UNIT 04

Cyber Security Theory Manual

1. Network Exploitation

- **Definition**: Network exploitation involves leveraging vulnerabilities in network services or devices to gain unauthorized access to systems.
- **Key Concepts**:
  - Vulnerabilities in network protocols (TCP/IP stack, DNS, HTTP, etc.)
  - Common attack vectors (man-in-the-middle, DDoS, ARP spoofing, etc.)
  - Goals: Eavesdropping, Data Exfiltration, Privilege Escalation

2. OS Detection in Network

- **Definition**: Identifying the operating system running on a host within a network.
- **Techniques**:
  - **Passive OS Fingerprinting**: Analyzing network traffic without direct interaction (e.g., p0f).
  - **Active OS Fingerprinting**: Sending crafted packets to the target and analyzing responses (e.g., using Nmap's -O option).
- **Purpose**: Helps attackers and defenders to identify systems and assess potential vulnerabilities.

3. Scanning Techniques

Nmap (Network Mapper)

- **Purpose**: A tool for network discovery and security auditing.
- **Key Scanning Types**:
  - **Host Discovery**: Identifying active devices (e.g., `nmap -sn`).
  - **Port Scanning**: Identifying open or closed ports (e.g., `nmap -p-` for full port range).
  - **Service Detection**: Discovering services running on open ports (`nmap -sV`).
  - **OS Detection**: Determining the OS of the target (`nmap -O`).
  - **Script Scanning**: Using Nmap Scripting Engine (NSE) for more in-depth scanning (`nmap --script`).
  - **Nmap Configuration**: Customizing Nmap for stealthier or more detailed scans, adjusting timing, and scan options.

Open Ports vs Filtered Ports

- **Open Ports**: Ports that accept connections. These are the main entry points for exploitation.
- **Filtered Ports**: Ports protected by firewalls, appearing as filtered in Nmap results. They drop or reject packets without revealing much information.

4. Metasploit Framework

- **Purpose**: A powerful tool used for penetration testing and developing exploits.
- **Interface Overview**:
  - **msfconsole**: Command-line interface.
  - **msfdb**: Database for managing scan results and exploits.
  - **msfvenom**: Tool for generating payloads.
- **Common Metasploit Commands**:
  - `use exploit/multi/handler`
  - `set PAYLOAD windows/meterpreter/reverse_tcp`
  - `exploit`

5. Network Vulnerability Assessment

- **Definition**: The process of identifying, classifying, and prioritizing vulnerabilities in a network.
- **Tools**:
  - **Nessus**: Popular vulnerability scanning tool.
  - **OpenVAS**: Open-source vulnerability scanning framework.
- **Steps**:
  - Gathering information (scanning and enumeration)
  - Vulnerability scanning (active probing for weaknesses)
  - Exploitation (optional in penetration testing)

6. Evasion of Anti-Virus and Firewalls

- **Techniques**:
  - **Payload Obfuscation**: Encoding payloads to avoid detection (e.g., msfvenom's `-e` option).
  - **Encrypting Communication**: Using SSL/TLS to evade detection mechanisms.
  - **Traffic Shaping**: Mimicking legitimate traffic patterns to evade firewall detection.

7. Metasploit Scripting

- **Metasploit Module Creation**: Writing custom exploit or auxiliary modules.
- **Meterpreter Scripting**: Automating post-exploitation tasks.
- **msfvenom Custom Payloads**: Crafting customized payloads using various encoders and delivery mechanisms (e.g., adding encoding layers to avoid detection).

8. Exploits

- **Definition**: Code or techniques used to take advantage of a vulnerability.
- **Types**:
  - **Local Exploits**: Require local access to the system (privilege escalation).

    - **Remote Exploits**: Can be launched from a remote system (buffer overflow, remote code execution).
- **Exploit Delivery Methods**:
    - Direct attacks (via network services).
    - Through phishing emails or malicious downloads.

9. Vulnerabilities

- **Definition**: Weaknesses in software, hardware, or procedural systems that can be exploited by attackers.
- **Types**:
    - **Software Vulnerabilities**: Flaws in applications or operating systems (e.g., unpatched systems).
    - **Configuration Vulnerabilities**: Misconfigurations that expose systems (e.g., weak passwords, open ports).
    - **Zero-Day Vulnerabilities**: Previously unknown vulnerabilities that are not yet patched.

10. Payloads

- **Definition**: Code executed upon successful exploitation.
- **Types**:
    - **Meterpreter**: A post-exploitation tool with command-line access and more.

