

Penetration test and Ethical hacking

Prepared by Dr. Nermin Hamza

CYB740

Lecture 4



Penetration test and Ethical hacking

Lecture 4

CYB740

Prepared by
Dr. Nermin Hamza

Outlines

- Introduction to Exploitation
- Different types of Exploits
- Exploits classification
- How Do Exploitation Occur?
- Malware
 - Viruses
 - Trojans
 - Backdoor and Keyloggers
 - Ransomware

Chapter

04

Exploitation

- Exploitation is the process of gaining control over a system



- It is important to understand that not every exploit leads to total system compromise.
- In many ways, **exploitation is an attempt to turn the target machine into a puppet** ^{دمية} that will execute your commands.

- Just to be clear, exploitation is the process of launching an exploit.
- Exploits are issues or bugs in the software code that give a hacker or attacker the ability to launch or execute a payload against the target system

Chapter

04

Exploitation

- After gathering enough information about the target, the next and third phase of ethical hacking and penetration test is to gain access to the target by exploiting the vulnerabilities and weak points in targets identified during reconnaissance and scanning.

- A successful vulnerability **exploit grants the control of the target to penetration** testers.
- For example, an ethical hacker that identifies open FTP ports on the target during the scanning phase may be able to exploit the FTP service to plant malware.

Different types of Exploits :

- **Known vulnerabilities:** Exploits security researchers know about and have documented. Exploits that target known vulnerabilities are often already patched but still remain a viable threat because of slow patching.
- **Zero-day exploits:** Vulnerabilities that have not been reported to the public or listed . This means cybercriminals have found the exploit before developers have been able to issue a patch, in some cases the developer may not even know of the vulnerability.

Exploits can be classified into five broad categories:

- **Hardware:** Poor encryption, lack of configuration management or firmware vulnerability.
- **Software:** Memory safety violations (buffer overflows, over-reads, dangling pointers), input validation errors (code injection, cross-site scripting (XSS), directory traversal, email injection, format string attacks, HTTP header injection, HTTP response splitting, SQL injection).
- **Network:** Unencrypted communication lines, man-in-the-middle attacks, domain hijacking, poor network security, lack of authentication or default passwords.
- **Personnel:** Poor setting policy and process, lack of security awareness training,, poor password management or falling for common social engineering attacks like phishing.
- **Physical site:** Poor physical security and lack of keycard access control.

How Do Exploits Occur?

There are several ways exploits occur:

- **Remote exploits:** Works over a network and exploits the vulnerability without prior access to the vulnerable system.
- **Local exploits:** Requires prior access to the vulnerable system and increases the privilege of the attacker past those granted by the security administrator.
- **Client exploits:** Exploits against client applications exist and usually consist of modified servers that send an exploit when accessed with a client application.

Hackers typically use many hacking tools and techniques to simulate attempted unauthorized access, including:

- Malware
- Password crack
- Remote exploitation
- Client exploitation
- Sniffing and Phishing
- Injection attacks
- Web hacking



Malware

Chapter

04

Malware

- Malware is malicious software that damages or disables computer systems and gives limited or full control of the system to the malware creator .

Chapter

04

Malware

Type	What It Does	Real-World Example
Ransomware	disables victim's access to data until ransom is paid	RYUK
Fileless Malware	makes changes to files that are native to the OS	Astaroth
Spyware	collects user activity data without their knowledge	DarkHotel
Adware	serves unwanted advertisements	Fireball
Trojans	disguises itself as desirable code	Emotet
Worms	spreads through a network by replicating itself	Stuxnet
Rootkits	gives hackers remote control of a victim's device	Zacinlo
Keyloggers	monitors users' keystrokes	Olympic Vision
Bots	launches a broad flood of attacks	Echobot
Mobile Malware	infects mobile devices	Triada
Wiper Malware	A wiper is a type of malware with a single purpose: to erase user data beyond recoverability.	WhisperGate



Virus

Chapter

04

Virus

- What is a virus?
 - A Computer Virus is one of the malware.
 - It is computer program that spreads or replicates by copying itself.
- The main parts of a virus' code are :-
 - The replication routine.
 - The payload routine.

