EC-Council

The Ethical Hacker's Guide To System Hacking

Attacker acquires information through techniques such as foot printing, scanning and enumeration to hack the target system.

1

System Hacking concepts

Footprinting

It is the process of accumulating data regarding a specific network environment. In this phase, the attacker creates a profile of the target organization, obtaining information such as its IP address range, namespace and employees. Footprinting eases the process of system hacking by revealing its vulnerabilities

Scanning

This is a procedure for identifying active hosts, open ports, and unnecessary services enabled on ports. Attackers use different types of scanning, such as port scanning network scanning, and vulnerability, scanning of target networks or systems which help in identifying possible vulnerabilities.

Enumeration Module

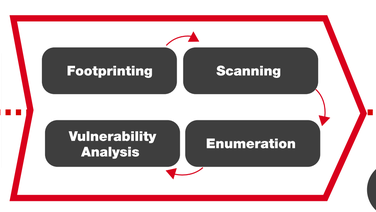
This is a method of intrusive probing, through which attackers gather information such as network user lists, routing tables, security flaws, and simple network protocol data (SNMP) data.

Vulnerability Analysis

Vulnerability Assessment is an examination of the ability of a system or application, including current security procedures, and controls to with stand assault. Attackers perform this analysis to identify security loopholes, in the target organization's network, communication infrastructure, and end systems.

2

CEH Methodology



3

CEH Hacking Methodology (CHM)

Gaining Access

It involves gaining access to low-privileged user accounts by cracking passwords through techniques such as brute forcing, password guessing, and social engineering and then escalate their privileges to administrative levels, to perform a protected operation.

Maintaining Access

After gaining access to the target system, attackers work to maintain high levels of access to perform malicious activities, such as stealing, hiding or tampering with sensitive files.

Clearing Logs

To maintain future system access, attackers attempt to avoid recognition by legitimate system users. To remain undetected, Attackers wipe out the entries corresponding to their activities in the system log.

4

System Hacking Goals

Hacking Stage	Escalating Privileges
Goal	To acquire the rights of another user or and admin
Technique used	Exploiting known system vulnerabilities

Hacking Stage	Gaining Access
Goal	To bypass access controls to gain access to the system
Technique used	Password cracking, Social engineering

Hacking Stage	Executing Applications
Goal	To create and maintain remote access
Technique used	Trojans, spywares, backdoors, keyloggers

Hacking Stage	Hiding Files
Goal	To hide attackers malicious activities and data theft
Technique used	Rootkits, stenography

Hacking Stage	Covering Tracks
Goal	To hide the evidence of compromise
Technique used	Clearing logs

5

Password Cracking

Attackers use this technique to gain unauthorized access to vulnerable system. Such a technique is mostly successful due to weak or easy passwords.

Types of Password attacks

Non- Electronic

Social Engineering
Convincing people to reveal passwords

Shoulder Surfing
Looking at either the user's keyboard or screen while he/she is logging in

Dumpster diving
Searching for sensitive information in the user's trash-bins, printer trash bins, and user desk for sticky notes.

Active Online Attack – Dictionary, Brute Forcing and Rule Based attack

Social Engineering
Convincing people to reveal passwords

Shoulder Surfing
Looking at either the user's keyboard or screen while he/she is logging in

Dumpster diving
Searching for sensitive information in the user's trash-bins, printer trash bins, and user desk for sticky notes.

Active Online Attack – Dictionary, Brute Forcing and Rule Based attack

Dictionary
A dictionary file is loaded into the cracking application that runs against user accounts

Brute Forcing
The program tries every combination of characters until the password is broken

Rule Based attack
This attack is used when the attacker gets some information about the password

Active Online Attack – Password Guessing

The attacker creates a list of all possible passwords from the information collected through social engineering or any other way and tries them manually on the victim's machine to crack the passwords.

