**Nama : bland deny ginting**

**Nim : 71160132**

**TUGAS**

1. **jelaskan serangan serangan keamanan dari sisi mana saja?**

Jawab:

Ancaman Eksternal dan Internal

Pengguna internal, seperti karyawan didalam sebuiah perusahaan, dapat secara tidak sengaja atau sengaja Mencuri dan menyalin data rahasia ke media yang dapat dilepas, email, perangkat lunak pengiriman pesan, dan media lainnya.

* Mengompromikan server internal atau perangkat infrastruktur jaringan.
* Putuskan koneksi jaringan yang kritis dan menyebabkan pemadaman jaringan.
* Sambungkan drive USB yang terinfeksi ke sistem komputer perusahaan.

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.

1. **Ada beberapa jenis istilah untuk hacker dan jenjangnya, coba anda diskripsikan?**

Jawab:

Ada beberapa macam hacker yaitu:

* White Hat Hacker

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.

* Black Hat Hacker

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

Peretasan dimulai pada 1960-an dengan telepon panik, atau phreaking, yang mengacu pada penggunaan frekuensi audio untuk memanipulasi sistem telepon.

Pada pertengahan 1980-an, modem dial-up komputer digunakan untuk menghubungkan komputer ke jaringan. Peretas menulis program "panggilan perang" yang memutar setiap nomor telepon di area tertentu untuk mencari komputer. Ketika komputer ditemukan, program peretas kata sandi digunakan untuk mendapatkan akses.

1. **Sebutkan penetration  testing tool beserta diskripsinya dan tipe tipe serangan beserta diskripsinya pula?**

Jawab:

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.

Dan masih banyak lagi karna banyak alat-alat baru yang bermunculan.

**Berikut ini adalah beberapa typr jenis serangan:**

1. Serangan dengan cara menguping

adalah saat aktor ancaman menangkap dan "mendengarkan" lalu lintas jaringan. Serangan ini juga disebut sebagai sniffing atau snooping.

2. Serangan Modifikasi DataJika pelaku ancaman telah menangkap lalu lintas perusahaan, mereka dapat mengubah data dalam paket tanpa sepengetahuan pengirim atau penerima.

3. Serangan Spoofing Alamat IP Aktor Athreat membangun paket IP yang tampaknya berasal dari alamat yang valid di dalam intranet perusahaan.

4. Serangan Berbasis Kata Sandi Jika aktor ancaman menemukan akun pengguna yang valid, aktor ancaman memiliki hak yang sama dengan pengguna sebenarnya. Pelaku ancaman dapat menggunakan akun yang valid untuk mendapatkan daftar pengguna lain, informasi jaringan, mengubah server dan konfigurasi jaringan, dan memodifikasi, mengalihkan rute, atau menghapus data.

5. Serangan Denial of Service Serangan DoS mencegah penggunaan normal komputer atau jaringan oleh pengguna yang valid. Serangan DoS dapat membanjiri komputer atau seluruh jaringan dengan lalu lintas hingga shutdown terjadi karena kelebihan beban. Serangan DoS juga dapat memblokir lalu lintas, yang mengakibatkan hilangnya akses ke sumber daya jaringan oleh pengguna yang berwenang.

6. Serangan Man-in-the-Middle Serangan ini terjadi ketika aktor ancaman telah memposisikan diri antara sumber dan tujuan. Mereka sekarang dapat secara aktif memantau, menangkap, dan mengendalikan komunikasi secara transparan.

7. Serangan Kunci yang Dikompromikan Jika aktor ancaman memperoleh kunci rahasia, kunci itu disebut sebagai kunci yang dikompromikan.

1. **Jelaskan mengenai malware dan apa saja yang ada didalamnya, termasuk acaman apa yang bisa terjadi?**

Jawab:

**Malware** adalah adalah suatu program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer. Malware dapat menginfeksi banyak komputer dengan masuk melalui email, download internet, atau program yang terinfeksi.

**Virus** adalah perangkat lunak berbahaya yang menjalankan fungsi tertentu, tidak diinginkan, dan seringkali berbahaya, di komputer.

**Worm** menjalankan kode arbitrer dan menginstal salinannya sendiri di memori komputer yang terinfeksi. Tujuan utama worm adalah untuk secara otomatis mereplikasi dirinya sendiri dan menyebar ke seluruh jaringan dari satu sistem ke sistem lainnya.

**Trojan horse** adalah jenis malware yang tidak dapat direplikasi sendiri. Ini sering berisi kode berbahaya yang dirancang agar terlihat seperti sesuatu yang lain, seperti aplikasi atau file yang sah. Ketika aplikasi atau file yang terinfeksi diunduh dan dibuka, kuda Trojan dapat menyerang perangkat akhir dari dalam.

