



Penetration Testing

Implementation Plan

Azhar Ghafoor

Fall-2024

*Department of Cyber Security, FCAI
Air University, Islamabad*

3. System Hacking

Hacking is classified into some system hacking methods. These methods are also termed as CEH hacking methodology by EC-council. This methodology includes:

Topics discussed in this section:

Cracking passwords

Escalating privileges

Executing applications

Hiding files

Covering tracks

3.1. Cracking Passwords

- *Cracking passwords is the process of breaking into a system by guessing or stealing passwords.*

Common methods include:

- *Brute force attacks: Trying every possible combination of letters and numbers.*
- *Social engineering: Tricking people into giving their passwords.*

Examples:

*If your password is "password123," a hacker might guess it because it's a **common, weak password**. Once they break in, they can access your personal files.*

3.2 Privilege Escalation

- *Once inside a system, a hacker will attempt to gain higher access rights (admin or root access).*
- *With these elevated privileges, they can make changes to the system that a normal user wouldn't be allowed to do.*

Privilege escalation is further classified into two types: -

- *Horizontal privileges escalation*
- *Vertical privileges escalation*

Examples:

A hacker starts with guest access on your computer but finds a way to take over your admin account, giving them full control over your settings and files.

3.2 Privilege Escalation

Privilege Escalation by Operating System

Operating System	Credential Exploitation	Vulnerabilities & Exploits	Misconfigurations	Malware	Social Engineering
Windows	H	H	M	H	H
macOS	H	H	L	H	H
Unix	H	M	L	L	L
Linux	H	H	L	M	M
Infrastructure	H	M	M	M	M
Third-Party Applications	H	H	H	H	H
IoT	H	M	H	L	L
IIoT	H	M	H	L	L

Table Legend:

H – High occurrence and probability of an attack vector with a wide variety of threats against the organization

M – Medium probability of an attack vector against an organization with a medium chance of wide scale success

L – Rare or infrequent occurrence of an attack against an organization and a low probability it would be successful

3.2 Examples of Privilege Escalation

- ☐ *Windows Sticky Keys*
 - ☐ *Windows Sysinternals*
 - ☐ *Process Injection*
 - ☐ *Linux Passwd User Enumeration*
 - ☐ *Android Metasploit*
-
- ☐ **READ “What Are The Types Of Privilege Escalation Attacks?”**
 - ☐ **It's included in syllabus**
-

3.2.1 Horizontal privileges escalation

- *In horizontal privilege escalation, an attacker accesses resources or functionalities that belong to another user with the same privilege level.*

Working:

- *The attacker exploits a vulnerability in the application or system to gain access to another user's data or functions.*
- *This often involves manipulating session tokens, URLs, or access controls to bypass restrictions.*
- *Since the attacker does not increase their privilege level, the attack may go undetected by certain security measures.*

Examples:

A user with a regular account accesses another user's account data in a web application by changing the account ID in the URL.

3.2.2 Vertical privileges escalation

- *In vertical privilege escalation, an attacker moves from a lower privilege level to a higher one, gaining unauthorized access to more sensitive data or functions.*
- **Working:**
 - *The attacker exploits vulnerabilities in the system to elevate their privileges (e.g., from a regular user to an admin).*
 - *Techniques can include exploiting software vulnerabilities, leveraging insecure configuration, or bypassing access controls.*
 - *This type of escalation often involves gaining administrative or root access, which allows for greater control over the system.*

Examples:

An attacker exploits a flaw in an application to gain administrative privileges, allowing them to modify system settings and access sensitive information.

