PERTEMUAN 13
EKPLOITASI KEAMANAN

A. TUJUAN PEMBELAJARAN

Pada Pertemuan ini akan dijelaskan mengenai eksploitasi keamanan. Setelah mempelajari materi ini mahasiswa diharapkan mampu untuk:

1. Memahami konsep eksploitasi keamanan
2. Menganalisis fase serangan

B. URAIAN MATERI

1. Memahami Konsep Eksploitasi Keamanan

Eksploitasi keamanan/eksploit adalah sebuah kode yang menyerang keamanan komputer secara spesifik. Eksploit banyak digunakan untuk peretasan baik secara legal ataupun ilegal untuk mencari celah pada komputer yang dituju. Bisa juga dikatakan sebuah perangkat lunak yang menyerang celah keamanan dalam komputer melakukan dengan cara yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yang tidak diinginkan.

Ada beberapa metode untuk mengklasifikasikan eksploitasi. Yang paling umum adalah bagaimana exploit berkomunikasi dengan perangkat lunak yang rentan.

a. Eksploitasi jarak jauh bekerja melalui jaringan dan mengeksploitasi kerentanan keamanan tanpa akses sebelumnya ke sistem yang rentan.
b. Eksploitasi lokal memerlukan akses sebelumnya ke sistem yang rentan dan biasanya meningkatkan hak istimewa orang yang menjalankan eksploitasi melebihi yang diberikan oleh administrator sistem. Eksploitasi terhadap aplikasi klien juga ada, biasanya terdiri dari server yang dimodifikasi yang mengirim eksploit jika diakses dengan aplikasi klien.

Eksploitasi terhadap aplikasi klien mungkin juga memerlukan beberapa interaksi dengan *user* dan dengan demikian dapat digunakan dalam kombinasi dengan metode rekayasa sosial. Klasifikasi lainnya adalah berdasarkan tindakan terhadap sistem yang rentan dalam akses data yang tidak sah, eksekusi kode *arbitrer*, dan penolakan layanan adalah contohnya.

Banyak eksploitasi dirancang untuk menyediakan akses tingkat pengguna super ke sistem komputer. Namun, dimungkinkan juga untuk menggunakan beberapa eksploitasi, pertama untuk mendapatkan akses level rendah, kemudian untuk meningkatkan hak istimewa berulang kali hingga mencapai level administratif tertinggi (sering disebut "root").

Setelah eksploitasi diberitahukan kepada pembuat perangkat lunak yang terpengaruh, kerentanan sering kali diperbaiki melalui tambalan dan eksploitasi menjadi tidak dapat digunakan. Itulah alasan mengapa beberapa peretas topi hitam serta peretas militer atau badan intelijen tidak mempublikasikan eksploitasi mereka tetapi merahasiakannya.

Eksploitasi yang tidak diketahui semua orang kecuali orang yang menemukan dan mengembangkannya disebut sebagai *eksploitasi **zero day***.

Eksploitasi biasanya dikategorikan dan diberi nama berdasarkan jenis kerentanan yang mereka eksploitasi (lihat kerentanan untuk daftarnya), apakah eksploitasi itu lokal / jarak jauh dan hasil dari menjalankan eksploit (misalnya EOP, DOS, spoofing).

2. Menganalisis Fase Serangan

Jenis analisis ini menentukan fase serangan. Simak daftar berikut ini:

a. Footprinting
b. Scanning
c. Enumeration
d. Gaining access
e. Escalating privilege
f. Pilfering
g. Maintaining access
h. Covering tracks

a. Footprinting

Mencari rincian informasi terhadap sistem-sistem untuk dijadikan sasaran, mencakup pencarian informasi dengan menggunakan search engine, whois, dan DNS zone transfer.

