No.

Date:

Teknik Hacking

Eavesdroping Watering Hole Packet Sniffing

Aktivitas mendengarkan (listening) terhadap konversasi yang dilakukan pihak lain dengan tidak diketahui oleh pihak tersebut. Umumnya dapat terjadi pada media Telepon, Email, Instant Messaging, dan media komunikasi lainnya.

Definisi Eavesdropping

* Jurnal Teknik Informatika Kaputama

Eavesdropping adalah penangkapan komunikasi secara real-time antara dua titik oleh pihak yang tidak berwenang.

* Kesimpulan

Aktivitas menangkap / mendengarkan komunikasi secara real-time antara dua titik oleh pihak yang tidak berwenang, dan tidak diketahui oleh pihak yg bersangkutan.

Jenis Eavesdropping

1. Passive Eavesdropping

Ketika seseorang yang tidak berwenang hanya menangkap dan mendengarkan pesan dalam komunikasi secara diam-diam.

2. Active Eavesdropping

Ketika seseorang yang tidak berwenang tidak hanya menangkap dan mendengarkan pesan, tetapi juga melakukan modifikasi pesan.

Metode Eavesdropping

1. Electromagnetic Easesdropping

Eeavesdropping yang dilakukan melalui saluran elektromagnetik, seperti AP, radio.

2. Acoustic Eavesdropping

Eavesdropping yang dilakukan melalui komunikasi langsung manusia, seperti mengguping.

No.

Date:

Pencegahan Eavesdropping

* Kriptografi

Ilmu dan seni penyandian untuk menjaga keamanan dan kerahasiaan suatu pesan

Kelebihan dan Kekurangan Eavesdropping

* Kelebihan

Penyerang dapat mengetahui isi komunikasi dari dua pihak sehingga dapat melakukan aksi tertentu.

* Kekurangan

Mudah diputuskan / mudah dihentikan ketika pihak yang diserang mengetahui

Wateringhole Attack

Teknik yang hacking dimana hacker akan mengamati suatu situs web yang sering dikunjungi orang atau target, lalu menginfeksi situs web tersebut melalui celah yang ada, kemudian memanfaatkan celah tsb untuk meninjeksi virus. Jadi ketika seseorang mengunjungi situs tersebut, ia akan terkena virus yang ditanam oleh penyerang.

Alur Wateringhole

> Penyerang mengintai di situs web yang sah dan menunggu kesempatan untuk menargetkan korban.

> Penyerang mulai mencari profil target mereka, seringkali yang menjadi target adalah karyawan organisasi / perusahaan besar

> Penyerang menemukan jenis situs apa saja yang sering dikunjungi target.

> Penyerang mencari vulnerability situs, membuat exploit, menginjeksi exploit ke situs, dan memantau target.

> Penyerang seringkali menginfeksi situs web dengan menyuntikkannya dengan HTML atau kode Java Script berbahaya, yang mengarahkan korban ke situs web tertentu yang kemungkinan besar palsu yang merampung malware penyerang.

> Penyerang mengirimkan dan menginstall malware tanpa diketahui oleh target. Biasanya penyerang menggunakan RAT (Remote Access Trojan)

No.

Date:

Kelebihan dan Kekurangan Wateringhole

* Kelebihan

Penyerang dapat leluasa mengakses komputer target dan dapat melakukan apapun di komputer target.

* Kekurangan

Wateringhole memeliki metode rumit dan hacker harus dpt mengetahui alur wateringhole.

Packet Sniffing

Aktivitas penyadapan paket data pada sistem jaringan komputer, yang diantaranya dapat memonitor dan menangkap lalu lintas jaringan yang lewat dengan tujuan untuk mengambil data sensitive secara ilegal, biasanya "data" yang diambil adalah username dan password.

Cara Kerja Packet Snipping

Ketika Anda terhubung ke sistem jaringan komputer, saat Anda melakukan proses transfer data dari client server dan sebaliknya. Karena data yang mengalir pada client dan server yang bersifat bolak-balik, Snipping ini akan menangkap paket" yang dikirimkan secara ilegal menggunakan tools pembantu.

Jenis Snipping

1. Passive Sniffing

Aktivitas penyadapan dengan tidak merubah isi dari paket data yg dikirimkan antar server dan ~~client~~ Client. Biasanya dilakukan pada HUB

2. Active Sniffing

Aktivitas penyadapan dengan cara mengubah isi paket data dalam jaringan. Biasanya dilakukan pada Switch.

Date:

Kelebihan dan Kekurangan Packet Sniffing

* Kelebihan

Penyerang bisa mendapatkan akses login yang dimiliki oleh target dengan mengetahui credentialnya.

* Kekurangan

Penyerang mudah diputuskan aksesnya.