Network Penetration Testing for beginners

Author: Harshitaa Ashish

CONTENT

Module 1: Introduction to penetration testing
Module 2: Networking Fundamentals
Module 3: Preparing penetration testing
Module 4: Exploitation and post exploitation
Module 5: Reporting and Mitigation
Module 6: Assessment
Module 7: Lab activity
Conclusion
Glossary

Module 1: Introduction to Penetration Testing

Penetration testing, often abbreviated as "pen testing," is a simulated cyberattack on a computer system, network, or application to evaluate its security strength. The purpose of penetration testing is to identify vulnerabilities that malicious attackers could exploit. By simulating real-world attack scenarios, organizations can assess their security posture and take proactive measures to strengthen their defenses.

In the ever-evolving landscape of cybersecurity threats, organizations face a constant challenge in safeguarding their systems and data from malicious actors. Penetration testing emerges as a crucial strategy in the arsenal of defensive measures, offering a proactive approach to identifying and addressing vulnerabilities before they can be exploited. At its core, penetration testing involves simulated cyberattacks on a system, network, or application, conducted by skilled professionals to assess its security posture. By mimicking the tactics of real attackers, penetration testing provides invaluable insights into the effectiveness of existing security controls and helps organizations stay one step ahead in the ongoing battle against cyber threats.

Penetration testing is a proactive cybersecurity measure aimed at identifying vulnerabilities within systems, networks, or applications. By simulating real-world attack scenarios, it assesses the effectiveness of existing security controls, aiding in risk mitigation and incident response preparation. Through systematic probing and ethical exploitation attempts, organizations can prioritize and remediate vulnerabilities before malicious actors exploit them. Penetration testing also helps organizations meet compliance requirements by demonstrating adherence to industry standards. Overall, it plays a crucial role in fortifying cybersecurity defenses, enhancing resilience against evolving cyber threats.

Penetration testing encompasses various types, each tailored to specific objectives and areas of focus. Here are some common types:

- Network Penetration Testing: This type involves assessing the security of network infrastructure, including routers, switches, firewalls, and servers. Testers simulate attacks to identify vulnerabilities such as misconfigurations, weak authentication mechanisms, or outdated software.

- Web Application Penetration Testing: Focused on web applications, this type aims to uncover vulnerabilities in web-based interfaces, APIs, and underlying servers. Testers attempt to exploit flaws like injection attacks, cross-site scripting (XSS), and authentication bypass to assess the application's security posture.

- Wireless Network Penetration Testing: Evaluates the security of wireless networks and devices, including Wi-Fi routers, access points, and connected devices. Testers assess vulnerabilities such as weak encryption protocols, rogue access points, or insecure configurations.

- Social Engineering Testing: Explores human vulnerabilities through manipulation techniques to gain unauthorized access to systems or sensitive information. Testers employ tactics like phishing emails, pretexting, or phone calls to assess employees' security awareness and adherence to policies.

- Physical Penetration Testing: Assesses the physical security measures of facilities, data centers, or offices. Testers attempt unauthorized entry, tampering with equipment, or theft of sensitive information to evaluate the effectiveness of physical security controls.

- Red Team vs. Blue Team Exercises: Red team engagements simulate real-world attacks on a company's infrastructure, while blue team exercises assess the defensive capabilities and incident response procedures of an organization.

Module 2: Networking Fundamentals

OSI Model:

The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and standardize the functions of a telecommunication or computing system. In the late 1970s, the OSI model broke down the communication process into seven distinct layers, each responsible for specific tasks. These layers facilitate communication between different systems by defining standardized protocols and interfaces.

The OSI (Open Systems Interconnection) model consists of seven layers, each responsible for specific tasks in the process of network communication. Here's a brief description of each layer:

- Physical Layer: The lowest layer deals with the physical transmission of data over the network medium. It defines the hardware and electrical specifications, such as cables, connectors, and network interface cards (NICs).
- Data Link Layer: This layer ensures reliable data transmission between adjacent nodes on the network. It handles framing, error detection, and flow control, and it organizes data into frames for transmission over the physical layer.
- Network Layer: Responsible for routing and forwarding data packets between different networks. It addresses and routes data through intermediate devices (routers) to reach its destination using logical addresses (IP addresses).
- Transport Layer: Provides end-to-end communication between source and destination devices. It ensures the reliable delivery of data by handling segmentation, reassembly, flow control, and error recovery. Transmission Control Protocol (TCP) operates at this layer.
- Session Layer: Manages sessions or connections between applications on different devices. It establishes, maintains, and terminates communication sessions, ensuring that data exchange occurs smoothly.
- Presentation Layer: Responsible for data translation, encryption, and compression to ensure that information data sent between applications can be understood by the application layer of another system. It deals with data formatting and conversion.
- Application Layer: The highest layer interacts directly with the end-user applications and provides network services to applications. It supports user processes by providing network functionality such as email, file transfer, and web browsing.