Footprinting penting karena teknologi yang digunakan dalam sistem tertentu dan organisasi mereka adalah kunci kerentanan mereka. Tanpa metodologi footprinting yang tepat, poin-poin penting tentang teknologi dan organisasi sistem dapat diabaikan. Footprinting bisa menjadi tugas yang sulit saat mengidentifikasi postur keamanan

Area dan Informasi yang Dicari Penyerang:

1) Internet
   a) Nama domain
   b) Blok jaringan
   c) Alamat IP dari sistem yang dapat dijangkau
   d) Layanan Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP) sedang berjalan
   e) Sistem arsitektur
   f) Access Control List (ACL)
   g) Intrusion Detection Systems (IDSs) yang sedang berjalan
   h) Sistem enumeration (user and group names, system banners, routing tables)
2) Remote Access
   a) Analog/digital telephone numbers
   b) Tipe remote system
   c) Authentication mechanisms
3) Intranet
   a) Protokol jaringan digunakan
   b) Nama domain internal
   c) Blok jaringan
   d) Alamat IP dari sistem yang dapat dijangkau
   e) Layanan TCP dan UDP berjalan
   f) Sistem arsitektur
   g) ACLs
   h) IDSs berjalan

i) Pencacahan sistem

4) Extranet

a) Asal koneksi dan tujuan

b) Jenis koneksi

c) Mekanisme kontrol akses

b. Reconnaissance

Pengintaian mengacu pada fase persiapan ketika penyerang mengumpulkan informasi sebanyak mungkin tentang target sebelum benar-benar meluncurkan serangan. Footprinting, scanning, dan enumeration adalah bagian penting dari fase pengintaian.

Metodologi yang tepat yang diadopsi peretas saat mendekati target dapat sangat bervariasi. Beberapa mungkin secara acak memilih target berdasarkan kerentanan yang dapat dieksploitasi. Orang lain mungkin mencoba tangan mereka pada tingkat teknologi atau keterampilan baru. Yang lain mungkin secara metodologis bersiap untuk menyerang target tertentu karena sejumlah alasan.

c. Metodologi Pengumpulan Informasi

Kegiatan pengumpulan-informasi secara garis besar dapat dibagi menjadi tujuh tahap:

1) Gali informasi awal.
2) Temukan jangkauan jaringan.
3) Pastikan mesin aktif.
4) Temukan port terbuka / titik akses.
5) Mendeteksi sistem operasi.
6) Temukan layanan pada port.
7) Petakan jaringan.

d. Alat Footprinting

Berikut ini adalah daftar alat footprinting yang tidak lengkap tapi signifikan. Setiap alat memiliki penawaran khusus yang unik serta kekurangannya. Peretas memiliki preferensi perangkat lunak yang terkait dengan gaya dan pilihan subjek mereka sendiri.

1) Sensepost Footprint Tools 3

Sensepost menawarkan penilaian keamanan, pelatihan, dan layanan konsultasi. Untuk memperluas layanan ini, Sensepost telah mengembangkan alat bernama BiDiBLAH. Proses penilaian keamanan melibatkan hal-hal berikut:

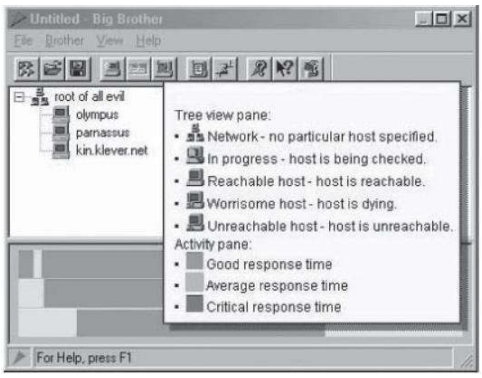
a) Information gathering
b) Footprinting
c) Targeting
d) Fingerprinting
e) Penemuan kerentanan
f) Penetration testing

Berikut ini adalah persyaratan sistem untuk BiDiBLAH:

a) Microsoft .NET framework
b) Nessus server atau login untuk fungsionalitas Nessus
c) Kunci Google API yang valid untuk penemuan subdomain
d) MetaSploit Framework untuk fungsionalitas MetaSploit

