Module 1
Lesson 1: Introduction to Ethical Hacking and Penetration Testing

- Ethical Hacking and Penetration Testing are critical components of modern cybersecurity

Defining Ethical Hacking

- Also known as penetration testing or white-hat hacking, involves legally and ethically attempting to penetrate a computer system, network or application to identify vulnerabilities and security weaknesses.

  Core Principles:

  - **Legality:** Ethical hackers must operate within the bounds of the law, meaning obtaining proper authorization before conducting any security assessments.

  - **Scope Definition:** A clear scope must be defined to outline the systems, networks, and applications that are permitted to be tested.

  - **Vulnerability Reporting:** Identified vulnerabilities must be reported to the organization with detailed recommendations for remediation. This allows the organization to address the weakness before being exploited by malicious actors.

  - **Data Confidentiality:** Ethical hackers must protect the confidentiality of any sensitive data they encounter during their assessments.

Objectives of Ethical Hacking

- **Identify Vulnerabilities:** The primary objective is to uncover security weaknesses in systems, networks, and applications.

- **Assessing Risks:** Determining the potential impacts of identified vulnerabilities on the organization’s assets and applications

- **Providing Remediation Recommendations:** Offering practical and actionable recommendations to address the identified vulnerabilities

- **Improving Security Posture:** Enhances the overall security of the organization by proactively identifying and mitigating risks

- **Compliance:** Meeting regulatory requirements and industry standards related to cybersecurity.

Understanding Penetration Testing

- A subset of ethical hacking that focuses on simulating real-world attacks to identify vulnerabilities and assess the effectiveness of security controls.

Penetration Testing Methodologies

- **Penetration Testing Execution Standard (PTES):** Provides a detailed framework for conducting penetration tests, conveying everything from planning and reconnaissance to reporting and remediation.

- **Open Source Security Testing Methodology Manual (OSSTMM):** Focuses on testing operational security, including processes, communication, and physical security controls.

- **NIST Special Publication 800-115:** Offers guidance on conducting information security assessments, including pentesting

- **OWASP Testing Guide:** Specifically focuses on website application security testing, providing a comprehensive tests to identify vulnerabilities

Phases of Penetration Testing

1. **Planning and Scoping -** Defining the objectives, scope, rules of engagement for the test. Includes identifying the systems to be tested, the types of attacks to be simulated, and any limitations or constraints.

2. **Reconnaissance -** Gathering all the information about the target system or network. This may involve passive reconnaissance (example is searching for public databases) and active reconnaissance (example is scanning network ports)

3. **Scanning -** Using tools to identify open ports, services, and potential vulnerabilities. This often involves using network scanners like Nmap, which we'll cover in detail later.

4. **Exploitation -** Attempting to exploit identified vulnerabilities to gain access to the system. This may involve using exploit frameworks like Metasploit (covered in Module 4).

5. **Post-Exploitation -** Performing activities after gaining access to the system, such as gathering additional information, escalating privileges, and maintaining access.

6. **Reporting -** Documenting the findings of the penetration test, including identified vulnerabilities, their potential impact, and recommendations for remediation.

Types of Penetration Testing

- **Black Box Testing:** The tester has no prior knowledge of the system being tested. This stimulates an external attacker attempting to gain access.

- **White Box Testing:** The tester has full knowledge of the system, including its architecture, code, and configurations. This allows for a more thorough and targeted assessment.

- **Gray Box Testing:** The tester has partial knowledge of the system. This is a common approach that balances the benefits of black box and white box testing.

Roles in Ethical Hacking and Penetration Testing

- **Penetration Tester:** The primary role is to conduct penetration tests and identify vulnerabilities. They possess strong technical skills in areas such as networking, system administration, and programming.

- **Security Analyst:** Security analysts analyze security data, investigate incidents, and implement security controls. They often work closely with penetration testers to understand identified vulnerabilities and develop remediation strategies.

- **Security Engineer:** Security engineers design, implement, and manage security systems and infrastructure. They are responsible for ensuring that security controls are properly configured and maintained.

- **Security Architect:** Security architects develop security strategies and architectures for organizations. They provide guidance on security best practices and ensure that security is integrated into all aspects of the organization's operations.

- **Chief Information Security Officer (CISO):** The CISO is responsible for the overall security of the organization. They develop security policies, manage security risks, and ensure compliance with regulatory requirements.

Distinguishing Ethical Hacking from Malicious Hacking

Feature	Ethical Hacking	Malicious Hacker
Intent	Improve security	Cause Harm or steal data
Authorization	Explicit Permission	No permission
Legality	Legal	Illegal
Disclosure	Reports vulnerabilities to the client	Exploits vulnerabilities for personal gain
Responsibility	Fixes vulnerability with permission	Intends to continue exploiting the system

Exercises

1. Scenario Analysis: Research a publicly disclosed data breach and analyze how an ethical hacker could have prevented it. Identify potential vulnerabilities that could have been exploited and recommend security measures to mitigate those risks.

2. Vulnerability Research: Choose a common software application (e.g., web browser, operating system) and research known vulnerabilities. Use online resources like the National Vulnerability Database (NVD) to find information about the vulnerabilities, their potential impact, and available patches or workarounds.

3. Ethical Hacking Simulation: Imagine you are hired by a small business to conduct a penetration test of their network. Develop a basic plan outlining the phases of the test, the tools you would use, and the types of vulnerabilities you would look for. Consider the specific challenges and constraints of working with a small business.