TCP/IP Protocol suite

The TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite is the foundational set of protocols used for communication over the Internet and many other computer networks. It consists of several protocols, each responsible for different aspects of network communication.

- Internet Protocol (IP): This protocol provides the basic addressing and routing mechanism for data packets in the network. It defines how data is broken into packets, addressed, and routed between devices across different networks.
- Transmission Control Protocol (TCP): TCP is a connection-oriented protocol that ensures reliable, ordered, and error-checked delivery of data between devices. It breaks

data into segments, manages the flow of data, and performs error recovery and retransmission if necessary.

- User Datagram Protocol (UDP): UDP is a connectionless protocol that provides a simpler, faster way to send datagrams (packets) without the overhead of establishing a connection. It is often used for applications where speed is more critical than reliability, such as real-time audio/video streaming and online gaming.
- Internet Control Message Protocol (ICMP): ICMP is used for diagnostic and error-reporting purposes in IP networks. It allows devices to communicate error messages, such as unreachable hosts or network congestion, back to the sender.
- Internet Protocol Security (IPsec): IPsec provides security services, including authentication, encryption, and integrity, for IP packets. It is commonly used to secure communication over public networks, such as the Internet, by creating virtual private networks (VPNs).
- Border Gateway Protocol (BGP): BGP is a routing protocol used to exchange routing information between autonomous systems (ASes) on the Internet. It enables routers in different cases to dynamically discover and exchange information about the best routes to reach specific destinations.
- Domain Name System (DNS): Although not part of the TCP/IP suite itself, DNS is a critical protocol used to translate domain names into IP addresses. It enables users to access websites and other resources using human-readable names instead of numerical IP addresses.

Common networking components:

Network Component	Description
Router	Forwards data packets between computer networks. Operates at the network layer, using routing tables.
Switch	Connects devices within a LAN, forwarding data packets based on MAC addresses. Operates at the data link layer.
Hub	Connects multiple devices in a LAN, broadcasting data packets to all connected devices. Operates at the physical layer.
Access Point (AP)	Allows wireless devices to connect to a wired network. Operates at the data link layer, providing WLAN connectivity.
Network Interface Card (NIC)	Hardware components allow devices to connect to a network, providing a physical interface for data transmission.
Modem	Modulates and demodulates digital data, enabling communication over analog channels such as telephone lines.
Firewall	Monitors and controls network traffic based on security rules, protecting against unauthorized access and threats.

Ethernet Cable	Used to connect devices in a wired Ethernet network, transmitting data at high speeds.
Wireless Access Point	Provides wireless connectivity, allowing devices to connect to a wired network via radio frequency signals.
Server	Provides resources, services, or data to other computers over a network, hosting websites, applications, etc.

Network architecture refers to the design and layout of a computer network, including its components, communication protocols, and connectivity methods. It defines how devices are organized and connected to facilitate data transmission and communication within the network. Network architecture can vary widely depending on factors such as the size of the network, its intended use, and the technologies employed. Common network architectures include:

- Client-Server Architecture: In this architecture, client devices (such as computers, smartphones, or tablets) request services or resources from centralized servers. Servers store data, applications, or services and respond to client requests over the network. This architecture is commonly used in enterprise networks, where centralized management and resource allocation are essential.

- Peer-to-Peer (P2P) Architecture: P2P networks enable devices to communicate and share resources directly with each other without the need for centralized servers. Each device acts as both a client and a server, offering resources to other devices while also accessing resources shared by others. P2P architectures are often used for file sharing, collaboration, and distributed computing applications.

- Hierarchical Architecture: This architecture organizes network devices into multiple layers or tiers, with each layer performing specific functions. Typically, access layer devices (such as switches and access points) connect end-user devices to the network, distribution layer devices (such as routers and switches) facilitate communication between different parts of the network, and core layer devices (such as high-speed switches) provide high-speed connectivity between distribution layer devices.