Chapter

04

Virus

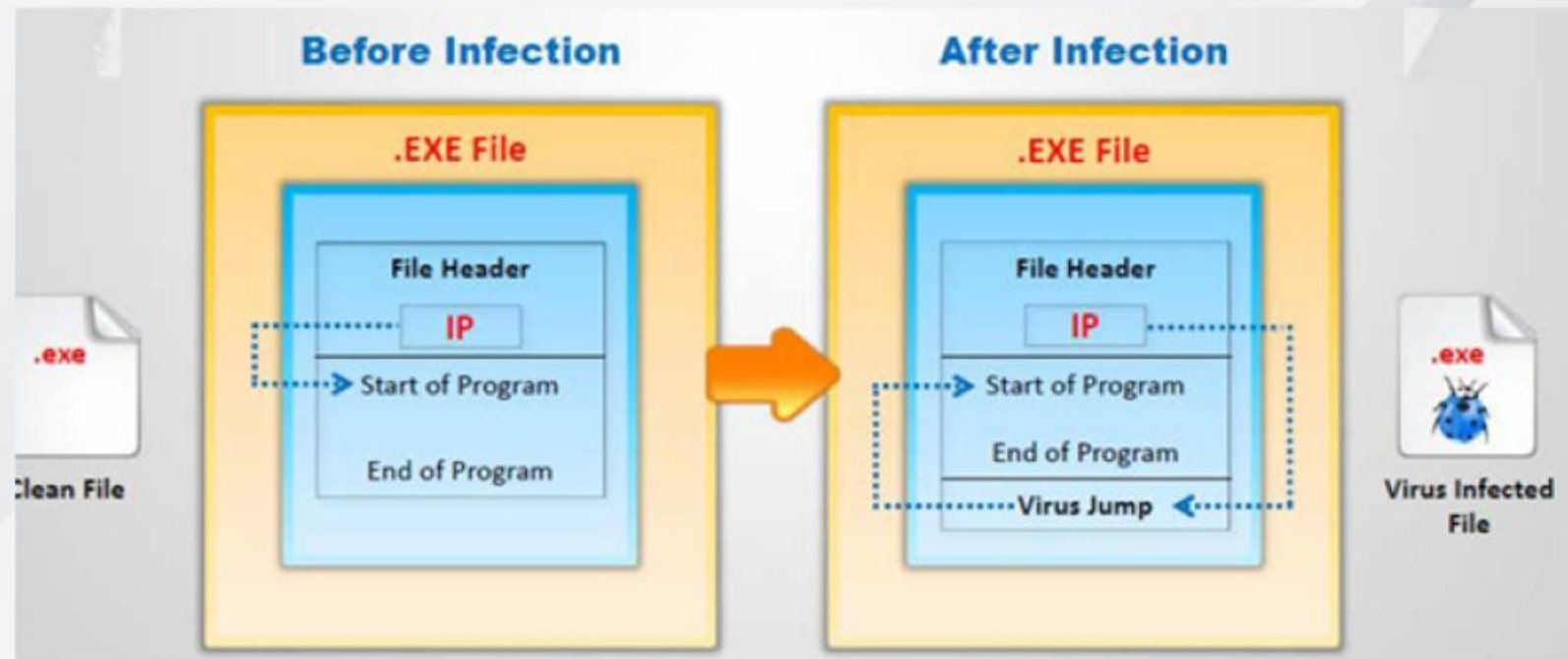
- The typical life-cycle of a computer virus takes place in four stages;
- The dormant phase **خامل**
- Propagation phase **التكاثر**
- The triggering phase **المشغل**
- And the execution phase **التنفيذ**.

Chapter

04

Virus

- Infection Phase : the virus replicates itself and attaches to an --- .exe file in the system



Different types of computer viruses



Polymorphic virus



Multipartite virus



Boot sector virus



File infector



Overwrite virus



Browser hijacker



Web scripting virus



Network virus



Macro virus

Chapter

04

File Infector Virus

- To persist on a system, a threat actor uses file infector viruses to inject malicious code into critical files that run the operating system or important programs.
- The computer virus is activated when the system boots or the program runs.
- One example of a file infector virus is the "CIH" virus, also known as the "Chernobyl" virus. CIH infects executable files on Windows systems and was first discovered in 1998. It spreads through infected files, typically distributed via email attachments or infected software downloads.
- CIH also contains a destructive payload that triggers on specific dates, such as April 26th (the anniversary of the Chernobyl nuclear disaster) .

What is a Boot Sector Virus?

- Boot sector viruses are a type of malware that infects a system's boot partition or the master boot record (MBR) of a hard disk. A boot sector is the section of a disk containing the code and data needed to start the operating system (OS) of a computer. While the computer is starting up and before security software is engaged, the virus executes its malicious code.



Chapter

04

Worms and virus

Computer worms and computer viruses are both types of malicious software, but they operate in slightly different ways.

