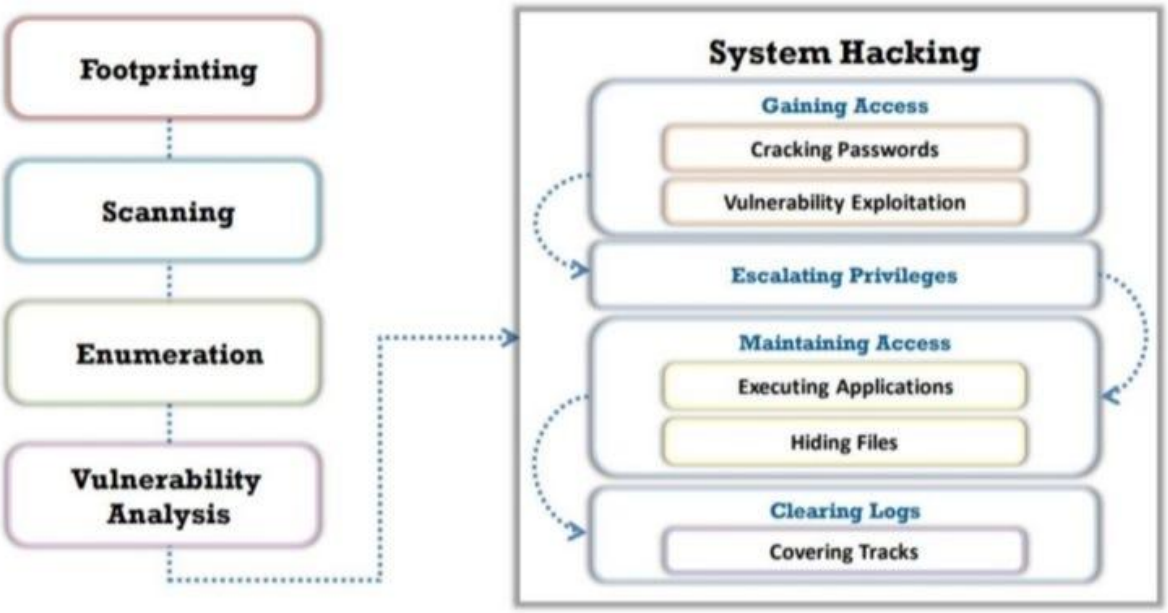
Hacking Methodology



This Shows The Steps Of Hacking to any system.

1. Reconnaissance (Foot printing): This initial phase focuses on gathering information about the target system or network. Attackers might use various techniques, such as public records searches, social engineering, and online mapping tools, to learn about the target's infrastructure, technologies, and security measures.

2. Scanning: After reconnaissance, attackers use scanning tools to identify potential vulnerabilities and weaknesses within the target system or network. This can include port scanning to identify open ports and services, vulnerability scanning to detect known security flaws, and network mapping to understand the system's architecture.

3. Gaining Access: This phase involves exploiting identified vulnerabilities to gain unauthorized access to the target system or network. Techniques may include password cracking, SQL injection, buffer overflows, or exploiting other software vulnerabilities.

4. Maintaining Access: Once access is gained, attackers may seek to maintain persistence and control over the target system. This can involve installing backdoors, rootkits, or other malicious software to establish a foothold and prevent detection.

5. Covering Tracks: Attackers often take steps to conceal their activity and remove evidence of their intrusion, making it harder to detect and attribute the attack. This may involve deleting log files, modifying system configurations, or using encryption.

1. Foot printing :

Foot printing is the first phase of ethical hacking or penetration testing, where information about a target system, organization, or individual is gathered to identify potential vulnerabilities.

Definition:

Foot printing is the process of collecting as much information as possible about a target system or network to identify ways to infiltrate it. It involves both passive and active techniques to gather data such as IP addresses, domain names, employee details, system configurations, and more.

Types of Foot printing:

1. **Passive Foot printing:**
    - Collects information without directly interacting with the target.
    - Example: Searching public websites, social media, WHOIS databases.
2. **Active Foot printing:**
    - Involves direct interaction with the target to gather information.
    - Example: Ping sweeps, traceroutes, and port scanning.