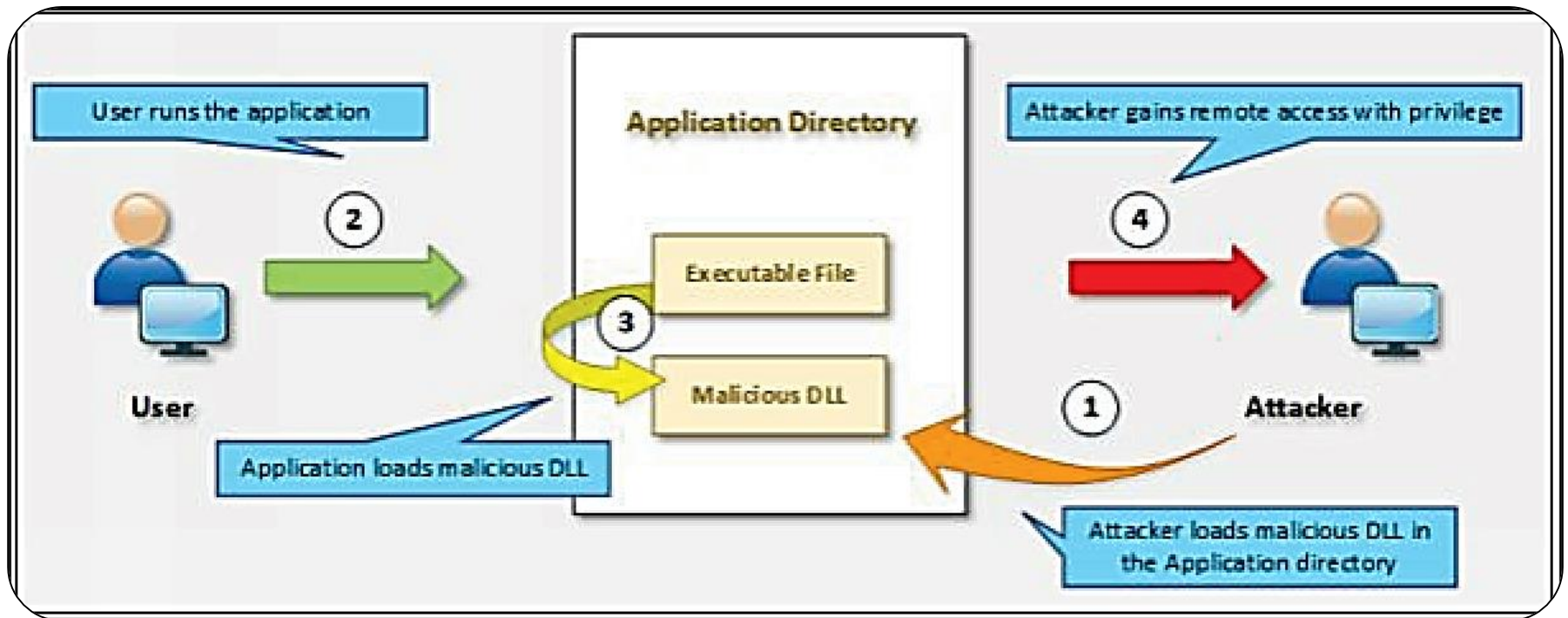
3.2.3 Privilege Escalation Using DLL Hijacking

- *DLL (Dynamic Link Library) hijacking is a type of attack where an attacker exploits a software application's reliance on specific DLL files.*
- *When a program runs, it loads DLL files, which contain code that the program needs. If an attacker can replace or insert a malicious DLL file, they can execute their code.*
 - Purpose: DLL files store reusable code, data, or resources used by multiple programs in Windows.
 - Function: They allow programs to share functionality without needing to duplicate code.
 - Example: A DLL might contain functions for displaying messages, managing files, or network communication.

Examples:

An attacker exploits a flaw in an application to gain administrative privileges, allowing them to modify system settings and access sensitive information.

Figure 3.2.3 Privilege Escalation Using DLL Hijacking



3.2.3 How DLL Hijacking Works

- **Targeting the Application:** *The attacker identifies a vulnerable application that loads a DLL file from a specific location.*
 - **Creating a Malicious DLL:** *The attacker creates a malicious DLL that performs actions like gaining elevated privileges or stealing data.*
 - **Replacing the Original DLL:** *The attacker places their malicious DLL in a location that the application searches for DLLs (like the same directory as the executable or a system path). When the application starts, it mistakenly loads the attacker's malicious DLL instead of the legitimate one.*
 - **Executing Malicious Code:** *Once loaded, the malicious DLL executes, potentially allowing the attacker to gain higher privileges or perform unauthorized actions within the application.*
-

3.2.3 Example Scenario

- ***Vulnerable Application:*** *A banking application that loads a DLL from its own directory.*
 - ***Malicious DLL Creation:*** *The attacker creates a DLL that captures user credentials.*
 - ***Hijacking the DLL:*** *The attacker places their DLL in the application's directory, replacing the legitimate one.*
 - ***Execution:*** *When the user opens the banking application, it unknowingly loads the attacker's DLL, allowing the attacker to capture sensitive information.*
-

3.3 Executing Applications

- *Hackers often run harmful programs once they have access. These programs can steal data, monitor activity, or give hackers remote control of your system.*

These are usually:

- *Remote Exec*
 - *Pdq Deploy*
 - *Keyloggers*
 - *Viruses*
 - *Spyware*
 - *Backdoors*
-

3.3.1. Remote Exec

- *Remote Exec is a tool or method that allows an administrator or attacker to execute commands or run scripts on a remote computer without needing direct access to it.*