Find a valid user
Create a list possible password
Rank passwords from high probability to low
Key in each password until correct password is discovered

Active Online Attack – Trojan/Spyware /Keylogger

- Attacker installs Trojan/spyware/keylogger on victim's machine to collect victim's usernames and passwords
- Trojan/spyware/keylogger runs in the background and sends back all user credentials to the attacker.

Active Online Attack – Hash Injection Attack

- A hash injection attack allows an attacker to inject a compromised hash into a local session and use the hash to validate network resources
- The attacker finds and extracts a logged-on domain admin account hash
- The attacker uses the extracted hash to log on to the domain controller.

Active Online Attack – LLMNR/NBT-NS Poisoning

- LLMNR/NBT are two main elements of windows operating systems used to perform name resolution for hosts present on the same link
- The attacker cracks the NTLMv2 hash obtained from the victim's authentication process
- The extracted credentials are used to log on to the host system in the network

Passive Online Attack – Wire Sniffing

- Attacker run packet sniffer tools on the local area network (LAN) to access and record the raw network traffic.
- The captured data may include sensitive information such as passwords (FTP, rlogin sessions, etc.) and emails.
- Sniffed credentials are used to gain unauthorized access to the target system

Passive Online Attack
Man in the Middle and replay attack

- In a MITM attack, the attacker acquires access to the communication channels between victim and server to extract the information
- In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant info is extracted, the tokens are placed back on the network to gain access.

6

How to Defend against Password Cracking

1.Enable information security audit to monitor and track password attacks
2.Do not use the same password during password change
3.Do not share passwords
4.Do not share passwords that can be found in a dictionary
5.Do not cleartext protocols and protocols with weak encryption
6.Set the password change policy to 30 days
7.Avoid storing passwords in an unsecured location
8.Do not use any systems default passwords
9.Make passwords hard to guess.
10.Ensure that applications neither store passwords to memory nor write them to disk in clear text.
11.Use a random string or prefix or suffix with the password before encrypting
12.Monitor servers' logs for brute force attacks on user accounts
13.Lock out an account subjected to too many incorrect password guesses
14.Enable SYSKEY with strong password to encrypt and protect SAM database

7

Escalating Privileges

- An attacker can gain access to the network using a non-admin user account and the next step would be to gain administrative privileges. These
- These privileges allow attacker to view critical/ sensitive information, delete files, or install malicious programs such as viruses, trojans, worms etc.,
- Attacker performs privilege escalation attack which takes advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and
software application to gain administrative access to the network and its associated applications.

- An attacker can gain access to the network using a non-admin user account and the next step would be to gain administrative privileges. These
- These privileges allow attacker to view critical/ sensitive information, delete files, or install malicious programs such as viruses, trojans, worms etc.
- Attacker performs privilege escalation attack which takes advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and
software application to gain administrative access to the network and its associated applications.

How to Defend Against keyloggers

1) Use pop up blocker and avoid opening junk emails
2) Install antispyware/virus programs and keep the signatures up to date
3) Install professional firewall software and anti-keylogging software
4) Recognize phishing emails and delete them
5) Update and patch system software regularly
6) Do not click on links in unwanted r doubtful emails that may point to malicious sites.
7) Use keystroke interference software which inserts randomized characters into every keystroke
8) Scan the files before installing and use registry editor or process explorer to check for the keystroke loggers
9) Use windows on-screen keyboard accessibility utility to enter the password or any other confidential information.
10) Install a host-based IDS, which can monitor your system and disable the installation of keyloggers
11) Use automatic form -filing password manager or virtual keyboard to enter username and password
12) Use software that frequently scans and monitors the changes in the system or network.

How to Defend against keyloggers

Hardware keylogger measures

1) Restrict physical access to sensitive computer systems
2) Periodically check all the computers and check whether there is any hardware device connected to the computer
3) Use encryption between the keyboard and its driver
4) Use an anti-keylogger that detects the presence of a hardware keyloggersuch as oxynger KeyShield
5) Use an On-screen keyboard and click on it.