- Mesh Architecture: In a mesh network, devices are interconnected in a decentralized manner, forming multiple paths for data transmission between nodes. This redundancy improves fault tolerance and resilience, as data can be rerouted along alternative paths if one link fails. Mesh architectures are commonly used in wireless networks and in scenarios where reliability and robustness are critical.

Network topology, on the other hand, refers to the physical or logical arrangement of devices and connections in a network. It defines how devices are connected and the structure of the network. Common network topologies include:

- Star Topology: In a star topology, all devices are connected to a central hub or switch, forming a centralized structure. All data transmissions pass through the central hub, which simplifies network management but can create a single point of failure.

- Bus Topology: In a bus topology, all devices are connected to a single communication line or cable, called a bus. Data transmissions travel along the bus, with each device receiving the transmitted data and determining whether it is the intended recipient. Bus topologies are simple and inexpensive but can suffer from network congestion and collisions.

- Ring Topology: In a ring topology, devices are connected in a closed loop or ring configuration, with each device connected to exactly two other devices. Data transmissions circulate around the ring from one device to the next until reaching the intended recipient. Ring topologies offer high reliability and fault tolerance but can be complex to manage.

- Mesh Topology: In a mesh topology, devices are interconnected with multiple redundant paths, forming a highly resilient and fault-tolerant network. Mesh topologies can be full mesh (every device connected to every other device) or partial mesh (only certain devices interconnected). Mesh topologies offer excellent reliability but require significant cabling and configuration.

- Hybrid Topology: A hybrid topology combines two or more basic network topologies to form a more complex structure. For example, a hybrid topology might combine elements of a star topology with elements of a bus or ring topology to create a network that meets specific requirements.

Module 3: Preparing for Penetration Testing

Before launching into penetration testing, thorough reconnaissance and information gathering are essential steps to understand the target environment. This phase involves collecting intelligence about the target's infrastructure, systems, and potential vulnerabilities. Effective reconnaissance lays the groundwork for successful penetration testing by providing insights into the target's attack surface.

Footprinting and Enumeration Techniques

Footprinting entails gathering information about the target's network infrastructure, domain names, IP addresses, and network topology. Techniques include:

- WHOIS Lookup: Extracting domain registration details to identify the organization's owner and contact information.
- DNS Interrogation: Querying domain name system (DNS) servers to map domain names to IP addresses.
- Network Mapping: Utilizing tools like traceroute or Nmap to identify active hosts and network topology.

Enumeration involves extracting additional information about the target's network, services, and users.

- LDAP Enumeration: Querying Lightweight Directory Access Protocol (LDAP) servers to retrieve information about users and groups.
- SNMP Enumeration: Gathering information from Simple Network Management Protocol (SNMP) enabled devices, such as routers and switches.
- SMB Enumeration: Extracting information about shared resources, users, and services from Windows systems using Server Message Block (SMB) protocol.

Tools for Information Gathering

Several specialized tools assist in reconnaissance and information gathering:

- Nmap: A versatile network scanning tool used to discover hosts, open ports, and services running on target systems.
- TheHarvester: A tool for gathering email addresses, subdomains, and other information from public sources.
- Shodan: A search engine that indexes internet-connected devices, providing insights into exposed services and vulnerabilities.
- Maltego: A graphical tool for visualizing and analyzing data gathered from various sources, aiding in reconnaissance and OSINT.

Open Source Intelligence (OSINT) involves collecting information from publicly available sources to build a comprehensive understanding of the target. Sources include:

- Social Media: Extracting information from platforms like LinkedIn, Twitter, and Facebook to identify employees, technologies, or organizational affiliations.
- Websites: Analyzing company websites, blogs, and forums for information about products, services, or recent events.
- Public Databases: Accessing databases such as WHOIS, DNS records, or government registries to gather information about domain names, IP addresses, and organizations.

Once reconnaissance and information gathering are complete, the next phase in preparation for penetration testing involves scanning and enumeration. These activities aim to identify active hosts, open ports, running services, and potential vulnerabilities within the target environment. By systematically scanning and enumerating the network, penetration testers can gain deeper insights into the attack surface and prioritize areas for further investigation.