    - **Shell**: Provides a direct shell on the victim's system.
- **Custom Payloads**: Using tools like `msfvenom` to generate customized payloads, modifying encoding and formats to evade detection.

11. Social Engineering Toolkit (SET)

- **Purpose**: A framework for social engineering attacks (phishing, credential harvesting, etc.).
- **Common Scenarios**:
    - **Email Phishing**: Crafting phishing emails to obtain sensitive information.
    - **Credential Harvesting**: Setting up fake login pages to steal credentials.

12. Xerosploit Framework

- **Purpose**: A penetration testing tool focused on MITM (Man-In-The-Middle) attacks and other network exploits.
- **Features**:
    - **DNS Spoofing**: Redirecting victim's DNS queries.
    - **Injecting Code**: Injecting malicious code into web pages viewed by the victim.
    - **Sniffing**: Capturing data flowing through the network.

13. Burp Suite

- **Purpose**: A comprehensive web application security testing tool.
- **Components**:
  - **Proxy**: Intercepts and modifies traffic between browser and web server.
  - **Scanner**: Automated tool for detecting vulnerabilities in web applications.
  - **Intruder**: A tool for automating customized attacks (e.g., brute-force or fuzzing).
  - **Repeater**: For manual testing of requests and responses.

14. End Point Security

- **Definition**: Security measures that focus on protecting individual devices (endpoints) like laptops, mobile phones, and desktops.
- **Techniques**:
  - **Antivirus Solutions**: Preventing malware infections.
  - **Host-Based Firewalls**: Blocking suspicious traffic at the device level.
  - **Data Loss Prevention (DLP)**: Preventing data exfiltration.
  - **Endpoint Detection and Response (EDR)**: Monitoring, detecting, and responding to threats in real-time.

UNIT 05

Unit V: Wireless Attacks

WEB CONTENT:

https://www.codecademy.com/article/wireless-attacks

1. Wireless Concept

- **Definition**: Wireless communication allows devices to communicate without physical connections using radio waves. Common standards include Wi-Fi (IEEE 802.11) and Bluetooth.
- **Key Components**:
  - **Access Points (APs)**: Provide wireless network services.
  - **Stations (Clients)**: Devices connecting to the wireless network.
  - **Wireless Channels**: Frequencies over which wireless data is transmitted.

2. Wireless Encryption

- **Purpose**: To secure communication between wireless devices and prevent unauthorized access.
- **Types**:
  - **WEP (Wired Equivalent Privacy)**: Early encryption standard, weak and easily breakable.
  - **WPA (Wi-Fi Protected Access)**: Improved security over WEP, with TKIP encryption.
  - **WPA2**: Stronger encryption using AES, but still vulnerable to certain attacks.
  - **WPA3**: Latest standard, with improved encryption and protection against brute-force attacks.

3. Wireless Threats

- **Common Wireless Threats**:
  - **Eavesdropping**: Intercepting wireless communication to gather sensitive information.
  - **Rogue Access Points**: Unauthorized APs used to intercept or inject data into a network.
  - **Man-in-the-Middle (MitM)**: Attacker intercepts communication between two devices.

- **Denial-of-Service (DoS)**: Flooding the wireless network, causing it to crash or become unavailable.

4. Wireless Hacking Methodology

- **Steps in Wireless Hacking**:
  1. **Reconnaissance**: Gathering information about wireless networks (SSID, BSSID, encryption type) using tools like `airmon-ng`, `airodump-ng`.
  2. **Vulnerability Assessment**: Identifying weaknesses in encryption or configuration.
  3. **Exploitation**: Attacking identified vulnerabilities (e.g., WEP cracking, WPA handshake capture).
  4. **Post-Exploitation**: Using the network to intercept data, perform MITM attacks, etc.

5. Wireless Hacking and Security Tools

- **Aircrack-ng Suite**: Includes tools like `airmon-ng`, `airodump-ng`, `aireplay-ng`, `aircrack-ng` for monitoring, attacking, and breaking encryption.
- **Kismet**: A wireless network detector, sniffer, and intrusion detection system.
- **Wireshark**: A powerful packet analyzer to capture and analyze network traffic.
- **Reaver**: Used for cracking WPA/WPA2-PSK by exploiting WPS.
- **Fluxion Framework**: A tool for performing Evil Twin attacks to capture WPA/WPA2 credentials.