Types of Keystroke Loggers

Hardware	Software
PC/BIOS Embedded	Application Keylogger
Embedded Keylogger Keyboard	Kernel Keylogger
External Keylogger	Hypervisor Based Keylogger
• PS/2 and USB Keylogger	Form Grabbing Based Keylogger
• Acoustic/CAM	
• Bluetooth keylogger	
• Wi-Fi Keylogger	

8

How to Defend against Privilege Escalation

1.Restrict the interactive logon privileges
2.Use encryption technique to protect sensitive data
3.Run users and applications on the least privileges
4.Reduce the amount of code that runs with privilege
5.Implement multi factor authentication and authorization
6.Perform de-bugging using bounds checkers and stress tests
7.Run services as unprivileged accounts
8.Test operating system and application coding errors and bugs thoroughly
9.Implement a privilege separation methodology to limit the scope of programming errors and bugs
10.Patch and update the kernel regularly

11.Change user account control settings to "Always Notify"
12.Restrict users from writing files to the search paths for applications
13.Continuously monitor file system permissions using auditing tools
14.Reduce the privileges of users and groups so that only legitimate administrators can make service changes
15.Use whitelisting tools to identify and block malicious software
16.Use fully qualified paths in all the windows applications
17.Ensure that all executables are placed in write-protect directories
18.In Mac operating systems make plist files read-only
19.Block unwanted system utilities or software that may be used to schedule tasks
20.Patch and update the web servers regularly

Other privilege Techniques

Access token Manipulation –
• Windows operating system uses access tokens to determine the security context of a process or thread
• Attackers can obtain access tokens of other users or generate spoofed tokens to escalate privileges and perform malicious activities by evading detection
Application Shimming
• Windows applications compatibility framework, shim is used to provide compatibility between the older and newer versions of windows operating system.
• Shims like RedirectEXE, injectDLL, GetProAddress, can be used by attackers to escalate privileges, install backdoors disable, windows defenders etc.
File System Permissions weakness
• If the file system permissions of binaries are not properly set, an attacker can replace the target binary with a malicious file
• If the process that is executing this binary is having higher level permissions, then the malicious binary also executes under higher level permissions.
Path Interception –
•Applications include many weaknesses and misconfigurations like unquoted paths, path environment variable misconfiguration and search order hijacking that lead to oath interception.
•Path interception helps an attacker to maintain persistence on a system and escalate privileges

Access token Manipulation –
• Windows operating system uses access tokens to determine the security context of a process or thread
• Attackers can obtain access tokens of other users or generate spoofed tokens to escalate privileges and perform malicious activities by evading detection
Application Shimming
• Windows applications compatibility framework, shim is used to provide compatibility between the older and newer versions of windows operating system.
• Shims like RedirectEXE, injectDLL, GetProAddress, can be used by attackers to escalate privileges, install backdoors disable, windows defenders etc.
File System Permissions weakness
• If the file system permissions of binaries are not properly set, an attacker can replace the target binary with a malicious file
• If the process that is executing this binary is having higher level permissions, then the malicious binary also executes under higher level permissions.

Type of privileges

• Horizontal – Refers to acquiring the same level of privileges that already has been granted but assuming the identity of another user with the similar privileges
• Vertical – Refers to gaining higher privileges than the existing

Scheduled Task –
•Windows task scheduler along with utilities such as 'at' and 'schtasks' can be used to schedule programs that can be executed at a specific date and time.
•Attacker can use this technique to execute malicious programs at system startup, maintain persistence, perform remote execution, escalate privileges etc.
Launch Daemon –
•LaunchD is used in MacOS and OS x boot up to complete the system initialization process by loading parameters for each launch on demand system-level daemon
•Daemons have plists that are linked to executable that run at start up
•Attacker can alter the daemons executable to maintain persistence or to escalate privileges
Plist Modification –
•Plist files in MacOS and OS X describe when programs should execute, executable file path, program parameters, required OS PERMISSIONS ETC.
•Attackers alter plist files to execute malicious code on behalf of a legitimate user to escalate privileges.
Setuid and Setgid
•In Linux and MacOS, is an application uses setuid or setgid then the application will execute within the privileges of the owning user or group
•An Attacker can exploit the applications with the setuid or setgid flags to execute malicious code with elevated privileges.
Web shell –
•A web shell is a web-based script that allows access to a web server
•Attackers create web shells to inject malicious script on a web server to maintain persistent access and escalate privileges