Propagation Method:

- **Worms:** Worms are standalone malware programs that replicate themselves and spread across networks or the internet without requiring a host program to attach to. They exploit vulnerabilities in network protocols or operating systems to spread from one computer to another automatically.
- **Viruses:** typically require some form of user action to spread, such as running an infected program or opening an infected file. Once executed, viruses can replicate themselves by infecting other files or programs.

Payload:

- Viruses often carry a payload, which is the malicious action they are designed to perform, such as deleting files, corrupting data, or stealing information.
- Worms may also carry a payload, but their primary function is to spread rapidly across networks and systems, often causing congestion or disruption by consuming bandwidth or overloading servers.

Chapter

04

Prevention Tips: Virus

- Use strong, up to date, antivirus software to scan your device for suspicious activity
- When using removable storage devices, such as USB drives, scan it with an antivirus tool before accessing any of the files stored on it
- Avoid using storage devices that you don't know the content of
- Don't download files from emails you weren't expecting

The word "Trojan" is written in a bold, blue, sans-serif font. It is positioned to the right of a series of five overlapping vertical panels. Each panel contains a different educational icon: a graduation cap, a laptop with a play button, a target with an arrow, an open book, and a magnifying glass. The background of the panels is a warm, golden-brown color with a subtle gradient. The overall design is clean and modern, with a focus on education and technology.

Chapter

04

Trojan

- Hiding payload inside of some legitimate program that would run normally, with the payload running in the background.



How Much Damage Can Trojans Do?

- So, still thinking that the attachment was legitimate, you unwittingly downloaded and installed a Trojan.
- What happens now? The malware executes and starts damaging your computer, but the amount of damage depends on how the hacker designed the Trojan.
- In general, Trojan malware can:
 - Delete your files
 - Install additional malware
 - Modify data on your device
 - Copy your data
 - Disrupt your device's performance
 - Steal your personal information

How to infect systems by Trojan

- Prepare Trojan
- Create Wrapper (using Wrapper Tool)
- Execute Damage

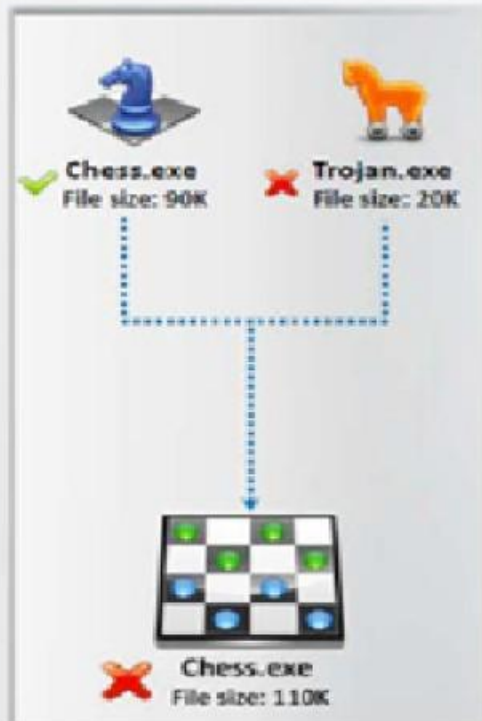


Chapter

04

Trojan

- A wrapper binds a Trojan executable with an innocent looking .exe application such as games or office applications.
- When the user runs the wrapped EXE, it first installs the Trojan in the background and then runs the wrapping application in the foreground .
- The two programs are Wrapped together into a single file.



Chapter

04

Types of Trojans

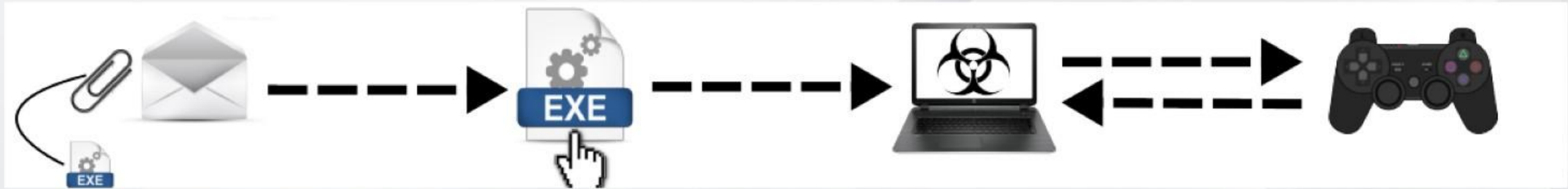
- Remote Access Trojans
- Data Sending Trojans
- Destructive Trojans
- Proxy Trojans
- FTP Trojans
- Security Software Disabler Trojans
- Denial of Service Attack Trojans

Chapter

04

Remote Access Trojans

- Remote Access Trojans (RATs) are software programs designed to facilitate covert enable unauthorized access to a victim's PC.



