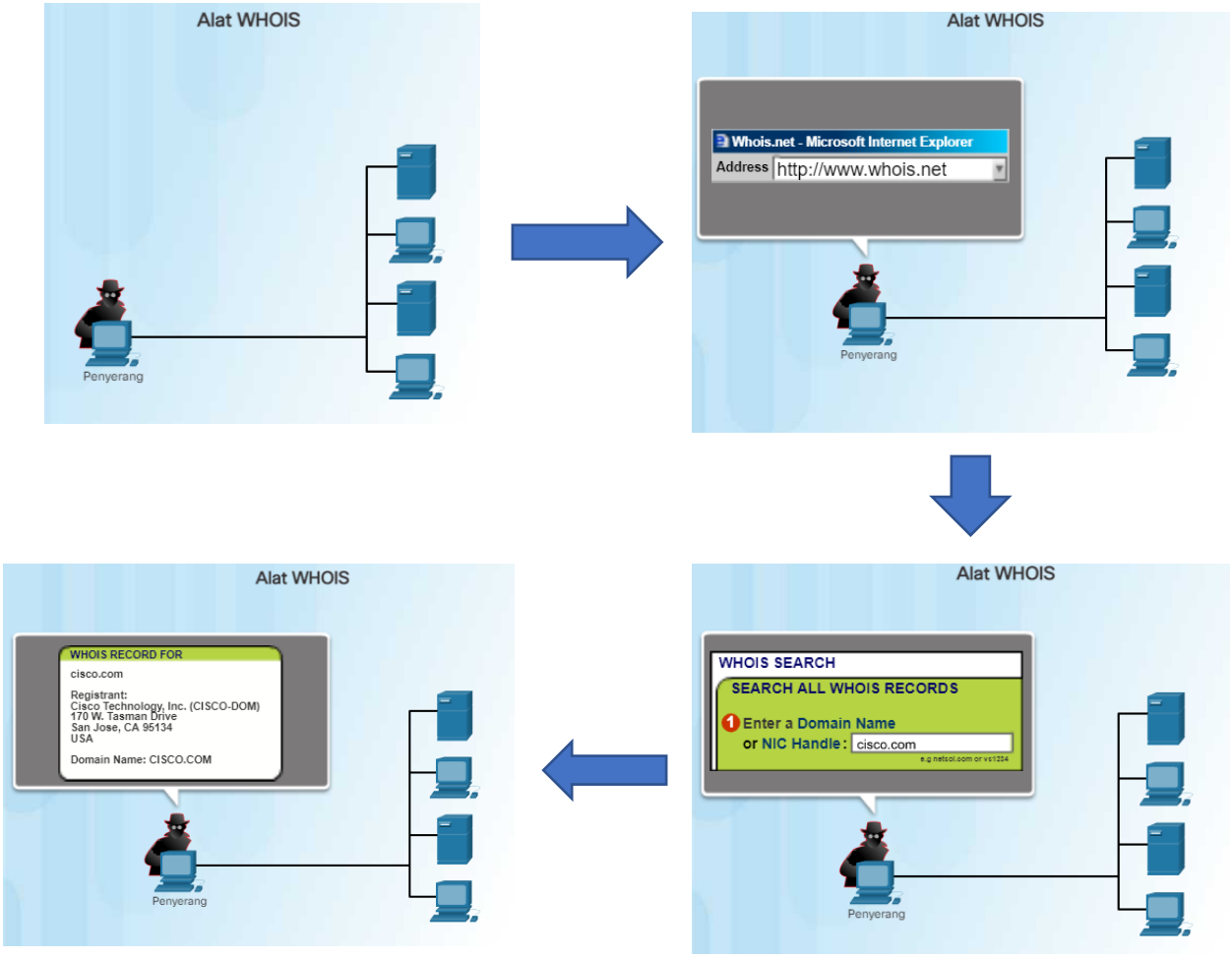
Dengan mendengarkan dan menangkap paket yang dikirim pada jaringan, penyerang mungkin dapat menemukan kata sandi jika kata sandi dikirim tidak terenkripsi (dalam teks biasa). Jika kata sandi dienkripsi, penyerang mungkin masih dapat mengungkapkannya dengan menggunakan alat peretas kata sandi.