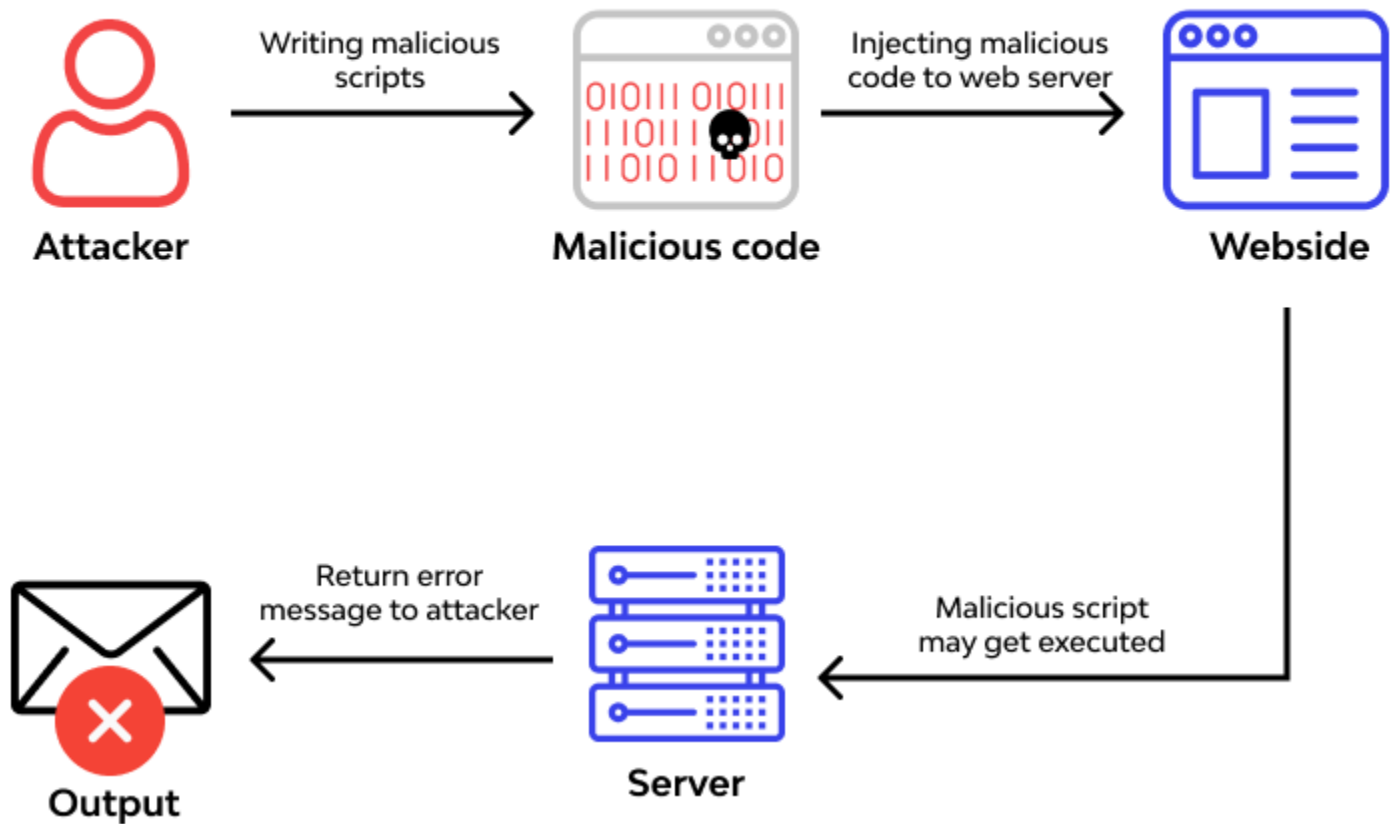
How it Works:

- *Connection Establishment: The tool connects to the target machine over a network using protocols like SSH or RDP.*
- *Command Execution: Once connected, it can execute commands, install software, or modify files on the remote system.*
- *Administrative Access: Typically requires administrative privileges to function effectively.*

Example:

System Administration: An IT admin uses Remote Exec to install software updates on multiple computers in a corporate network without physically accessing each machine.

3.3.1. Remote Exec



3.3.2. PDQ Deploy

- *PDQ Deploy is a software deployment tool/approach designed for Windows environments that enables administrators to remotely install software on multiple computers simultaneously.*

How it Works:

- *Package Creation: Administrators create deployment packages that include the software to be installed and any necessary configurations.*
- *Target Selection: The admin selects the target machines within the network for deployment.*
- *Execution: PDQ Deploy then pushes the package to the selected machines, executing the installation process remotely.*

Example:

Software Updates: An IT team uses PDQ Deploy to roll out a new version of an application to all employees' computers at once, saving time and effort.

3.3.3. Keyloggers

- *Keyloggers are malicious software or hardware designed to record keystrokes made by a user on their keyboard.*

How it Works:

Installation: Keyloggers can be installed through malware, phishing emails, or physical access to a device.

Keystroke Capture: Once active, the keylogger monitors and records every keystroke, including usernames, passwords, and other sensitive data.

Data Transmission: The captured data is typically sent back to the attacker through the internet, either in real-time or at scheduled intervals.

Types:

Software keylogger

Hardware keylogger

3.3.3 Software keylogger

- *A software keylogger is a malicious program installed on a computer or device that captures keystrokes and other user inputs.*

How it Works:

***Installation:** The keylogger is installed on the target device, often bundled with other software or downloaded via malicious links.*

***Keystroke Capture:** Once active, it runs in the background, monitoring and recording every keystroke, including passwords, messages, and other sensitive information.*

***Data Transmission:** The captured data is sent to the attacker, usually over the internet, either in real-time or at scheduled intervals.*

Example:

A user unknowingly downloads a free software tool that contains a hidden keylogger, which records their login credentials for online banking.