2) Big Brother

Big Brother adalah sistem berbasis web dan solusi pemantauan jaringan. Ini menyediakan sistem yang sangat skalabel, dapat disesuaikan, dan mudah dirawat dengan footprint kecil untuk memantau ketersediaan perangkat jaringan, server (Windows, UNIX, dan Linux) secara real-time, dan semua layanan terkait jaringan dalam infrastruktur TI apa pun. Gambar berikut contoh tampilan dari Big Brother:



Gambar 19. *Big Brother*

3) Advanced Administrative Tools

Advanced Administrative Tools adalah alat diagnostik jaringan dan sistem multithread. Ini dirancang untuk mengumpulkan informasi rinci dan status ketersediaan untuk jaringan dan komputer lokal. Ini mencakup beberapa fitur berikut:

a) Pemindai port
b) Penganalisis proxy
c) Pencari RBL
d) Penganalisis CGI
e) Pemverifikasi email
f) Penganalisis Link
g) Network monitor
h) Process monitor
i) WHOIS
j) System Information
k) Resource viewer

4) Wikto

Fitur alat footprinting Wikto (Gambar 2-8) adalah sebagai berikut:

a) Sidik jari server web menggunakan Net-Square's HTTPrint
b) Direktori dan ekstraksi link dari mirror menggunakan HTTrack
c) Deteksi director yang dapat diindeks di BackEnd
d) Pembaruan sekali klik dari database Nikto dan Google Hack
e) Dukungan SSL bawaan untuk Wikto dan BackEnd miner

e. Scanning

Pemindaian adalah salah satu fase terpenting dari pengumpulan intelijen bagi penyerang. Dalam proses pemindaian, penyerang mencoba mengumpulkan informasi tentang alamat IP tertentu yang dapat diakses melalui Internet, sistem operasi dan arsitektur sistem target, dan layanan yang berjalan di setiap komputer.

Tujuan pemindaian adalah untuk menemukan saluran komunikasi yang dapat dieksploitasi, menyelidiki sebanyak mungkin pendengar, dan melacak yang responsif atau berguna untuk kebutuhan khusus penyerang. Dalam fase pemindaian suatu serangan, penyerang mencoba menemukan berbagai cara untuk menyusup ke dalam sistem target. Penyerang juga mencoba untuk menemukan lebih banyak tentang sistem target dengan mencari tahu sistem

operasi apa yang digunakan, layanan apa yang sedang berjalan, dan apakah ada penyimpangan konfigurasi dalam sistem target atau tidak. Penyerang kemudian mencoba membentuk strategi serangan berdasarkan fakta yang dipelajari selama pemindaian. Berbagai jenis pemindaian adalah sebagai berikut:

1) *Port scanning*: Pemindaian port adalah proses pemeriksaan layanan yang berjalan pada komputer target dengan mengirimkan urutan pesan dalam upaya untuk masuk. Pemindaian port melibatkan koneksi ke port TCP dan UDP pada sistem target untuk menentukan apakah layanan sedang berjalan atau dalam kondisi mendengarkan.
2) *Network scanning*: Pemindaian jaringan adalah prosedur untuk mengidentifikasi host aktif di jaringan, baik untuk menyerang mereka atau sebagai penilaian keamanan jaringan.
3) *Vulnerability scanning*: Pemindaian kerentanan adalah metode yang digunakan untuk memeriksa apakah suatu sistem dapat dieksploitasi dengan mengidentifikasi kerentanannya. Pemindai kerentanan terdiri dari mesin pemindai dan katalog. Katalog terdiri dari daftar file umum dengan kerentanan yang diketahui dan eksploitasi umum untuk berbagai server.