3. Phishing

Phishing adalah saat pihak jahat mengirim email palsu yang disamarkan sebagai dari sumber yang sah dan tepercaya. Maksud pesan adalah untuk mengelabui penerima agar memasang malware di perangkat mereka, atau berbagi informasi pribadi atau keuangan. Contoh phishing adalah email yang dipalsukan agar terlihat seperti dikirim oleh toko ritel yang meminta pengguna mengklik tautan untuk mengklaim hadiah. Tautan tersebut mungkin mengarah ke situs palsu yang meminta informasi pribadi, atau mungkin memasang virus.

Spear phishing adalah serangan phishing yang sangat bertarget. Sementara phishing dan spear phishing sama-sama menggunakan email untuk menjangkau korban, email spear phishing disesuaikan untuk orang tertentu. Penyerang meneliti minat target sebelum mengirim email. Misalnya, penyerang mengetahui bahwa target tertarik pada mobil, dan telah mencari untuk membeli model mobil tertentu. Penyerang bergabung dengan forum diskusi mobil yang sama di mana target adalah anggota, memalsukan penawaran penjualan mobil dan mengirim email ke target. Email tersebut berisi link untuk gambar mobil. Ketika target mengklik tautan, malware dipasang di komputer target.

4. Vulnerability Exploitation



Copyright © September 2023

Gambar 1. Model Penyerangan Dengan mencari informasi domain dengan WHOIS

Exploiting vulnerabilities adalah metode umum lain dari penyusupan. Penyerang akan memindai komputer untuk mendapatkan informasi tentang mereka. Di bawah ini adalah metode umum untuk mengeksploitasi kerentanan:

a. Langkah 1

   Mengumpulkan informasi tentang sistem target. Ini dapat dilakukan dengan berbagai cara seperti pemindai port atau rekayasa sosial. Tujuannya adalah untuk belajar sebanyak mungkin tentang komputer

b. Langkah 2

   Salah satu informasi relevan yang dipelajari pada langkah 1 mungkin adalah sistem operasi, versinya, dan daftar layanan yang berjalan di dalamnya.

c. Langkah 3

   Ketika sistem operasi dan versi target diketahui, penyerang mencari kerentanan yang diketahui khusus untuk versi OS tersebut atau layanan OS lainnya.

d. Langkah 4

   Ketika kerentanan ditemukan, penyerang mencari eksploit yang ditulis sebelumnya untuk digunakan. Jika tidak ada eksploit yang ditulis, penyerang dapat mempertimbangkan untuk menulis eksploit.

Copyright © September 2023

Gambar 1 menggambarkan penyerang menggunakan whois , database Internet publik yang berisi informasi tentang nama domain dan pendaftarnya. Gambar 2 menggambarkan penyerang menggunakan alat nmap , pemindai port yang populer. Dengan pemindai port, penyerang dapat menyelidiki port komputer target untuk mempelajari tentang layanan mana yang berjalan di komputer itu.