3.3.3 Software keylogger

Refog Personal Monitor - your trial period ends soon!

File Tools View Help

Users

- Admin - 127 / 127
 - Keystrokes Typed - 11 / 11
 - Screenshots - 9 / 9
 - Social Networks - 0 / 0
 - Websites Visited - 6 / 6
 - Clipboard - 1 / 1
 - Program Activity - 90 / 90
 - Computer Activity - 4 / 4
 - Webcam Shots - 0 / 0
 - File Tracking - 6 / 6
- James - 0 / 0

Table Report Play

Date and Time	Application	Window title
10/9/2019 1:39:07 PM	Windows Explorer	Run
10/9/2019 1:26:14 PM	Windows Explorer	Program Manager
10/9/2019 1:22:44 PM	Microsoft Edge	Sign Up - Refog - Microsoft Edge
10/9/2019 11:13:09 AM	Windows Explorer	Program Manager
10/9/2019 11:12:49 AM	Google Chrome	Wikipedia - Google Chrome
10/9/2019 11:10:06 AM	Windows Explorer	C:\Users\Admin\Desktop\Clipboard Test for Files\Source Directory
10/9/2019 11:08:08 AM	Notepad	Clipboard Test for Text.txt - Notepad
10/9/2019 11:07:58 AM	Notepad	Keylogger Test.txt - Notepad
10/9/2019 10:55:57 AM	Windows Explorer	Program Manager

10/ 9/2019 Latest records Today Last 7 days Last 30 days All records Custom...

10/9/2019 11:07:58 AM
Notepad - C:\Windows\System32\notepad.exe
Keys: 122 symbols

Keystrokes Typed

[Shift]This[Space] is[Space] a[Space] test.[Space] [Shift]ley[Backspace]t[Backspace][Backspace][Backspace][Backspace][Backspace][Shift]let's
[Space] try[Space] pressing[Space] some[Space] control[Space] keys.[Space] [Shift]Here...[Space] [Ctrl][Shift][Alt][Alt][Alt][Shift][Enter]
[Shift]What[Space] about[Space] backspae[Backspace]ce[Shift]?[Space] [Shift]Here...[Backspace][Backspace][Backspace]

Settings

BUY NOW

Search:

Process Monitor

Windows Keylogger

3.3.3 Hardware Keylogger

- *A hardware keylogger is a physical device that connects between a keyboard and a computer to record keystrokes.*

How it Works:

Connection: *The hardware keylogger is typically plugged into a USB port between the keyboard and the computer or can be integrated into the keyboard itself.*




Keystroke Capture: *It captures all keystrokes made on the keyboard without requiring software installation or interaction with the operating system.*

Data Storage: *The device stores the captured data internally, which can later be retrieved by the attacker through physical access to the device.*

Example:

An attacker installs a hardware keylogger on a public computer to capture sensitive information typed by users, such as passwords and credit card numbers.

3.3.3 Hardware Keylogger

	AirDrive Forensic Keylogger		AirDrive Forensic Keylogger Cable		AirDrive Forensic Keylogger Module		AirDrive Keylogger	
	Standard	Pro	Standard	Pro	Standard	Pro	Standard	Pro
Built-in memory	16 MB	16 MB	16 MB	16 MB	16 MB	16 MB	16 MB	16 MB
32X FPGA oversampling	✓	✓	✓	✓	✓	✓	✓	✓
Wi-Fi Access Point	✓	✓	✓	✓	✓	✓	✓	✓
Wi-Fi Device	-	✓	-	✓	-	✓	-	✓
Date and time-stamping	-	✓ NTP	-	✓ NTP	-	✓ NTP	-	✓ NTP
E-mail reporting	-	✓	-	✓	-	✓	-	✓
Live data streaming	-	✓	-	✓	-	✓	-	✓
USB flash drive mode	-	-	-	-	-	-	-	-
Dimensions	10 mm (0.4") x 17 mm (0.7") x 11 mm (0.4")		50 cm (20") USB cable 		12 mm (0.5") x 12 mm (0.5") 		20 mm (0.8") x 18 mm (0.7") x 12 mm (0.5") 	

