Nama : Bland Deny Ginting

Nim :71160132

RIngkasan Materi Tekwan

**NETWORK SECURITY CONCEPT**

Akses tidak sah ke data, komputer, dan sistem jaringan adalah kejahatan dan sering disertai dengan konsekuensi yang parah, terlepas dari motivasi pelaku. Merupakan tanggung kita selaku mahasiswa, sebagai pengguna materi ini, untuk mengetahui dan mematuhi hukum penggunaan komputer. Agar kita tidak salah dalam penggunaannya.

Penjahat cyber sekarang memiliki keahlian dan alat yang diperlukan untuk menjatuhkan infrastruktur dan sistem kritis. Alat dan teknik mereka terus berkembang.

Penjahat dunia maya membawa malware ke tingkat kecanggihan dan dampak yang belum pernah terjadi sebelumnya. Mereka menjadi lebih mahir menggunakan teknik sembunyi-sembunyi dan penggelapan untuk menyembunyikan aktivitas mereka. Terakhir, penjahat cyber mengeksploitasi celah keamanan yang tidak dijaga.

Pelanggaran keamanan jaringan dapat mengganggu e-commerce, menyebabkan hilangnya data bisnis, mengancam privasi orang, dan membahayakan integritas informasi. Pelanggaran ini dapat mengakibatkan hilangnya pendapatan bagi perusahaan, pencurian kekayaan intelektual, tuntutan hukum, dan bahkan dapat mengancam keselamatan publik.

Mempertahankan jaringan yang aman memastikan keamanan pengguna jaringan dan melindungi kepentingan komersial. Organisasi membutuhkan individu yang dapat mengenali kecepatan dan skala di mana musuh mengumpulkan dan menyempurnakan persenjataan cyber mereka.

Ada banyak macam hal serangan yang dapat dilakukan siapa saja

Vektor serangan adalah jalur di mana aktor ancaman dapat memperoleh akses ke server, host, atau jaringan. Vektor serangan berasal dari dalam atau di luar jaringan perusahaan,

Misalnya, aktor ancaman dapat menargetkan jaringan melalui internet, untuk mengganggu operasi jaringan dan membuat serangan penolakan layanan (DoS).

jaringan dengan server dan beberapa host di belakang firewall; host di jaringan telah dikompromikan; panah menunjukkan itu bisa jadi ancaman eksternal dari Internet melalui firewall atau ancaman internal dari host lain di jaringan

* Ancaman Eksternal dan Internal

InternetExternal ThreatCompromised Host Internal Threat

Catatan: Serangan DoS terjadi ketika perangkat jaringan atau aplikasi tidak mampu dan tidak lagi mampu mendukung permintaan dari pengguna yang sah.

Pengguna internal, seperti karyawan, dapat secara tidak sengaja atau sengaja:

Mencuri dan menyalin data rahasia ke media yang dapat dilepas, email, perangkat lunak pengiriman pesan, dan media lainnya.

1. Mengompromikan server internal atau perangkat infrastruktur jaringan.
2. Putuskan koneksi jaringan yang kritis dan menyebabkan pemadaman jaringan.
3. Sambungkan drive USB yang terinfeksi ke sistem komputer perusahaan.
4. Ancaman internal berpotensi menyebabkan kerusakan lebih besar daripada ancaman eksternal karena pengguna internal memiliki akses langsung ke gedung dan perangkat infrastrukturnya. Karyawan juga dapat memiliki pengetahuan tentang jaringan perusahaan, sumber dayanya, dan data rahasianya.

Profesional keamanan jaringan harus menerapkan alat dan menerapkan teknik untuk mengurangi ancaman eksternal dan internal.

Dalam topik ini, Anda akan mempelajari lebih detail tentang jenis aktor ancaman tertentu.

Hacker adalah istilah umum yang digunakan untuk menggambarkan aktor ancaman.

Ada beberapa masam hacker yaitu:

* White Hat Hacker

ini adalah hacker etis yang menggunakan keterampilan pemrograman mereka untuk tujuan yang baik, etis, dan legal. Peretas white hat dapat melakukan tes penetrasi jaringan dalam upaya untuk mengkompromikan jaringan dan sistem dengan menggunakan pengetahuan mereka tentang sistem keamanan komputer untuk menemukan kerentanan jaringan. Kerentanan keamanan dilaporkan kepada pengembang untuk diperbaiki sebelum kerentanan dapat dieksploitasi.

* Gray Hat Hacker

Ini adalah individu yang melakukan kejahatan dan melakukan hal-hal yang dianggap tidak etis, tetapi tidak untuk keuntungan pribadi atau menyebabkan kerusakan. Peretas topi abu-abu dapat mengungkapkan kerentanan terhadap organisasi yang terpengaruh setelah kompromi jaringan mereka.