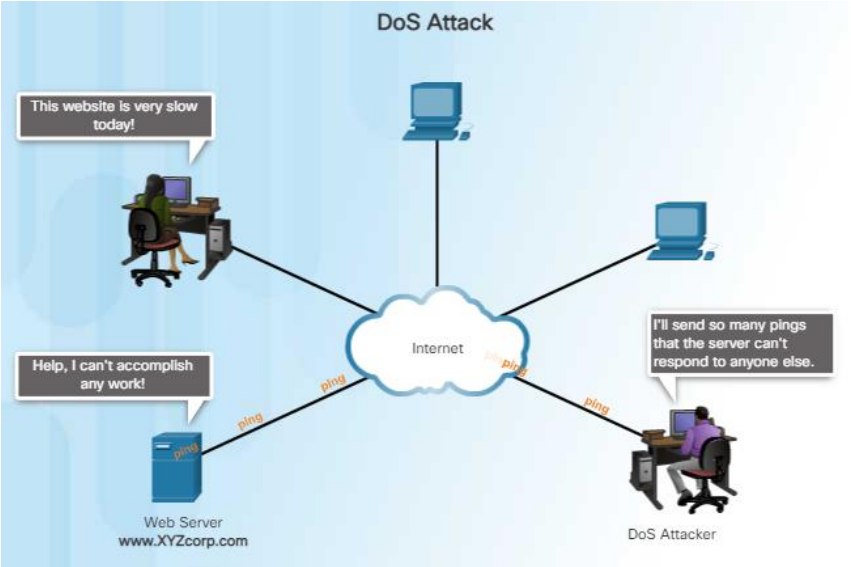
e. Advanced Persistent Threats

Salah satu cara di mana infiltrasi dicapai adalah melalui Advanced Persistent Threats (APT). Mereka terdiri dari operasi multi-fase, jangka panjang, tersembunyi dan lanjutan terhadap target tertentu. Karena kompleksitas dan tingkat keterampilan yang dibutuhkan, APT biasanya didanai dengan baik. APT menargetkan organisasi atau negara untuk alasan bisnis atau politik.

Biasanya terkait dengan spionase berbasis jaringan, tujuan APT adalah untuk menyebarkan malware yang disesuaikan pada satu atau beberapa sistem target dan tetap tidak terdeteksi. Dengan beberapa fase operasi dan beberapa jenis malware khusus yang memengaruhi perangkat berbeda dan menjalankan fungsi tertentu, penyerang individu sering kali tidak memiliki keahlian, sumber daya, atau ketekunan untuk menjalankan APT.

1.1.5. DoS, DDoS dan SEO

1. Dos



Gambar 2. DoS attack

Serangan Denial-of-Service (DoS) adalah jenis serangan jaringan. Serangan DoS menghasilkan semacam gangguan layanan jaringan kepada pengguna, perangkat, atau aplikasi. Ada dua jenis utama serangan DoS:

a. Overwhelming Quantity of Traffic

   Ini adalah saat jaringan, host, atau aplikasi dikirimi sejumlah besar data dengan kecepatan yang tidak dapat ditanganinya. Hal ini menyebabkan pelambatan dalam transmisi atau respons, atau kerusakan perangkat atau layanan.