Chapter

04

Remote Access Trojans



SubSeven:

- The SubSeven Trojan is a RAT, which gives hackers remote control over Windows computers and networks. When it infiltrates a computer, SubSeven modifies system files and registries, causing the Trojan to execute upon startup.

- Proxy Trojans are malicious software intended for hijacking, transforming the victim's device into a proxy server.
- This grants hackers full control over the compromised device, enabling illegal activities like credit card fraud.
- Proxy Trojans conceal the true location of both the target user and the hacker's computer.

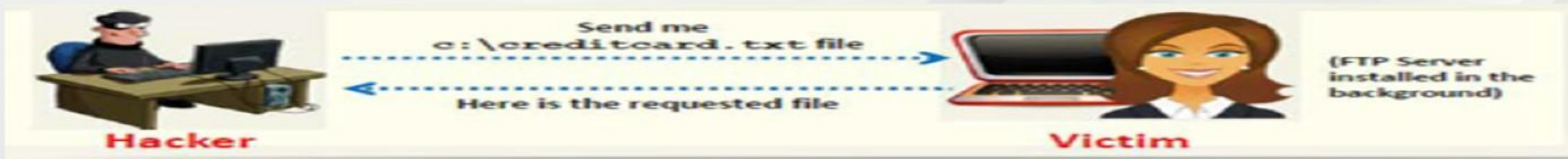


Chapter

04

Trojans: FTP Trojans

- FTP Trojans install an FTP server on the victim's machine which open FTP ports
- An attacker can then connect to the victim's machine
- Using FTP port to download any files that exist on the victim's computer



Chapter

04

Backdoor

- A backdoor refers to a hidden method or vulnerability within a computer system or software that allows unauthorized access to the system.
- A developer might create a backdoor to access an application, operating system (OS), or data for troubleshooting or other reasons. Attackers exploit these backdoors, either by utilizing ones installed by developers or by installing their own as part of a computer exploit.
- Backdoors can provide hackers with remote access to a system, allowing them to execute commands, steal data, or install additional malware without the user's knowledge.

Chapter

04

Backdoor

- Backdoors can provide hackers with remote access to a system, allowing them to execute commands, steal data, or install additional malware without the user's knowledge.
- In the context of an attack, backdoors are hidden mechanisms attackers use to access a system without authentication.
- However, vendors sometimes create backdoors for legitimate purposes, such as restoring a user's lost password or providing government entities with access to encrypted data.

Chapter

04

Backdoor

- Other backdoors are created and installed nefariously by hackers.
- Developers sometimes use backdoors during the development process and don't remove them, leaving them as a potential vulnerability point.

Chapter

04

Backdoor

- **Zyxel.** In early 2021, a Dutch cybersecurity firm discovered a backdoor secret account hardcoded in Zyxel firewalls and access point (AP) controllers. The secret account let attackers give themselves administrative privileges, including the ability to change firewall settings and intercept traffic. The backdoor exploited a vulnerability in the credentials used to update firewall and AP controller firmware.

Chapter

04

Backdoor

- **Back Orifice.** The hacker group Cult of the Dead Cow created this malware in 1998 to take advantage of vulnerabilities in the Windows OS. It installed backdoors that allowed remote control of Windows computers.

Chapter

04

keylogger

- A keylogger is a type of software or hardware device designed to record and log every keystroke made on a computer or mobile device.
- This includes keystrokes typed into applications, websites, or even passwords and sensitive information entered by users.
- Keyloggers can operate stealthily in the background, often without the user's knowledge, and the recorded keystrokes are typically saved to a file or transmitted to a remote location controlled by an attacker.

Chapter

04

Trojan , backdoor , Keylogger

- Trojan horse attacks often serve as the vehicle for delivering malware, including backdoors and keyloggers.
- In this context, a Trojan horse disguises itself as legitimate software, tricking users into unwittingly installing it.
- Once installed, the Trojan horse can deploy backdoors, which are hidden access points allowing attackers to enter systems undetected.
- Additionally, the Trojan horse may install keyloggers, which record keystrokes and other user activity, enabling attackers to capture sensitive information such as passwords and financial data.
- In summary, Trojan horse attacks deliver backdoors and keyloggers, facilitating unauthorized access and data theft.

Chapter

04

Ransomware

- Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.
- While some people might think "a virus locked my computer," ransomware would typically be classified as a different form of malware than a virus. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail.