* BLACK Hat Hacker

Ini adalah penjahat tidak etis yang membahayakan keamanan komputer dan jaringan untuk keuntungan pribadi, atau untuk alasan jahat, seperti menyerang jaringan.

Catatan: Dalam kursus ini, kami tidak akan menggunakan istilah peretas di luar modul ini. Kami akan menggunakan istilah aktor ancaman. Aktor ancaman jangka termasuk peretas. Tetapi aktor ancaman juga termasuk alat, orang, kelompok, atau negara bangsa apa pun yang secara sengaja atau tidak sengaja menjadi sumber serangan.

Peretasan etis melibatkan berbagai jenis alat yang digunakan untuk menguji jaringan dan mengamankan datanya. Untuk memvalidasi keamanan jaringan dan sistemnya, banyak alat pengujian penetrasi jaringan telah dikembangkan. Sangat disayangkan bahwa banyak dari alat ini dapat digunakan oleh BLACK Hat Hacker untuk eksploitasi.

BLACK Hat Hacker juga telah menciptakan banyak alat peretasan. Alat-alat ini dibuat secara eksplisit untuk alasan jahat.BLACK Hat Hacker juga harus tahu cara menggunakan alat ini saat melakukan tes penetrasi jaringan.

Perhatikan bagaimana beberapa alat digunakan oleh White Hat dan BLACK Hat. Ingatlah bahwa daftar ini tidak lengkap karena alat baru selalu dikembangkan.

Ada banyak jenis alat yang digunakan untuk melakukan suatu peretasan

1. **Peretas Kata Sandi**

Alat peretas kata sandi sering disebut sebagai alat pemulihan kata sandi dan dapat digunakan untuk memecahkan atau memulihkan kata sandi. Ini dapat dilakukan dengan menghapus kata sandi asli, setelah melewati enkripsi data, atau dengan penemuan kata sandi secara langsung. Pemecah kata sandi berulang kali membuat tebakan untuk memecahkan kata sandi. Contoh alat peretas kata sandi termasuk John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, dan Medusa.

1. **Alat Peretasan Nirkabel**

Alat peretasan nirkabel digunakan untuk secara sengaja meretas ke dalam jaringan nirkabel untuk mendeteksi kerentanan keamanan. Contoh alat peretasan nirkabel termasuk Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, dan NetStumbler.

1. **Pemindaian Jaringan dan Alat Peretasan**

Alat pemindaian jaringan digunakan untuk menyelidiki perangkat jaringan, server, dan host untuk membuka port TCP atau UDP. Contoh alat pemindaian termasuk Nmap, SuperScan, Pemindai IP Marah, dan NetScanTools.

1. **Paket Alat Kerajinan**

Alat-alat ini digunakan untuk menyelidiki dan menguji ketahanan firewall menggunakan paket-paket palsu yang dibuat khusus. Contohnya termasuk Hping, Scapy, Socat, Yersinia, Netcat, Nping, dan Nemesis.

1. **Packet Sniffers**

Alat-alat ini digunakan untuk menangkap dan menganalisis paket-paket dalam LAN Ethernet atau WLAN tradisional. Alat termasuk Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, dan SSLstrip.

Setelah kita membahas alat peretasan selanjutnya adalah jenis malware:

Jenis malware komputer yang pertama dan paling umum adalah virus.

Virus memerlukan tindakan manusia untuk menyebarkan dan menginfeksi komputer lain. Misalnya, virus dapat menginfeksi komputer ketika korban membuka lampiran email, membuka file pada drive USB, atau mengunduh file.

Virus bersembunyi dengan melampirkan dirinya ke kode komputer, perangkat lunak, atau dokumen di komputer. Ketika dibuka, virus mengeksekusi dan menginfeksi komputer.

Virus dapat:Mengubah, merusak, menghapus file, atau menghapus seluruh drive.

Menyebabkan masalah booting komputer, dan aplikasi rusak.Menangkap dan mengirim informasi sensitif ke aktor ancaman. Akses dan gunakan akun email untuk menyebar.

bahkan virus juga digunakan untuk menyerang antar perusahaan yang sedang bersaing .

Jenis-jenis Deskripsi Virus

* Virus sektor boot Virus menyerang sektor boot, tabel partisi file, atau sistem file.
* Virus firmware Virus menyerang firmware perangkat
* Virus makro Virus menggunakan MS Office atau fitur makro aplikasi lain dengan jahat.
* Virus program Virus memasukkan dirinya dalam program yang dapat dieksekusi lainnya.
* Virus skrip Virus menyerang interpreter OS yang digunakan untuk menjalankan skrip.