**Ada beberapa ancaman yang dapat disebabkan oleh sebuah virus.**

1. Mengubah, merusak, menghapus file, atau menghapus seluruh drive.
2. Menyebabkan masalah booting komputer, dan aplikasi rusak.
3. Menangkap dan mengirim informasi sensitif ke threat actor.
4. Akses dan gunakan akun email untuk menyebar.
5. Berbaring tidak aktif sampai dipanggil oleh threat actor.
6. Serangan kata sandi
7. Serangan Spoofing
8. **Jelaskan apa itu Reconnaissance attack dan Social Engineering Attacks serta berikan contohnya?**

Jawab:

1. **Reconnaissance attack** adalah tahap mengumpulkan data, dimana hacker akan mengumpulkan data tentang target sebanyak-banyaknya. Baik nama anggota keluarga, tanggal lahir, tempat kerja beserta informasi didalamnya. Dan itu hanya sebagian kecil kegunaan dari tahapan Reconnaissance.
2. **Social Engineering Attacks** merupakan kegiatan untuk mendapatkan informasi/hak akses dengan cara memanipulasi psikologis dengan berinteraksi langsung dengan pemilik informasi (orang nya) dan  menipu user secara halus tanpa user sadari.

Interaksi bisa dilakukan melalui berbagai jalur komunikasi seperti Yang bahkan paling marak sekarang adalah penipuan melalu media sosial, telfon, sms, email, DM,

FB, WA, dan lain-lain. atau bahkan bertemu langsung dengan orang nya/target/korban.

Contohnya : Phishing Seorang aktor ancaman mengirim sms palsu yang mengatas namakan sebuah perusahaan atau lainnya yang berisi sms hadiah yang disamarkan sebagai sumber yang sah dan tepercaya untuk menipu penerima agar penerima sms percaya dengan sms tersebut dan mau diarahkan untuk mentransfer uang ke pelaku utama.

1. **Jelaskan kerentanan dan ancaman ancaman yang ada pada Internet Protocol ( IP )?**

Jawab:

* ICMP attacks : threat actor menggunakan ICMP untuk pengintaian dan pemindaian serangan. Mereka dapat meluncurkan serangan pengumpulan-informasi untuk memetakan topologi jaringan, menemukan host mana yang aktif (dapat dijangkau), mengidentifikasi sistem operasi host (sidik jari OS), dan menentukan keadaan firewall.
* DHCP Spoofing Attack : Serangan spoofing DHCP terjadi ketika server DHCP jahat terhubung ke jaringan dan memberikan parameter konfigurasi IP palsu kepada klien yang sah. Server jahat dapat memberikan berbagai informasi yang menyesatkan:
* Wrong Default Gateway - Threat actor menyediakan gateway yang tidak valid, atau alamat IP inangnya untuk membuat serangan MITM. Ini mungkin sepenuhnya tidak terdeteksi karena penyusup memotong aliran data melalui jaringan.
* Wrong DNS Server - Threat actor memberikan alamat server DNS yang salah yang mengarahkan pengguna ke situs web berbahaya.
* Wrong IP Address - Threat actor memberikan alamat IP tidak valid, alamat IP gateway default tidak valid, atau keduanya. Threat actor kemudian menciptakan serangan DoS pada klien DHCP.

1. **Jelaskan kerentanan protocol TCP , UDP , ARP dan DHCP dan berikan contoh bagaimana memanfaatkan kerentanan pada ARP dan DHCP?**

Jawab:

DHCP Attack

Gateway default salah - Aktor ancaman menyediakan gateway yang tidak valid, atau alamat IP inangnya untuk membuat serangan MITM. Ini mungkin sepenuhnya tidak terdeteksi karena penyusup memotong aliran data melalui jaringan.

Server DNS salah - Aktor ancaman memberikan alamat server DNS yang salah yang mengarahkan pengguna ke situs web berbahaya.

Alamat IP salah - Aktor ancaman memberikan alamat IP tidak valid, alamat IP gateway default tidak valid, atau keduanya. Aktor ancaman kemudian menciptakan serangan DoS pada klien DHCP.

1. **Untuk meminimalisir serangan dan penyusup yang tidak berhak atas akses jaringan dan data, cara apa saja  yang bisa dilakan di lingkup jaringan komputer?**

Jawab:

1. 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.
2. 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.
3. 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.
4. ESA / WSA - Alat keamanan email (ESA) menyaring spam dan email yang mencurigakan. Alat keamanan web menyaring situs malware internet yang dikenal dan mencurigakan.
5. AAA Server - Server ini berisi basis data aman tentang siapa yang berwenang untuk mengakses dan mengelola perangkat jaringan. Perangkat jaringan mengautentikasi pengguna administratif menggunakan database ini.
6. **Apa perbedaan enkripsi simetraik dengan enkripsi asimetrik?**

Jawab:

****Enkripsi simetris****

Adalah teknik tua dan terkenal. Kunci rahasia, yang dapat berupa angka, word atau rangkaian huruf acak, diterapkan untuk teks dari pesan untuk mengubah konten dengan cara tertentu. Hal ini mungkin sederhana seperti pergeseran setiap huruf jumlah tempat abjad. Selama pengirim dan Penerima tahu kunci rahasia, mereka dapat mengenkripsi dan mendekripsi semua pesan yang menggunakan kunci ini.

****Enkripsi asimetris****

Adalah masalah dengan kunci rahasia bertukar mereka melalui Internet atau jaringan besar sementara mencegah mereka jatuh ke tangan yang salah. Siapa saja yang mengetahui kunci rahasia dapat mendekripsi pesan. Satu jawaban adalah asimetris enkripsi, di mana ada dua kunci terkait--pasangan utama. Kunci publik yang tersedia secara gratis bagi siapa saja yang dapat mengirim pesan. Kunci kedua, pribadi disimpan rahasia, sehingga hanya pengguna yang tahu.