5th Assignment Ech - Malware And System Hacks

1. Types of Viruses

Viruses are malicious programs that infect files and systems. Common types include:

File Infector Virus – Attaches to executable files (.exe, .dll).
Boot Sector Virus – Infects the master boot record (MBR) of a disk.
Macro Virus – Targets documents (MS Word, Excel) using macros.
Polymorphic Virus – Changes its code to evade detection.
Resident Virus – Hides in RAM and activates when programs run.
Multipartite Virus – Spreads using multiple attack methods (files, boot sector).
Ransomware – Encrypts files and demands ransom for decryption.

2. Creating a Virus using HTTP RAT Trojan Tool

⚠ Disclaimer: Creating or distributing malware is illegal and unethical. This is for educational awareness only.

Steps (For Ethical Testing & Research):
Download HTTP RAT – A remote access Trojan (RAT).
Configure the Server – Enter attacker's IP and port.
Generate Payload – Creates a disguised executable file (.exe).
Spread via Phishing – Sent through fake emails or malicious links.
Control Infected System – Access victim’s system remotely.
◐ Prevention:

Use updated antivirus and firewalls.
Avoid downloading unknown files.
Enable behavior-based detection.

3. Explanation of Antivirus (Example: Windows Defender)

Antivirus software detects, prevents, and removes malware.

Example: Windows Defender
Built-in with Windows OS.
Uses real-time protection and cloud-based scanning.
Detects viruses, ransomware, phishing, and rootkits.
Features sandboxing to isolate threats.
◐ Why It’s Effective?

Automatic updates ensure new threats are blocked.
Low resource usage, ideal for home and business use.

==> System Hacking

1. Different Types of Hacking Methods

Hacking methods vary based on attack techniques and targets. Common types include:

Phishing – Tricking users into revealing credentials via fake emails/websites.
Keylogging – Capturing keystrokes to steal passwords.

MITM (Man-in-the-Middle) Attack – Intercepting data between two parties.
DDoS (Distributed Denial of Service) – Overloading a server to crash it.
SQL Injection – Injecting malicious SQL queries to steal database data.
XSS (Cross-Site Scripting) – Injecting scripts into websites to steal session data.
Zero-Day Exploits – Attacking unknown software vulnerabilities.
Brute Force Attack – Trying multiple password combinations.
Social Engineering – Manipulating people to give up sensitive info.

2. Types of Password Attacks
Brute Force Attack – Tries all possible password combinations.
Dictionary Attack – Uses common passwords from a predefined list.
Credential Stuffing – Uses leaked username-password combos.
Rainbow Table Attack – Precomputed hashes to decrypt passwords quickly.
Keylogging – Captures keystrokes to steal credentials.
Phishing – Tricks users into revealing passwords.
Shoulder Surfing – Physically spying on someone entering their password.
◐ Prevention: Use strong passwords, multi-factor authentication (MFA), and password managers.

3. Password Cracking Tools
pwdump7
Extracts hashed passwords from Windows SAM (Security Account Manager) files.
Requires Administrator privileges to run.
Used for forensic analysis & penetration testing.
Medusa
Fast brute force tool for cracking passwords.
Supports multiple protocols (SSH, FTP, HTTP, MySQL, etc.).
Can use wordlists & username lists for targeted attacks.
Hydra
Powerful parallel password cracking tool.
Supports over 50 protocols (SSH, RDP, Telnet, etc.).
Works on Windows, Linux, macOS.
Example:

hydra -l admin -P passlist.txt ssh://192.168.1.1
◐ Prevention: Use strong passwords, rate-limiting, MFA, and CAPTCHA protections.

4. Types of Steganography & Tools
Steganography is the technique of hiding secret data inside a normal file (images, audio, video).

Types:
Image Steganography – Hiding data inside images.
Audio Steganography – Encoding data in sound files.
Video Steganography – Embedding data in video frames.
Text Steganography – Using invisible characters in text.
Tools:
✔ QuickStego (Image Steganography)

Hides text messages inside images.

Simple UI, supports BMP and JPG formats.
✔ Echo (Audio Steganography)

Hides messages inside audio files using frequency masking.
Detectable only with specialized tools.
◐ Prevention: Use steganalysis tools and hash verification to detect hidden data.

5. Practical on Keylogger Tool
⚠ For Ethical Use Only! Keyloggers can be misused for illegal activities.

Steps to Use a Keylogger (Spyrix Free Keylogger as an Example)
Download & Install – Get Spyrix Free Keylogger or any ethical keylogging tool.
Run as Administrator – Ensures full logging permissions.
Enable Hidden Mode – Runs in the background without user awareness.
Start Logging – Records keystrokes, clipboard data, and screenshots.
Review Logs – Check captured keystrokes in the dashboard.
◐ Protection Against Keyloggers:

Use on-screen keyboards for sensitive input.
Enable antivirus and behavior monitoring.
Regularly check for suspicious processes in Task Manager