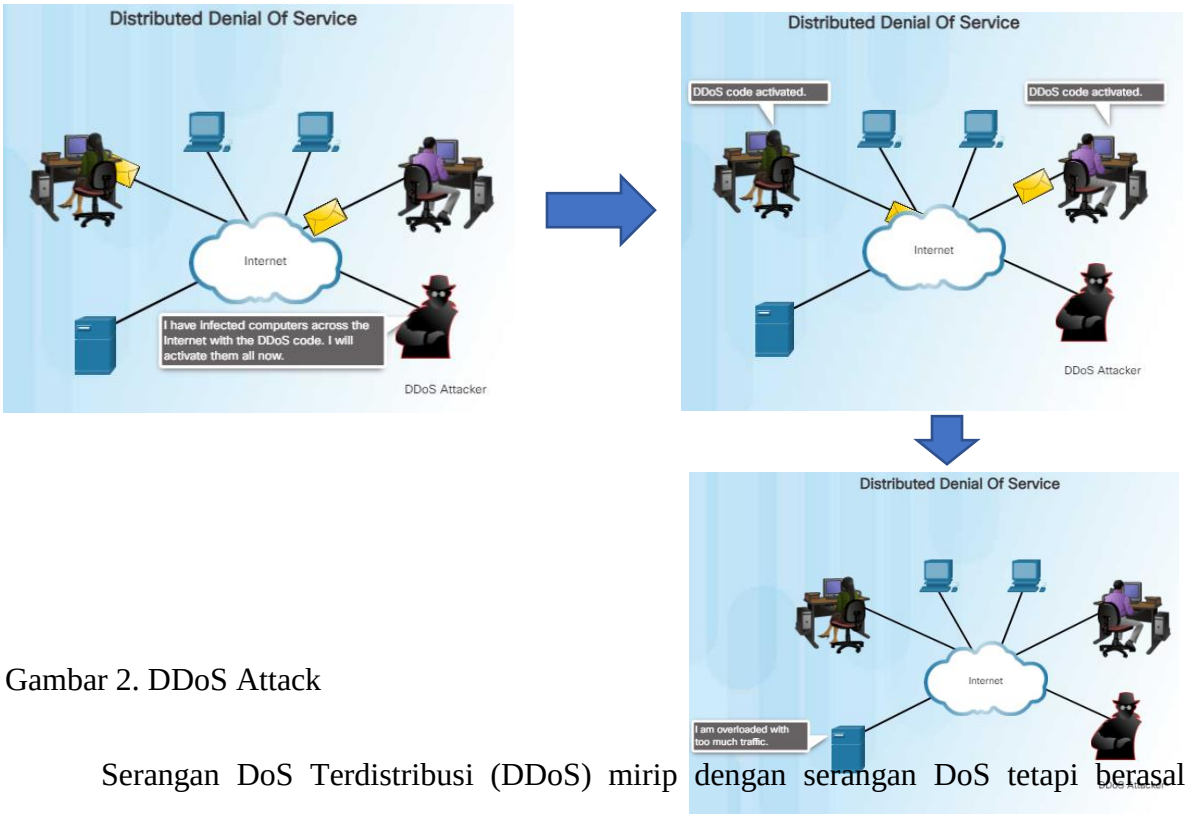
b. Maliciously Formatted Packets

   Ini adalah saat paket berformat jahat dikirim ke host atau aplikasi dan penerima tidak dapat menanganinya. Misalnya, penyerang meneruskan paket yang berisi kesalahan yang tidak dapat diidentifikasi oleh aplikasi, atau meneruskan paket yang diformat dengan tidak benar. Hal ini menyebabkan perangkat penerima berjalan sangat lambat atau crash.

Copyright © September 2023

Serangan DoS dianggap sebagai risiko besar karena dapat dengan mudah mengganggu komunikasi dan menyebabkan kerugian waktu dan uang yang signifikan. Serangan ini relatif mudah dilakukan, bahkan oleh penyerang yang tidak terampil.

2. DDoS



Gambar 2. DDoS Attack

Serangan DoS Terdistribusi (DDoS) mirip dengan serangan DoS tetapi berasal dari banyak sumber yang terkoordinasi. Sebagai contoh, serangan DDoS dapat berlangsung sebagai berikut:

Penyerang membangun jaringan host yang terinfeksi, yang disebut botnet. Host yang terinfeksi disebut zombie. Zombi dikendalikan oleh sistem pawang.

Komputer zombie terus-menerus memindai dan menginfeksi lebih banyak host, menciptakan lebih banyak zombie. Saat siap, peretas menginstruksikan sistem penangan untuk membuat botnet zombie melakukan serangan DDoS.

Copyright © September 2023

3. SEO Poisoning

Mesin pencari seperti Google bekerja dengan memberi peringkat halaman dan menyajikan hasil yang relevan berdasarkan permintaan pencarian pengguna. Bergantung pada relevansi konten situs web, konten itu mungkin muncul lebih tinggi atau lebih rendah dalam daftar hasil pencarian. SEO, kependekan dari Search Engine Optimization, adalah seperangkat teknik yang digunakan untuk meningkatkan peringkat situs web oleh mesin pencari. Sementara banyak perusahaan yang sah mengkhususkan diri dalam mengoptimalkan situs web untuk memposisikan mereka dengan lebih baik, pengguna jahat dapat menggunakan SEO untuk membuat situs web jahat muncul lebih tinggi dalam hasil pencarian. Teknik ini disebut keracunan SEO.

Tujuan paling umum dari SEO Poisoning adalah untuk meningkatkan lalu lintas ke situs jahat yang mungkin menghosting malware atau melakukan rekayasa sosial. Untuk memaksa situs jahat berperingkat lebih tinggi dalam hasil pencarian, penyerang memanfaatkan istilah pencarian populer.