9

Executing Applications

Once attacker gain higher privileges on the target system by trying various privilege escalation attempts, they may attempt to execute a malicious application by exploiting a vulnerability to execute arbitrary code.

10

Tools for Executing Applications

Attackers execute malicious applications in this stage.
This is called "owning" the system.
The malicious programs attackers execute on target system:
Backdoors – Program designed to deny or disrupt operation, gather information that leads to exploitation or loss of privacy, gain unauthorized access to system resources.
Crackers – piece of software or program designed for cracking a code or passwords.
Keyloggers – This can be hardware or a software type. In either case, the objective is to record each keystroke made on the computer keyboards. It allows attacker to gather confidential information about victim such as email ID, passwords, banking details, chat room activity, IRC etc.
Spyware - Spy software may capture screenshots and send them to a specified location defined by the hacker.

11

Keyloggers

RemoteExe – Remotely installs applications, executes programs/scripts and updates files and folders on windows systems throughout the network.

- Tools used for executing application remotely helps attackers perform various malicious activities on target systems. After gaining administrative privileges, attackers use these tools to install, execute, delete and/or modify the restricted resource on the victim machine.
- It allows attacker to modify the registry, change local admin passwords, disable local accounts, and copy/update/delete files and folders.

- Keystroke loggers are programs or hardware devices that monitor each keystroke as user types on a keyboard, logs onto a file, or transmits them to a remote location.
- Legitimate applications for keyloggers include office and industrial settings to monitor employee's computer activities and in-home environments where parents can monitor and spy on children's activity.
- It allows attacker to gather confidential information about victim such as email ID, passwords, banking details, chat room activity, IRC, instant messaging etc.
- Physical keyloggers are placed between the keyboard hardware and the operating system.

12

Spyware

Spyware allows attackers to gather information about a victim or organization such as email addresses, user logins, passwords, credit cards, banking credentials etc.

Spyware	USB Spyware	Audio Spyware
ACTIVtrak	USB Analyzer	Spy Voice Recorder
Veriato 360	USB Monitor	Spy Audio listening Device
Netvizor	USB Deview	Spy USB Voice Recorder
Activity Monitor	Advanced USB Port Monitor	Audio Spy
Soft Activity TS Monitor	USB Monitor Pro	Voice activated flash drive voice recorder

Video	Telephone/cellphone	GPS Spyware
Mov, avi Video Editor	Phone spy	Spyera
Free2x webcam recorder	XNSPY	mSpy
iSpy	iKeyMonitor	Mobile spy
NET video Spy	OneSpy	Mobistealth
Eyeline Video Surveillance Software	TheTruthSpy	FlexiSpy

How to Defend against Spyware

- Try to avoid using any computer system which is not totally under control
- Adjust browser security settings to medium or higher for internet zone
- Be cautious about suspicious emails and sites
- Enable firewall to enhance the security level of the computer
- Update the software regularly and use a firewall with outbound protection
- Regularly check task manager report and MS configuration manager report

Update virus definition files and scan the system for spyware regularly

- Install and use anti-spyware software
- Perform web surfing safely and download cautiously
- Do not use administrative mode unless it is necessary
- Keep your operating system up to date
- Do not download free music files, screensavers, or smiley faces from internet
- Beware of pop-up windows or webpages.
- Carefully read all disclosures, including the license agreement and privacy statement before installing any application

13

Hiding Files

Root Kits

Root Kits are programs that **hide their presence** as well as attacker's malicious activities, granting them full access to the server or host at that time and in future.