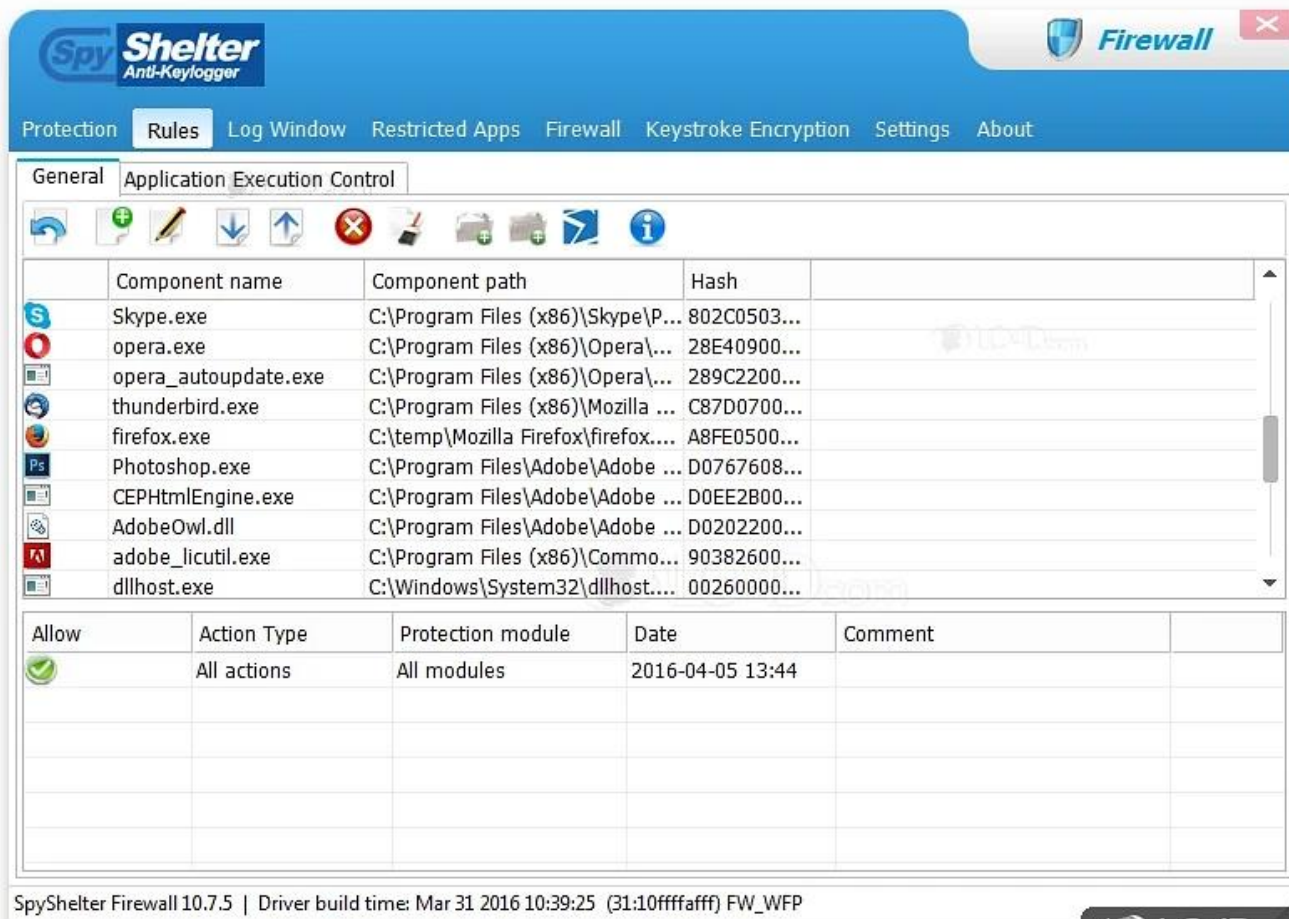
3.3.3 Anti-Keyloggers

- *Anti-keyloggers are application software which ensures protection against keylogging.*
- *This software eliminates the threat of keylogging by providing ssl protection, keylogging protection, clipboard logging protection and screen logging protection.*

Some of the anti-keylogger software are listed below: -

- *Zemana anti-keylogger (<https://www.Zemana.Com>)*
 - *Spyselter anti-keylogger software (<https://www.Spyselter.Com>) anti-keylogger (<http://anti-keyloggers.Com>)*
-

3.3.3 Anti-Keyloggers



3.3.4. Viruses

- *A virus is a type of malware that attaches itself to legitimate files or programs and spreads to other systems when infected files are shared.*

How it Works:

***Infection:** A user unknowingly executes an infected file, allowing the virus to activate.*

***Replication:** The virus replicates itself by attaching to other files or programs on the infected system.*

***Damage:** Viruses can corrupt or delete files, disrupt system performance, and lead to data loss.*

Example:

A user downloads a file that appears harmless but contains a virus that corrupts their operating system files.

3.3.5. Spyware

- *Spyware is malware designed to secretly monitor user activity and collect information without their knowledge.*

How it Works:

Installation: Spyware often comes bundled with legitimate software or is installed through deceptive methods (e.g., phishing).

Data Collection: It tracks user behavior, such as browsing history, keystrokes, and personal information.

Data Transmission: Collected data is sent to the attacker, who can use it for identity theft or financial fraud.

Example:

A user installs a free application that secretly installs spyware to monitor their online banking activity.