Trojan horse adalah program yang terlihat berguna tetapi juga membawa kode jahat. Trojan horse sering diberikan dengan program online gratis seperti game komputer. Pengguna yang tidak curiga mengunduh dan menginstal game, bersama dengan Trojan horse.

Dan banyak lagi jenis Malware lainnya

1. **Adware**

Adware biasanya didistribusikan dengan mengunduh perangkat lunak online.

Adware dapat menampilkan iklan yang tidak diminta menggunakan jendela browser web pop-up, toolbar baru, atau secara tak terduga mengarahkan ulang halaman web ke situs web yang berbeda.

Jendela pop-up mungkin sulit dikendalikan karena jendela baru dapat muncul lebih cepat daripada yang bisa ditutup oleh pengguna.

1. **Ransomware**

Ransomware biasanya menolak akses pengguna ke file mereka dengan mengenkripsi file dan kemudian menampilkan pesan yang menuntut tebusan untuk kunci dekripsi.

Pengguna tanpa cadangan terkini harus membayar tebusan untuk mendekripsi file mereka.

Pembayaran biasanya dilakukan menggunakan transfer kawat atau mata uang kripto seperti Bitcoin.

1. **Rootkit**

Rootkit digunakan oleh aktor ancaman untuk mendapatkan akses tingkat akun administrator ke komputer.

Mereka sangat sulit dideteksi karena mereka dapat mengubah firewall, perlindungan antivirus, file sistem, dan bahkan perintah OS untuk menyembunyikan keberadaan mereka.

Dan banyak lagi jenis” malware lainnya.

Kita selaku mahasiswa terlebih yang berkecimpung di dunia IT

harus bisa menjaga Kerahasiaan, Integritas

Keamanan jaringan terdiri dari melindungi informasi dan sistem informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan.

Sebagian besar organisasi mengikuti triad keamanan informasi CIA:

* Kerahasiaan

Hanya individu, entitas, atau proses yang sah yang dapat mengakses informasi sensitif. Mungkin diperlukan penggunaan algoritma enkripsi kriptografi seperti AES untuk mengenkripsi dan mendekripsi data.

* Integritas

Mengacu pada melindungi data dari perubahan yang tidak sah. Ini membutuhkan penggunaan algoritma hashing kriptografi seperti SHA.

Ketersediaan - Pengguna yang berwenang harus memiliki akses tanpa gangguan ke sumber daya dan data penting.

Beberapa perangkat dan layanan keamanan diterapkan untuk melindungi pengguna dan aset organisasi terhadap ancaman TCP / IP.

**VPN**

Router digunakan untuk menyediakan layanan VPN aman dengan situs perusahaan dan dukungan akses jarak jauh untuk pengguna jarak jauh menggunakan terowongan terenkripsi yang aman.

**ASA Firewall**

Perangkat khusus ini menyediakan layanan firewall stateful. Ini memastikan bahwa lalu lintas internal dapat keluar dan kembali, tetapi lalu lintas eksternal tidak dapat memulai koneksi ke host di dalam.

**IPS**

Intrusion Prevention System (IPS) memonitor lalu lintas masuk dan keluar mencari malware, tanda tangan serangan jaringan, dan banyak lagi. Jika ia mengenali ancaman, ia dapat segera menghentikannya.

Semua perangkat jaringan termasuk router dan switch dikeraskan, yang berarti bahwa mereka telah diamankan untuk mencegah aktor ancaman dari mendapatkan akses dan merusak perangkat.

Selanjutnya, Anda harus mengamankan data saat melintasi berbagai tautan. Ini mungkin termasuk lalu lintas internal, tetapi lebih penting untuk melindungi data yang melakukan perjalanan di luar organisasi ke situs cabang, situs telekomunikasi, dan situs mitra.

**Firewall**

Firewall adalah sistem, atau sekelompok sistem, yang memberlakukan kebijakan kontrol akses antar jaringan.

* Operasi Firewall Menolak semua lalu lintas masuk dengan alamat jaringan yang cocok dengan alamat IP terdaftar internal.
* Menolak semua lalu lintas masuk ke server dari alamat eksternal. Menolak semua masuk ICMP permintaan gema lalu lintas.
* Menolak semua permintaan MS Active Directory masuk. Memungkinkan lalu lintas dari setiap alamat eksternal ke server web .
* Mengizinkan lalu lintas ke server FTP.
* Memungkinkan lalu lintas ke server SMTP.
* Memungkinkan lalu lintas ke server IMAP internal.
* Menolak semua lalu lintas masuk ke permintaan server MS SQL.
* Menolak semua MS Domain Broadcast Lokal.