1.2. The Cybersecurity Landscape

1.2.1. Blended Attack

1. Pengertian Blended attacks

Blended attacks atau Serangan campuran adalah serangan yang menggunakan beberapa teknik untuk mengkompromikan target. Dengan menggunakan beberapa teknik serangan yang berbeda sekaligus, penyerang memiliki malware yang merupakan hibrida dari worm, Trojan horse, spyware, keyloggers, spam dan skema phishing. Tren serangan campuran ini mengungkapkan

Jenis serangan campuran yang paling umum menggunakan pesan email spam, pesan instan, atau situs web yang sah untuk mendistribusikan tautan tempat malware atau spyware secara diam-diam diunduh ke komputer. Serangan campuran umum lainnya menggunakan DDoS yang dikombinasikan dengan email phishing. Pertama, DDoS digunakan untuk menghapus situs bank populer dan mengirim email ke pelanggan bank, meminta maaf atas ketidaknyamanan ini. Email tersebut juga mengarahkan pengguna ke situs darurat palsu di mana informasi login mereka yang sebenarnya dapat dicuri. malware yang lebih kompleks dan menempatkan data pengguna dalam risiko besar.

Banyak dari worm komputer yang paling merusak seperti Nimbda, CodeRed, BugBear, Klez dan Slammer lebih baik dikategorikan sebagai serangan campuran, seperti yang ditunjukkan di bawah ini:

- Beberapa varian Nimbda menggunakan lampiran email; unduhan file dari server web yang disusupi; dan berbagi file Microsoft (misalnya, pembagian anonim) sebagai metode propagasi.
- Varian Nimbda lainnya mampu memodifikasi akun tamu sistem untuk memberikan penyerang atau kode berbahaya dengan hak administratif.

Cacing Conficker dan ZeuS/LICAT baru-baru ini juga merupakan serangan campuran. Conficker menggunakan semua metode distribusi tradisional.

1.2.2. Impact Reduction

1. Pengertian Impact Reduction

Sementara sebagian besar perusahaan sukses saat ini menyadari masalah keamanan umum dan berupaya keras untuk mencegahnya, tidak ada serangkaian praktik keamanan yang 100%

efisien. Karena pelanggaran kemungkinan besar terjadi jika hadiahnya besar, perusahaan dan organisasi juga harus siap menanggung kerugiannya.

Penting untuk dipahami bahwa Impact Reduction tidak hanya terkait dengan aspek teknis, data yang dicuri, database yang rusak, atau kerusakan kekayaan intelektual, kerusakan juga meluas ke reputasi perusahaan. Menanggapi pelanggaran data adalah proses yang sangat dinamis.

Di bawah ini adalah beberapa tindakan penting yang harus diambil perusahaan ketika pelanggaran keamanan diidentifikasi, menurut banyak pakar keamanan:

- Komunikasikan masalahnya. Karyawan internal harus diberitahu tentang masalah ini dan dipanggil untuk bertindak. Secara eksternal, klien harus diinformasikan melalui komunikasi langsung dan pengumuman resmi. Komunikasi menciptakan transparansi, yang sangat penting dalam situasi seperti ini.
- Bersikaplah tulus dan bertanggung jawab jika perusahaan bersalah.
- Berikan detail. Jelaskan mengapa situasi itu terjadi dan apa yang dikompromikan. Perusahaan juga diharapkan menanggung biaya layanan perlindungan pencurian identitas bagi pelanggan yang terkena dampak.
- Pahami apa yang menyebabkan dan memfasilitasi pelanggaran tersebut. Jika perlu, pekerjakan ahli forensik untuk meneliti dan mempelajari detailnya.
- Terapkan apa yang dipelajari dari penyelidikan forensik untuk memastikan pelanggaran serupa tidak terjadi di masa depan.
- Pastikan semua sistem bersih, tidak ada pintu belakang yang dipasang, dan tidak ada lagi yang dikompromikan. Penyerang akan sering mencoba untuk meninggalkan pintu belakang untuk memfasilitasi pelanggaran di masa depan. Pastikan ini tidak terjadi.

Copyright © September 2023

- Mendidik karyawan, mitra, dan pelanggan tentang cara mencegah pelanggaran di masa mendatang.