3.3.6. Backdoors

- *A backdoor is a hidden method of bypassing normal authentication or security measures, allowing unauthorized access to a system.*

How it Works:

***Installation:** Hackers install a backdoor on a compromised system to maintain access even after the initial vulnerability is patched.*

***Remote Control:** Once installed, the hacker can remotely control the system, execute commands, and install additional malware.*

***Stealth:** Backdoors are often hidden from the user and security software, making detection difficult.*

Example:

An attacker uses a backdoor to regain access to a system after the victim changes their passwords or security settings.

3.4. Hiding Files

- *Hackers conceal malicious files so that they're difficult to find.*
- *They may rename files to look like regular system files or hide them in deep directories so that system users or antivirus programs don't detect them.*

Examples:

A hacker hides malicious software in a folder labeled "System Updates," making it seem like a harmless program and avoiding detection by antivirus software.

3.5. Covering Tracks

- *Hackers work hard to delete any evidence that they were inside a system. They may clear system logs, delete browser history, or wipe any downloaded files to ensure they remain undetected.*

Examples:

A hacker deletes all the logs showing that they accessed your computer, making it almost impossible to trace their actions or figure out how they got in.

4. Goals of System hacking

In the methodological approach of system hacking, bypassing the access control and policies by password cracking or social engineering attacks will lead to gain access to the system.

Topics discussed in this section:

Data Theft

Unauthorized Access

System Control

Disruption of Services

Financial Gain

4.1. Data Theft

- *Hackers exploit vulnerabilities in systems or applications to gain unauthorized access to sensitive data.*
- *Techniques such as **SQL injection, phishing, or malware** can be employed to infiltrate databases and extract information.*
- *Stolen data can be sold on the dark web, generating significant profits for the hacker.*

Examples:

A hacker breaches an online retail database, stealing credit card information and personal details of thousands of customers.

4.2. Unauthorized Access

- *Hackers use techniques like credential stuffing (using **stolen credentials**) or exploiting **unpatched vulnerabilities** to gain access to user accounts and systems without permission.*
- *Once inside the network, the hacker can gather intelligence or further exploit the system for other malicious activities.*

Examples:

A hacker uses a list of leaked passwords to gain access to a corporate network and retrieve sensitive documents.

4.3. Bypassing System Controls

- *Hackers gain control over a compromised system by installing backdoors or rootkits, allowing them to bypass security controls and access system functionalities at will.*
- *Full control over the system enables the hacker to carry out further attacks, install additional malware, or gather intelligence.*

Examples:

A hacker installs a rootkit on a server to maintain persistent access, allowing them to execute commands and manipulate system processes remotely.

4.4. Disruption of Services

- *Hackers initiate Distributed Denial of Service (DDoS) attacks, overwhelming a target's resources to render services unavailable. This can be done using botnets to send a flood of requests.*
- *Disruption can cause financial losses for the target and damage their reputation, providing leverage in extortion scenarios.*

Examples:

A hacker launches a DDoS attack on an online gaming platform, causing server crashes and making the service unavailable for players.

4.5. Financial Gain

- *Hackers utilize various techniques to extort money from victims, such as deploying ransomware that encrypts files and demands payment for decryption keys or stealing payment information for fraudulent transactions.*
- *Successful financial gain can lead to substantial profits, often with minimal investment in the attack.*

Examples:

A hacker deploys ransomware on a hospital's network, encrypting patient data and demanding a ransom to restore access.