Port scanning involves probing target systems to identify open ports and services. Various techniques are employed to conduct comprehensive port scans:

- TCP Connect Scan: Establishes a full TCP connection to each port to determine whether it is open, closed, or filtered by a firewall.
- SYN Scan (Half-open Scan): Initiates a TCP connection by sending a SYN packet and analyzes the response to determine the port's status.
- UDP Scan: Sends UDP packets to target ports and analyzes responses to identify open UDP services.
- ACK Scan: Sends ACK packets to target ports and analyzes responses to determine whether the port is filtered or unfiltered.

Service Enumeration

Once open ports are identified, service enumeration involves identifying the specific services running on those ports. Techniques include:

- Banner Grabbing: Analyzing service banners or responses from open ports to determine the software, version, and configuration of running services.
- Service Version Detection: Utilizing tools like Nmap or Netcat to query open ports for service version information.
- Protocol-specific Enumeration: Conducting protocol-specific enumeration techniques tailored to specific services, such as HTTP, FTP, SSH, or SNMP.

Vulnerability Scanning

Vulnerability scanning aims to identify potential weaknesses or security vulnerabilities within the target environment. Techniques include:

- Authenticated Scanning: Conducting scans with valid credentials to assess the security posture of systems from an insider's perspective.
- Unauthenticated Scanning: Scanning target systems without credentials to identify vulnerabilities accessible to external attackers.
- Credentialed Scanning: Utilizing privileged access to gather detailed information about system configurations, patches, and installed software.

Module 4: Exploitation and Post-Exploitation

In the penetration testing process, the phase of exploiting vulnerabilities involves leveraging identified weaknesses within the target environment to gain unauthorized access, escalate privileges, or compromise systems. This phase is crucial for demonstrating the real-world impact of identified vulnerabilities and assessing the effectiveness of existing security controls.

Introduction to Exploitation

Exploitation refers to the process of taking advantage of security vulnerabilities to compromise target systems or networks. Attackers exploit vulnerabilities to achieve various objectives, including gaining unauthorized access, stealing sensitive data, or causing disruption. Exploitation can involve leveraging software bugs, misconfigurations, weak authentication mechanisms, or insecure coding practices.

Common Exploitation Techniques

Several common exploitation techniques are employed by attackers during penetration testing:

- Buffer Overflow: Exploiting programming errors to overwrite memory buffers and execute arbitrary code.
- SQL Injection: Injecting malicious SQL queries into web application input fields to manipulate databases or execute commands.
- Cross-Site Scripting (XSS): Injecting malicious scripts into web pages viewed by other users to steal cookies or perform actions on behalf of the victim.
- Privilege Escalation: Elevating privileges from a lower level of access to a higher level to gain additional permissions or control over systems.
- Brute Force Attacks: Attempting to guess passwords or encryption keys through systematic trial and error.

Exploitation Frameworks

Exploitation frameworks provide penetration testers with a collection of tools, exploits, and payloads to automate and streamline the exploitation process. Popular exploitation frameworks include:

- Metasploit: An open-source framework for developing, testing, and executing exploits against target systems.
- ExploitDB: A repository of exploits and vulnerability information, providing ready-made exploits for various software vulnerabilities.
- Canvas: A commercial exploitation framework offering a comprehensive set of tools and exploits for penetration testing and vulnerability assessment.

Following successful exploitation, attackers often engage in post-exploitation activities to maintain access, escalate privileges further, and exfiltrate sensitive data from compromised systems.

Privilege Escalation

Privilege escalation involves increasing the level of access or permissions beyond what is typically granted to a user. Attackers exploit vulnerabilities or misconfigurations to elevate privileges from standard user accounts to administrator or root-level access. Techniques for privilege escalation include exploiting unpatched vulnerabilities, misconfigured permissions, or weakly protected administrative interfaces.

Maintaining Access

After gaining initial access to a target system, attackers aim to maintain persistent access to ensure continued control over compromised systems. This involves installing backdoors, rootkits, or remote access trojans (RATs) to maintain access even after the initial exploitation vector has been remediated. Attackers may also create additional user accounts, modify system configurations, or exploit scheduled tasks to ensure access persistence.

Data Exfiltration

Data exfiltration involves stealing sensitive information from compromised systems and exfiltrating it to an external location controlled by the attacker. Attackers use various techniques to exfiltrate data, including transferring files over network protocols, encrypting data to evade detection, or hiding data within seemingly innocuous communications. Data exfiltration poses a significant risk to organizations as it can lead to loss of intellectual property, financial damage, or regulatory compliance violations.