Berbagai tujuan dilakukannya pemindaian adalah sebagai berikut:

1) Mendeteksi sistem hidup yang berjalan di jaringan.
2) Temukan port mana yang terbuka: Berdasarkan port yang terbuka, penyerang akan menentukan cara terbaik untuk masuk ke sistem.
3) Menemukan sistem operasi dari sistem target: Ini juga dikenal sebagai sidik jari. Penyerang akan merumuskan strategi berdasarkan kerentanan sistem operasi.
4) Menemukan layanan yang berjalan / mendengarkan pada sistem target: Ini memberi penyerang indikasi tentang kerentanan apa pun (berdasarkan layanan) yang dapat dieksploitasi untuk mendapatkan akses ke sistem target.
5) Menemukan alamat IP dari sistem target.
6) Mengidentifikasi aplikasi atau versi tertentu dari layanan tertentu.
7) Identifikasi kerentanan di salah satu sistem dalam jaringan: Hal ini dapat berguna dalam mengambil tindakan balasan untuk mengamankan sistem agar tidak diselidiki oleh penyerang.

f. Metodologi Scanning

Seorang penyerang mengikuti urutan langkah tertentu untuk memindai jaringan. Pendekatan umum telah disajikan, sehingga metode pemindaian mungkin berbeda berdasarkan tujuan spesifik penyerang. Langkah-langkah yang termasuk dalam pemindaian jaringan adalah sebagai berikut:

1) Memeriksa live systems: Seorang penyerang dapat memulai dengan tujuan memeriksa sistem live di jaringan.
2) Periksa port terbuka: Setelah sistem hidup ditemukan, penyerang akan mencari port terbuka untuk menentukan layanan mana yang berjalan pada sistem. Ini bisa menjadi langkah penting, karena beberapa layanan mungkin memiliki prioritas yang jauh lebih tinggi dari sudut pandang penyerang.
3) Sidik jari sistem operasi: Fase selanjutnya melibatkan sidik jari sistem operasi dengan mencari tahu tata letak jaringan target.
4) Pindai kerentanan: Identifikasi kerentanan di OS target adalah langkah selanjutnya. Peretas mungkin mencoba mengeksploitasi kerentanan ini selama serangan.
5) Selidiki jaringan: Penyerang juga dapat memilih untuk menyelidiki jaringan secara aktif atau diam-diam memantau lalu lintasnya. Ini dapat dilakukan dengan menggunakan proxy. Teknik penjelajahan anonim menyulitkan pelacakan aktivitas ini ke penyerang.

g. Enumeration

Teknik lain yang umum digunakan sebelum serangan sebenarnya adalah *enumeration*. *Enumeration* hanyalah proses mencari tahu apa yang ada di sistem target. Jika targetnya adalah seluruh jaringan, penyerang ingin mengetahui server, komputer, dan printer apa yang ada di jaringan itu. Jika targetnya adalah komputer tertentu, penyerang ingin mengetahui pengguna dan folder bersama mana yang ada di sistem itu.

Berikut ini adalah beberapa alat *enumeration* lain yang populer di kalangan peretas dan dapat dengan mudah ditemukan di Internet:

1) Sid2User
2) Cheops (khusus Linux)
3) UserInfo
4) UserDump

5) DumpSec
6) Netcat
7) NBTDump

Daftar ini tidak lengkap, tetapi mencakup beberapa alat hitung yang paling umum digunakan. Untuk melindungi diri Anda dari pemindaian, Anda harus menggunakan teknik berikut:

1) Perhatikan jumlah informasi yang Anda posting di Internet tentang organisasi dan jaringan Anda.
2) Buat kebijakan perusahaan yang membutuhkan personel teknis untuk menggunakan papan buletin, ruang obrolan, dll. untuk data teknis, jangan gunakan nama asli Anda atau sebutkan nama perusahaan.
3) Gunakan IDS yang mendeteksi banyak pemindaian.
4) Blokir paket Internet Control Message Protocol (ICMP) masuk.

h. Gaining access

Akses adalah tempat di mana sebagian besar kerusakan biasanya terjadi, tetapi peretas dapat melakukan banyak kerusakan tanpa mendapatkan akses ke sistem. Misalnya, serangan penolakan layanan eksternal dapat menghabiskan sumber daya atau mencegah layanan berjalan di sistem target. Layanan dapat dihentikan dengan menghentikan proses, menggunakan logika atau bom waktu, atau bahkan mengkonfigurasi ulang dan mengunci sistem. Sumber daya dapat digunakan secara lokal dengan menyelesaikan tautan komunikasi keluar.