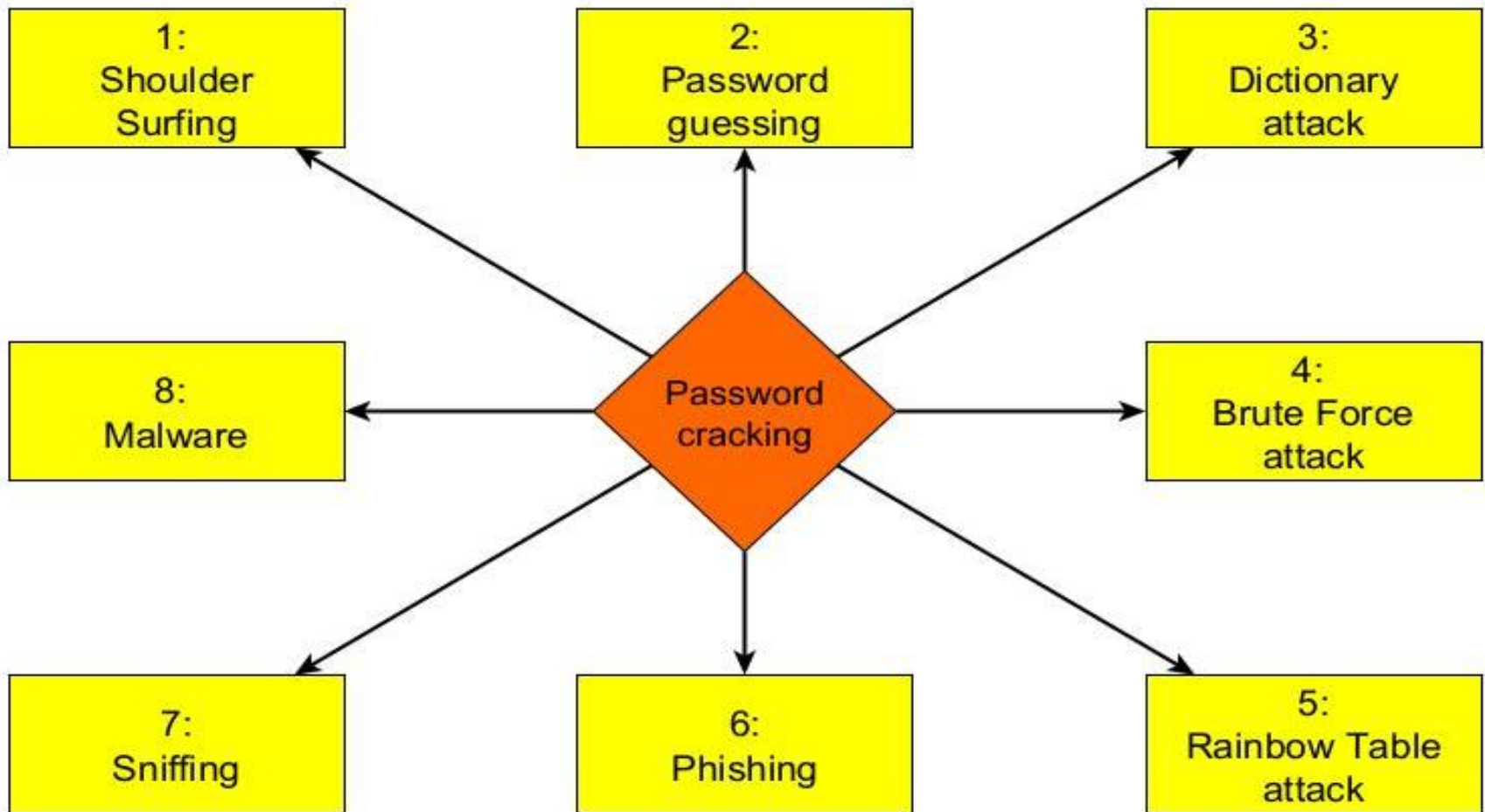
5 Password Cracking

Before proceeding to password cracking, you should know about three types of authentication factors:

- *Something I have, like username and password.*
- *Something I am, like biometrics*
- *Something I possess, like registered / allowed devices*

Password cracking is the method of extracting the password to gain authorized access to the target system in the guise of a legitimate user.

Figure 5.1 Types of Password Cracking



5.1. Shoulder Surfing

- *Observers watch a user enter sensitive information, such as passwords or PINs, in public settings.*
- *This can occur in crowded places like cafes, airports, or offices.*
- *Attackers can also use cameras or binoculars to capture this information from a distance.*

Examples:

A hacker stands close to someone using an ATM, watching as the user enters their PIN.

5.2. Password Guessing

- *Attackers attempt to access accounts by guessing passwords based on known information about the user (like birthdays, names, or common words).*
- *This method often involves trial and error, especially when the password is weak or predictable.*
- *Social engineering can also play a role, where hackers gather personal information to inform their guesses.*

Examples:

An attacker knows a user's birthday and tries using that date as a password to gain access to their social media account.

5.3. Dictionary Attack

- *Attackers use a list of common passwords or phrases (a "dictionary") to attempt unauthorized access.*
- *This method is efficient for cracking weak passwords, as it focuses on probable combinations rather than random attempts.*
- *Automated tools can significantly speed up the process by quickly cycling through the dictionary entries.*

Examples:

An attacker uses a program that tests every word in a pre-compiled list of common passwords against a target login.

5.4. Brute Force Attack

- *Attackers systematically try all possible combinations of characters to crack a password.*
- *This method can take a long time, depending on the complexity and length of the password.*
- *Advanced tools and computing power can help speed up this process by trying multiple combinations simultaneously.*

Examples:

An attacker uses a tool that attempts every combination of a six-character password, starting from "aaaaaa" and ending with "zzzzzz."

5.5. Rainbow Table Attack

- *Attackers utilize precomputed tables (rainbow tables) that contain hashed values of many possible passwords.*
- *When they obtain hashed passwords from a compromised database, they compare these hashes to those in the rainbow tables to find matches.*
- *This significantly reduces the time needed to crack passwords, as the heavy computational work is done in advance.*

Examples:

An attacker hashes a stolen password and checks it against a rainbow table to quickly find the original plaintext password.