Rootkits replace certain operating system calls and utilities with its own **modified versions** of those routines that in turn determine the security of the target system causing **malicious functions** to be executed.

A typical rootkit comprises of backdoor programs, Ddos programs, packet-sniffers, log-wiping utilities, IRCBots, etc.

Objectives of Rootkit

- To root the host system and gain remote backdoor access.
- To mask attacker tracks and presence of malicious applications or processes.
- To gather sensitive data, network traffic, from the system to which attackers might be restricted or possess no access.
- To store other malicious programs on the system and act as a server resource for bot updates.

Attackers Places a Rootkit by:

- Scanning for vulnerable computers and servers on the web.
- Wrapping it in a special package like games.
- Installing it on the public computers or corporate computers through social engineering.
- Launching zero day attack (privilege escalation, buffer overflow windows kernel exploitation, etc).

Types of Rootkits

Hypervisor Level	Acts as a hypervisor and modifies the boot sequence of the computer system to load the host operating system as a **virtual machine**
Hardware / Firmware	Hides in hardware devices or platform firm which is not inspected for **code integrity**
Kernel Level	Adds malicious code or replaces original **OS kernel** and **device driver codes**
Boot Loader Level	Replaces the original boot loader with one controlled by a remote attacker.

Types of Rootkits

Application Level	Replaces regular **application binaries** with fake trojan or modifies the behavior of existing applications by injecting malicious codes.
Library Levels	Replaces original system calls with fake ones to hide information about the attacker

Detecting Rootkits

Integrity Based Detection	It compares a snapshot of the file system, boot records or memory with a known trusted baseline
Signature - Based Detection	This technique compares characteristics of all system processes and executable files with a database of known rootkits fingerprints
Heuristic . Behavior Based Detection	Any deviation in the system's normal activity or behavior may indicate the presence of rootkit
Runtime Execution Path Profiling	This technique compares runtime execution paths of all system processes and executable files before and after the rootkit infection

14

Stenography

Detecting Rootkits

Cross View-based Detection	Enumerates key elements in the computer system such as system files, processes, and registry keys and compares them to an algorithm used to generate a similar data set that does not rely on the common APIs. Any discrepancies between these two data sets indicate the presence of rootkit

Stenography

- Stenography is a technique of hiding secret message with an ordinary message and extracting it at the destination to maintain confidentiality of data.
- Utilizing a graphic image as a cover is the most popular method to conceal data in files.
- Attackers can use stenography to hide messages such as list of the compromised servers, source code for the hacking tool, plans for future attacks etc.

Classification of Stenography

- Stenography
- Linguistic Stenography
  - ———— Semagrams — open codes
  - Visual semagrams — Covered Ciphers ———— Null Cipher
  - Text semagrams — Jargon code ———— Griller Cipher
- Technical stenography

15

Covering Tracks

Types of Stenography

- Image
- Document
- Folder
- Video
- Audio
- Whitespace
- Web
- Spam/email
- DVD-ROM
- Natural Text
- Hidden OS
- Source Code

16

Ways to Clear Online Tracks

Covering Tracks

Once intruders have successfully gained administrator access on a system, they will try to cover the tracks to avoid their detection.

Attackers use the following techniques to cover tracks on the target system

- Disable auditing – Disables auditing features
- Clearing Logs – clear/delete the system log entries
- Manipulating Logs -Manipulates logs in such a way that he/she will not be caught in legal actions.

Ways to Clear Online Tracks

Attackers clear online tracks maintained using web history, logs, cookies, cache, downloads. This way the victims cannot notice what online activities attacker have performed.

What attackers do to clear their online tracks

- Delete history
- Delete private data
- Delete cookies
- Clear cache on exit
- Delete all downloads
- Disable password manager
- Turnoff autocompletes
- Delete user JavaScript
- Remove most recently used
- Delete saved sessions.