Akses dapat diperoleh secara lokal, offline, melalui LAN atau melalui Internet. Contohnya mencakup buffer overflows berbasis heap, penolakan layanan, dan pembajakan sesi. Penyerang menggunakan teknik yang disebut ***spoofing*** untuk mengeksploitasi sistem dengan menyamar sebagai pengguna yang sah atau sistem yang berbeda. Mereka dapat menggunakan teknik ini untuk mengirim paket data yang berisi kesalahan ke sistem target untuk mengeksploitasi kerentanan. Paket flooding dapat digunakan untuk mengganggu ketersediaan layanan penting dari jarak jauh. Serangan *Smurf* mencoba membuat pengguna jaringan membanjiri satu sama lain dengan data, memberikan kesan bahwa semua orang menyerang dan membiarkan peretas anonim.

Peluang peretas untuk mendapatkan akses ke sistem target dipengaruhi oleh faktor-faktor seperti arsitektur dan konfigurasi sistem target, tingkat keahlian pelaku, dan tingkat akses awal yang diperoleh. Jenis serangan denial-of-service yang paling merusak dapat didistribusikan dengan serangan denial-of-service, di mana penyerang menggunakan perangkat lunak yang didistribusikan melalui beberapa mesin di Internet untuk memicu serangan denial-of-service terkoordinasi dari berbagai sumber.

i. Escalating privilege

Bila baru mendapatkan user password di tahap sebelumnya, di tahap ini diusahakan mendapat *privilese* admin jaringan dengan password *cracking* atau *exploit* sejenis getadmin, *sechole*, atau lc_messages. *Escalating Privilege* mengasumsikan bahwa penyerang sudah mendapatkan login access pada sistem sebagai user biasa. Penyerang kini berusaha naik kelas menjadi admin (pada sistem Windows) atau menjadi root (pada sistem Unix/Linux). Teknik yang digunakan sudah tidak lagi dictionary attack atau brute-*force attack* yang memakan waktu itu, melainkan mencuri password file yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem. Pada sistem Windows 9x/ME password disimpan dalam file. PWL sedangkan pada Windows NT/2000 dalam file SAM.

j. Pilfering

Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup evaluasi trust dan pencarian cleartext password di registry, config file, dan user data.

k. Covering tracks

Untuk alasan yang jelas, seperti menghindari masalah hukum dan mempertahankan akses, penyerang biasanya akan berusaha untuk menghapus semua bukti tindakan mereka. Trojan seperti ps atau netcat sering kali digunakan untuk menghapus aktivitas penyerang dari file log sistem. Setelah Trojan dipasang, penyerang kemungkinan besar telah menguasai sistem secara total. Dengan menjalankan skrip di Trojan atau rootkit, berbagai file penting diganti dengan versi baru, menyembunyikan penyerang dalam hitungan detik.

Teknik lain termasuk steganografi dan tunneling. Steganografi adalah proses menyembunyikan data dalam data lain, seperti file gambar dan suara. *Tunneling* memanfaatkan protokol transmisi dengan mengangkut satu protokol ke protokol lainnya. Bahkan sejumlah kecil ruang ekstra di header TCP dan IP dari sebuah paket data dapat digunakan untuk menyembunyikan informasi. Penyerang dapat menggunakan sistem yang disusupi untuk meluncurkan serangan baru terhadap sistem lain atau menggunakannya sebagai sarana untuk menjangkau sistem lain di jaringan tanpa terdeteksi.