Module 5: Reporting and Mitigation

Report Writing

Penetration test reports are essential deliverables that communicate the findings, vulnerabilities, and recommendations discovered during the assessment. Effective report writing is crucial for conveying the results of the penetration test to stakeholders and facilitating informed decision-making regarding security posture improvement.

Structure of Penetration Test Reports

A well-structured penetration test report typically includes the following sections:

1. Executive Summary: Provides a high-level overview of the assessment findings, key vulnerabilities, and recommendations for stakeholders who may not have technical expertise.

2. Scope and Objectives: Defines the scope of the penetration test, including the systems, networks, and applications assessed, as well as the objectives and methodologies used.
3. Methodology: Describes the techniques, tools, and procedures employed during the assessment, including reconnaissance, scanning, exploitation, and post-exploitation activities.
4. Findings and Vulnerabilities: Presents detailed findings of vulnerabilities discovered during the assessment, categorized by severity level and impact.
5. Recommendations: Provides actionable recommendations for remediation, including prioritized steps to address identified vulnerabilities and improve overall security posture.
6. Conclusion: Summarizes the key findings and recommendations of the report, emphasizing the importance of addressing identified vulnerabilities.

Communicating Findings Effectively

Effective communication of findings is essential to ensure that stakeholders understand the implications of identified vulnerabilities and the urgency of remediation efforts. Key considerations for communicating findings include:

- Using clear and concise language understandable to both technical and non-technical audiences.
- Providing evidence and supporting documentation, such as screenshots, logs, and exploit results, to validate findings.
- Tailoring the level of detail and technical depth to the audience's knowledge and expertise.
- Highlighting critical vulnerabilities and their potential impact on business operations, data confidentiality, and regulatory compliance.

Reporting Tools and Templates for Pentesting

Various tools and templates can streamline the report writing process and ensure consistency in reporting. Popular tools and templates include:

- ➔ Microsoft Word or Google Docs: Standard word processing software for creating and formatting penetration test reports.
- ➔ LaTeX: A typesetting system for creating professional-looking reports with advanced formatting and layout options.
- ➔ Report Templates: Pre-defined templates or frameworks tailored to penetration testing, containing sections, headings, and formatting guidelines for creating comprehensive reports efficiently.

Remediation recommendations following a penetration test should prioritize addressing identified vulnerabilities based on severity and potential impact. Each recommendation should provide detailed steps for mitigation, including configuration changes, software updates, and patches. Organizations must allocate resources efficiently to remediate critical vulnerabilities promptly, reducing the risk of exploitation and enhancing overall security posture. Additionally, offering alternative mitigation strategies and compensating controls for vulnerabilities that cannot be immediately addressed ensures a comprehensive approach to risk management.

Prioritizing vulnerabilities involves assessing severity, potential impact, and exploitability to allocate resources effectively. Critical vulnerabilities with high severity and likelihood of exploitation should receive immediate attention to mitigate risks and enhance overall security posture, ensuring optimal allocation of remediation efforts.

Patch management is essential for maintaining a secure and resilient IT environment. Best practices include establishing a formal patch management process, identifying, testing, deploying, and verifying patches. Prioritizing critical patches based on severity, impact, and exploitability ensures timely remediation of high-risk vulnerabilities. Automating patch deployment and monitoring patch compliance streamline the patching process and enhance security posture.

Module 6: Assessment

What is the primary objective of network penetration testing?
a) To identify security vulnerabilities in network infrastructure
b) To monitor the network traffic for suspicious activity
c) To encrypt network communication channels
d) To increase network bandwidth
Answer: a

Which of the following tools is commonly used for network scanning in penetration testing?
a) Metasploit
b) Wireshark
c) Nmap
d) John the Ripper
Answer: c

What is the purpose of vulnerability scanning in network penetration testing?

a) To analyze network traffic patterns
b) To identify and prioritize security vulnerabilities
c) To encrypt sensitive data in transit
d) To authenticate network users
Answer: b

Which network topology connects all devices to a central hub or switch?
a) Star
b) Mesh
c) Bus
d) Ring
Answer: a

What is the term for elevating privileges from a lower level to gain additional permissions in a network?
a) Enumeration
b) Exploitation
c) Privilege Escalation
d) Vulnerability Scanning
Answer: c

Which protocol is commonly exploited in SQL injection attacks?
a) HTTP
b) FTP
c) SNMP
d) SQL
Answer: d

What is the purpose of post-exploitation activities in network penetration testing?
a) To maintain access and control over compromised systems
b) To identify open ports and services on target systems
c) To gather information about network topology
d) To perform vulnerability scanning
Answer: a

Module 7: Lab activity

Lab Activity 1: Network Scanning and Enumeration

Objective:

In this lab activity, participants will learn the fundamentals of network scanning and enumeration, crucial stages in network penetration testing. They will practice using Nmap, a popular network scanning tool, to discover live hosts and open ports on a target network. Through enumeration, they will gather detailed information about the services running on these ports, providing insights into potential vulnerabilities.