Chapter

04

Ransomware

- Today, ransomware authors order that payment be sent via cryptocurrency or credit card, and attackers target individuals, businesses, and organizations of all kinds.

Ransomware attacks

- How exactly does a threat actor carry out a ransomware attack?
- First, they must gain access to a device or network. Having access enables them to utilize the malware needed to encrypt, or lock up, your device and data.
- There are several different ways that ransomware can infect your computer

Types of ransomware

Three main types of ransomware include scareware, screen lockers, and encrypting ransomware:

- **Scareware**: It includes rogue security software and tech support scams. You might receive a pop-up message claiming that malware was discovered and the only way to get rid of it is to pay up.

Screen lockers:

- When lock-screen ransomware gets on your computer, it means you're frozen out of your PC entirely. Upon starting up your computer, a full-size window will appear, often accompanied by an official-looking FBI or US Department of Justice seal saying illegal activity has been detected on your computer and you must pay a fine. However, the FBI would not freeze you out of your computer or demand payment for illegal activity. If they suspected you of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.

Chapter

04

Ransomware

Encrypting ransomware:

- These are the guys who snatch up your files and encrypt them, demanding payment in order to decrypt and redeliver.
- The reason why this type of ransomware is so dangerous is because once cybercriminals get ahold of your files, no security software or system restore can return them to you.
- Unless you pay the ransom—for the most part, they're gone. And even if you do pay up, there's no guarantee the cybercriminals will give you those files back.

Chapter

04

Ransomware

- <https://www.comparitech.com/ransomware-attack-map/>

Database of US ransomware attacks

Search in table

Page 1 of 175 >

Year	Month, Year ▾	Company Affected	Industry	Sub-Industry	City/County	State	# Records Affected	Ransom Paid	Ransom Amount	Ransomware Strain
2024	Oct, 2024	Wayne County	Government	Government	Detroit	Michigan	Unknown	Unknown	Unknown	Unknown
2024	Oct, 2024	Superior Court of California - County of Sonoma	Government	Government	Santa Rosa	California	Unknown	Unknown	20,000	Meow
2024	Oct, 2024	C.R. Laurence (CRL)	Business	Manufacturing	Los Angeles	California	Unknown	Unknown	Unknown	Unknown
2024	Oct, 2024	OzarksGo	Business	Utilities	Fayetteville	Arkansas	Unknown	Unknown	Unknown	Play
2024	Oct, 2024	Transak	Business	Finance	Miami	Florida	92,554	Unknown	Unknown	Stormous
2024	Oct, 2024	Globe Life	Business	Finance	McKinney	Texas	5,000	Unknown	Unknown	Unknown
2024	Sep, 2024	Great Plains Regional Medical Center	Healthcare	Healthcare	Elk City	Oklahoma	Unknown	Unknown	Unknown	Unknown
2024	Sep, 2024	Providence Public Schools	Education	Education	Providence	Rhode Island	Unknown	No	1,000,000	Medusa
2024	Sen	Delaware								

Chapter

04

How Antivirus Applications Work

- Most antivirus solutions start by comparing potentially dangerous code to a set of patterns and rules that make up the antivirus definitions, which match known malicious code.
- Antivirus definitions are updated regularly as new malware is identified by each vendor.
- This sort of identification is called **static analysis**.

Chapter

04

How Antivirus Applications Work

- In addition to static analysis against a set of signatures, more advanced antivirus solutions also test for malicious activity, called **dynamic analysis**.
- For example, a program that tries to replace every file on the hard drive or connects to a known botnet command and control server every 30 seconds is exhibiting potentially malicious activity and may be flagged.

Chapter

04

Online Scan

- One way to see which antivirus solutions will flag a program as malicious is to upload the file in question to the VirusTotal website (<https://www.virustotal.com/>).
- As of this writing, VirusTotal scans uploaded files with about 51 antivirus programs and reports which ones detect malware



Chapter

04

Online Scan



SHA256: 5a261239fe890e43d800afe373cff0733b51c98bea04a09d76cd75cb1c7ea7c7

File name: radmin.exe

Detection ratio: 25 / 51

Analysis date: 2014-03-24 04:58:44 UTC (1 minute ago)



Analysis

File detail

Additional information

Comments

Votes

Behavioural information

Antivirus	Result	Update
AVG	Win32/Patched.IA	20140324
Ad-Aware	Backdoor.Shell.AC	20140324
AntiVir	TR/Crypt.EPACK.Gen2	20140324



Thank You

Some references

- <https://www.geeksforgeeks.org/what-is-proxy-trojan/>