5.6. Phishing

- *Attackers send fraudulent emails or messages that appear to come from legitimate sources to trick users into providing sensitive information.*
- *These messages often include links to fake websites designed to capture login credentials.*
- *Phishing can also occur via SMS (smishing) or phone calls (vishing).*

Examples:

An email appears to be from a bank, urging the recipient to click a link to verify their account information, leading to a fake login page.

5.7. Sniffing

- *Attackers capture network traffic using specialized software known as packet sniffers.*
- *This can be done on unsecured networks (like public Wi-Fi) where data packets are transmitted without encryption.*
- *Sniffers can collect sensitive information such as passwords, credit card numbers, and other personal data transmitted over the network.*

Examples:

An attacker on the same public Wi-Fi network uses a packet sniffer to capture login credentials as users access their email accounts.

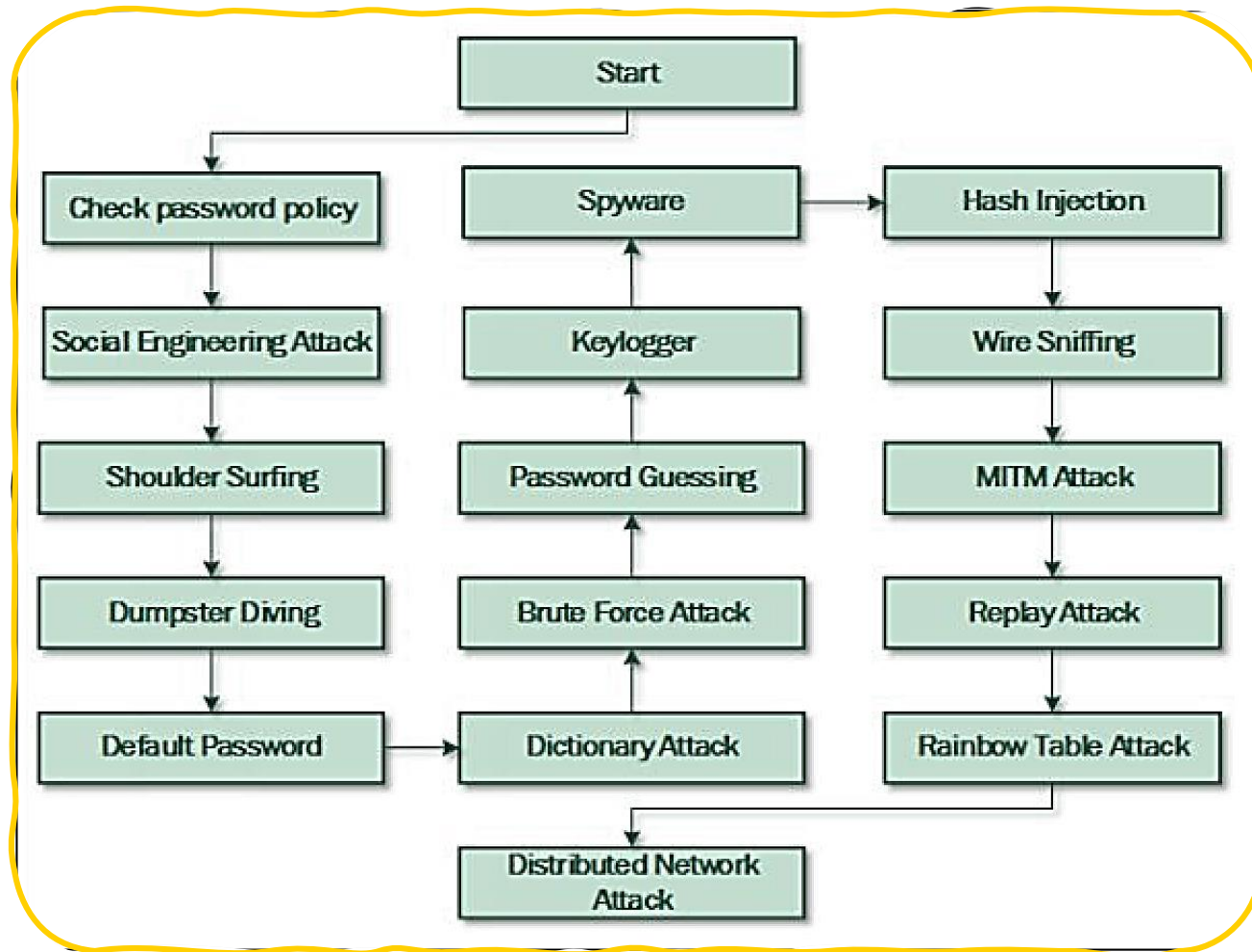
5.8. Malware

- *Malware is malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.*
- *It can be delivered through infected downloads, email attachments, or malicious websites.*
- *Once installed, malware can perform various functions, including stealing data, encrypting files, or creating backdoors for attackers.*

Examples:

A user downloads a seemingly legitimate software update that secretly installs ransomware, encrypting their files and demanding payment for recovery.

Figure 5.8 Password Cracking Flow Chart





Q&A



Thankyou