Description:

Setup Environment:

- Participants will set up a small network environment consisting of multiple virtual machines or devices.
- This environment will mimic a real-world network, allowing participants to perform scanning and enumeration activities safely.

Network Scanning:

- Participants will use Nmap to conduct a network scan, identifying live hosts and open ports on the target network.
- They will experiment with different scan types and options, such as TCP SYN, UDP, and comprehensive scans, to understand their impact on scan results.

Service Enumeration:

- After identifying open ports, participants will perform service enumeration to gather information about the services running on these ports.
- They will use tools like Nmap scripts or manual techniques to retrieve details such as service versions, banners, and configurations.

Documentation and Analysis:

- Participants will document their findings, including discovered hosts, open ports, and identified services.
- They will analyze the results to identify potential attack vectors and prioritize further exploitation based on the discovered vulnerabilities.

Discussion:

- Facilitators will lead a discussion on the importance of reconnaissance and enumeration in penetration testing.
- Participants will share their experiences and insights gained from the lab activity.

Lab Activity 2: Vulnerability Scanning and Exploitation

Objective:

This lab activity focuses on vulnerability scanning and exploitation, essential stages in identifying and exploiting weaknesses in network systems. Participants will use vulnerability scanning tools to identify known vulnerabilities in a target network and practice exploiting these vulnerabilities using Metasploit or manual techniques.

Description:

Setup Vulnerable Environment:

- Participants will set up a vulnerable virtual machine or deliberately misconfigure a service on one of the machines in the lab environment.
- This will simulate a realistic scenario where systems are vulnerable to exploitation.

Vulnerability Scanning:

- Using tools like Nessus or OpenVAS, participants will scan the target network to identify known vulnerabilities.
- They will analyze the scan results and prioritize vulnerabilities based on severity, potential impact, and exploitability.

Exploitation:

- Participants will select one of the identified vulnerabilities and attempt to exploit it using Metasploit or manual exploitation techniques.
- They will gain access to the vulnerable system and document the steps taken during the exploitation process.

Documentation and Analysis:

- Participants will document their exploitation process, including the vulnerability exploited and the methods used.
- They will analyze the implications of successful exploitation and discuss potential mitigation strategies.

Discussion:

- Facilitators will lead a discussion on the importance of patch management and proactive security measures in preventing exploitation.
- Participants will share their insights and lessons learned from the lab activity.

Conclusion

Network penetration testing is crucial for securing network infrastructure. Through this course, you've learned essential techniques like reconnaissance, scanning, and exploitation. Effective communication of findings and continuous learning are key. Remember, vigilance and ethical hacking principles contribute to creating a safer digital environment.

In this course, we covered:

- The fundamentals of network penetration testing, including reconnaissance, scanning, enumeration, exploitation, and post-exploitation.
- Common tools and methodologies used in each phase of the penetration testing process, such as Nmap, Metasploit, Nessus, and OpenVAS.
- Best practices for identifying, prioritizing, and exploiting vulnerabilities in network systems.
- The importance of documentation, analysis, and communication in conveying findings and recommendations to stakeholders.

Glossary

1. Penetration Testing: Ethical hacking to identify and exploit network vulnerabilities.

2. Reconnaissance: Gathering information about target systems and network infrastructure.
3. Scanning: Automated probing to discover live hosts and open ports.
4. Enumeration: Extracting detailed information about services running on identified ports.
5. Exploitation: Taking advantage of vulnerabilities to gain unauthorized access.
6. Vulnerability: Weakness in a system that can be exploited.
7. Mitigation: Strategies to address and reduce the impact of vulnerabilities.
8. Patch Management: Process of applying software updates to fix vulnerabilities.
9. Privilege Escalation: Elevating user permissions to gain more control.
10. Post-Exploitation: Activities carried out after gaining initial access to maintain control.