Oleh karena itu, fase serangan ini bisa menjadi fase pengintaian dari serangan lain. Administrator sistem dapat menyebarkan IDS berbasis host (sistem deteksi intrusi) dan perangkat lunak antivirus untuk mendeteksi Trojan dan file serta direktori lain yang tampaknya dikompromikan. Sebagai seorang ethical hacker, Anda harus mengetahui alat dan teknik yang digunakan penyerang, sehingga Anda dapat mendukung dan menerapkan tindakan pencegahan.

l. Creating Backdoors

Pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ini dengan cara membentuk user account palsu, menjadwalkan batch job, mengubah startup file, menanamkan servis pengendali jarak jauh serta monitoring tool, dan menggantikan aplikasi dengan trojan.

m. Denial-of-service

Salah satu bentuk serangan yang paling umum dan paling sederhana pada sistem adalah DoS. Serangan ini bahkan tidak mencoba untuk mengganggu sistem Anda atau untuk mendapatkan informasi sensitif; ini hanya bertujuan untuk mencegah pengguna yang sah mengakses sistem. Jenis serangan ini cukup mudah dilakukan. Konsep dasar membutuhkan minimal keterampilan teknis. Ini didasarkan pada fakta bahwa perangkat apa pun memiliki batasan operasional.

Komputer tidak berbeda dari mesin lainnya; mereka juga memiliki batasan. Semua sistem komputer, server web, atau jaringan hanya dapat menangani beban terbatas. Beban kerja untuk sistem komputer dapat ditentukan oleh jumlah pengguna secara bersamaan, ukuran file, kecepatan

transmisi data, atau jumlah data yang disimpan. Jika Anda melebihi salah satu dari batas tersebut, kelebihan beban akan menghentikan sistem dari merespons. Misalnya, jika Anda dapat membanjiri server web dengan lebih banyak permintaan daripada yang dapat diprosesnya, itu akan kelebihan beban dan tidak dapat lagi menanggapi permintaan lebih lanjut.

Serangan ini sebenarnya jauh lebih sederhana daripada banyak serangan lainnya, dan karenanya cukup lazim. Setiap teknologi memiliki batasan; jika Anda dapat melebihi batas tersebut, maka Anda dapat membuat sistem offline. Realitas inilah yang mendasari serangan DoS. Cukup membebani sistem dengan permintaan, dan itu tidak akan dapat lagi menanggapi pengguna sah yang mencoba mengakses server web.

C. SOAL LATIHAN/ TUGAS

1. Jelaskan apa yang dimaksud dengan eksploitasi keamanan!
2. Jelaskan metode untuk mengklasifikasikan eksploitasi!
3. Sebutkan jenis analisis fase serangan!
4. Sebutkan langkah yang termasuk dalam pemindaian jaringan!
5. Terkait keamanan media sosial. Jelaskan mengenai metode social engineering yang saat ini sedang marak!

D. REFERENSI

Vacca, J. R. (2017). *Computer and Information Security Handbook*. 3rd Edition. Elsevier, Inc.

Lincke, S. (2015). Security Planning An Applied Approach. London: Springer International Publishing Switzerland.

Bosworth, S., Kabay, M. E., & Whyne, E. (2014). Computer Security Handbook. 6th Edition. Canada: John Wiley & Sons, Inc.

Walker, M. (2017). CEHTM Certified Ethical Hacker Exam Guide Premium. 3rd Edition. New York: McGraw-Hill Education.

Garrison, C. P. (2010). Digital Forensics for Network, Internet, and Cloud Computing. Syngress, Elsevier, Inc.

EC-Council Press. (2010). Ethical Hacking and Countermeasures Attack Phases. Australia: EC-Council.

Hoffman, A. (2020). Web Application Security Exploitation and Countermeasures for Modern *Web Applications*. O'Reilly Media, Inc.

Paulsen, C., & Byers, R. D. *Glossary of Key Information Security Terms* [Internet]. Juli 2019. NIST Pubs. Tersedia pada: https://www.nist.gov/publications/glossary-key-information-security-terms-2, https://csrc.nist.gov/glossary

http://www.iana.org/assignments/port-numbers