Information Collected During Foot printing:

- Domain names and IP addresses
- Network blocks and services
- Operating systems and software versions
- Security mechanisms (firewalls, IDS)
- Employee contact details
- Website structure and technologies used

2. Scanning :

Scanning is the second phase of ethical hacking, where the attacker actively probes the target system or network to discover live hosts, open ports, services, and vulnerabilities. It involves sending packets and analyzing responses to gather detailed information about the target's infrastructure.

Purpose of Scanning:

- Identify live systems in the network
- Discover open ports and running services
- Detect operating system and service versions
- Find security loopholes and misconfigurations

Types of Scanning:

1. **Port Scanning** – Checks for open ports on a system (e.g., using tools like Nmap)
2. **Network Scanning** – Identifies active devices on the network
3. **Vulnerability Scanning** – Searches for known vulnerabilities in systems and applications

Common Scanning Tools:

- Nmap
- Angry IP Scanner
- Nessus
- OpenVAS

3. Enumeration:

Enumeration is the third phase of ethical hacking, where the attacker extracts more detailed and structured information from the target system or network. It involves making active connections to the system and listing out resources such as usernames, shares, services, and network information.

Purpose of Enumeration:

- Identify valid **usernames and groups**
- Discover **network resources** and **shared folders**
- Detect **running services** and **applications**
- Reveal **configuration settings** and **system details**

Common Enumeration Techniques:

1. **NetBIOS Enumeration** – Gathers information about Windows systems.
2. **SNMP Enumeration** – Uses SNMP protocol to extract system data.
3. **LDAP Enumeration** – Extracts user and directory info from LDAP servers.
4. **SMTP Enumeration** – Identifies valid email users on mail servers.
5. **DNS Enumeration** – Reveals domain records and zone transfers.

Popular Enumeration Tools:

- Nmap (with scripts)
- Netcat
- SNMPWalk
- Enum4linux
- LDAPsearch

4. Vulnerability Analysis :

Vulnerability Analysis is the process of identifying, classifying, and evaluating security weaknesses (vulnerabilities) in a system, network, or application that could be exploited by attackers. It helps organizations understand potential risks and prioritize remediation.

Purpose of Vulnerability Analysis:

- Detect security flaws before attackers do
- Assess the **impact and severity** of vulnerabilities
- Help prioritize **patching and mitigation** efforts
- Strengthen overall **security posture** of systems

Types of Vulnerabilities Identified:

- Software bugs and misconfigurations
- Missing security patches
- Weak passwords and poor authentication
- Exposed services and ports
- Outdated or vulnerable software components

Common Vulnerability Analysis Tools:

- Nessus
- ZAP Proxy
- Police (online)
- OpenVAS
- Nexpose
- Qualys
- Burp Suite (for web apps)

5. System Hacking :

System Hacking is the phase in ethical hacking where the attacker gains access to a target system, maintains that access, and attempts to escalate privileges to take full control over the system. It focuses on exploiting identified vulnerabilities to breach system defenses.

Objectives of System Hacking:

1. **Gain Access** – Exploit vulnerabilities to enter the system.
2. **Escalate Privileges** – Move from limited access to administrative control.
3. **Maintain Access** – Install backdoors or create hidden accounts to return later.
4. **Clear Tracks** – Delete logs and traces to avoid detection.

Steps Involved in System Hacking:

1. Gaining Access

- Using exploits or weak credentials to enter the system.
- Common techniques:
    - Password Cracking (Brute Force, Dictionary, Rainbow Tables)
    - Exploiting software vulnerabilities
    - Keyloggers or phishing

2. Privilege Escalation

- Raising user-level access to admin/root access.
- Done by exploiting:
    - Misconfigured permissions
    - Bugs in OS or applications

    - Stored passwords in plaintext

3. Maintaining Access

- Attackers want persistent control:
    - Backdoors
    - Rootkits
    - Trojans
    - Creating hidden admin users

4. Clearing Tracks

- Covering up their presence:
    - Deleting log files
    - Disabling audit trails
    - Using tools like Timestomp or Logcleaner

Common Tools Used in System Hacking:

- **Metasploit Framework** – For exploiting systems
- **John the Ripper / Hydra** – For password cracking
- **Mimikatz** – For credential dumping on Windows
- **Netcat** – For creating backdoors
- **Cain and Abel** – For cracking and sniffing passwords