6. Bluetooth Hacking

- **Bluetooth Attacks**:
  - **Bluesnarfing**: Unauthorized access to a Bluetooth device's data (contacts, files, etc.).
  - **Bluejacking**: Sending unsolicited messages to Bluetooth-enabled devices.
  - **Bluebugging**: Gaining remote control of a Bluetooth device, allowing calls or SMS to be made without the user's knowledge.
- **Countermeasures**: Disable Bluetooth when not in use, set devices to non-discoverable mode, use strong pairing methods.

7. Countermeasures to Wireless Threats

- **Security Best Practices**:
  - **Use WPA3 Encryption**: Stronger protection against brute-force attacks.
  - **Disable WPS (Wi-Fi Protected Setup)**: Vulnerable to brute-force attacks.
  - **Regularly Update Firmware**: Ensure routers and devices have the latest security patches.
  - **Network Segmentation**: Isolate critical systems from guest or public networks.

8. Protocols

- **Common Wireless Protocols**:
  - **802.11**: Wi-Fi standard, covers all modern wireless networking protocols.
  - **WPA/WPA2/WPA3**: Encryption protocols securing wireless communication.
  - **WPS (Wi-Fi Protected Setup)**: Simplifies network setup but is vulnerable to attacks.
  - **EAP (Extensible Authentication Protocol)**: A framework for providing authentication.

9. MAC Filtering

- **Definition**: Allows only specific devices (based on their MAC addresses) to connect to the wireless network.
- **Limitations**: MAC addresses can be spoofed, making this an insufficient security measure on its own.

10. Packet Encryption

- **Purpose**: Ensures that the contents of transmitted packets are unreadable to unauthorized users.
- **Techniques**:
  - **WEP**: Weak encryption, can be cracked using tools like Aircrack-ng.
  - **WPA2-AES**: Stronger encryption standard, uses Advanced Encryption Standard.

11. Packet Sniffing

- **Definition**: Capturing packets transmitted over a network to analyze the data.
- **Tools**: Wireshark, Tcpdump.
- **Uses**: Detecting vulnerabilities, monitoring traffic, eavesdropping.

12. Types of Authentication

- **Open System Authentication**: No encryption, anyone can connect.
- **Pre-Shared Key (PSK)**: Password-based authentication, used in WPA/WPA2.
- **Enterprise Authentication**: Uses a RADIUS server for centralized authentication (e.g., WPA2-Enterprise with EAP).

13. ARP Replay Attack

- **Definition**: Attacker captures ARP (Address Resolution Protocol) packets and replays them to generate more network traffic, which can be used for cracking WEP encryption.
- **Tool**: `aireplay-ng` (from Aircrack-ng suite).

14. Fake Authentication Attack

- **Definition**: The attacker sends authentication requests to a wireless access point to stay connected long enough to capture more packets.
- **Use in Cracking**: Helps in maintaining a connection to capture the WPA handshake for cracking.

15. Deauthentication Attack

- **Definition**: Attacker forces devices off a wireless network by sending forged deauthentication frames, causing disconnection.
- **Purpose**: Can be used to capture WPA handshakes for password cracking.
- **Tool**: `aireplay-ng` (deauth mode).

16. Attacks on WEP, WPA, and WPA-2 Encryption

- **WEP Attacks**:
  - **Key Reinstallation Attack (KRACK)**: Exploits weaknesses in WPA2's four-way handshake.
  - **Weak IV Vulnerability**: Allows attackers to recover encryption keys and decrypt WEP packets.
- **WPA/WPA2 Attacks**:
  - **WPA Handshake Capture**: Attacker captures the WPA handshake between the client and the AP, which can then be brute-forced.
  - **WPS PIN Attack**: Attacker exploits weak WPS PINs to gain access to the WPA2 network.

17. Fake Hotspots

- **Definition**: Rogue wireless access points set up by attackers to mimic legitimate ones.
- **Purpose**: Trick users into connecting and capturing sensitive data.
- **Countermeasure**: Educate users to check for legitimate SSIDs and use VPNs.

18. Evil Twin Attack

- **Definition**: An attacker sets up a rogue access point mimicking a legitimate AP to intercept communication.
- **Steps**:
  1. Create an identical SSID to a legitimate network.
  2. Capture the victim's traffic.
  3. Perform MITM attacks to steal credentials or data.
- **Tools**: `airbase-ng`, `fluxion`.

19. Fluxion Framework

- **Definition**: A powerful tool that automates Evil Twin attacks and allows attackers to capture WPA/WPA2 credentials.
- **Features**:

- Rogue AP setup.
- Fake captive portal for credential harvesting.
- Real-time WPA password cracking.