# UNIT 2

## Footprinting

1. **What is Footprinting?**
    - Footprinting is the process of collecting as much information as possible about a target system to identify potential vulnerabilities. It is typically the first phase of ethical hacking, used to gather data before launching an attack.
2. **Threats Introduced by Footprinting:**
    - **Privacy violations**: Sensitive data can be exposed, leading to identity theft or unauthorized access.
    - **Network mapping**: Attackers can gather detailed information on your network and systems, aiding them in exploiting weaknesses.
    - **Legal risks**: Invasive footprinting techniques can lead to legal consequences if done without consent.
3. **The Footprinting Process:**
    - **Active Footprinting**: Directly interacting with the target (e.g., pinging a server).
    - **Passive Footprinting**: Gathering information without directly contacting the target (e.g., using public sources like websites).
4. **Using Various Methods for Information Gathering:**
    - **Search Engine Footprinting**: Using search engines like Google to find publicly available data (e.g., documents, IP addresses, URLs, etc.). Example: Google hacking involves using special search operators to find sensitive or hidden data.
    - **Social Networking**: Gathering information from social media platforms like LinkedIn, Facebook, and Twitter to learn about employees, network structures, or user behaviors.
    - **Financial Services**: Financial data and information about a company's structure, transactions, and key employees can sometimes be accessed through websites or public records.

## Scanning

1. **What is Scanning?**
    - Scanning is the process of actively probing a network or system to identify open ports, services, and vulnerabilities. This is a critical part of penetration testing.
2. **Types of Scans:**
    - **Port Scanning**: Identifying open ports on a target system.
    - **Network Scanning**: Mapping the entire network to find live hosts.
    - **Vulnerability Scanning**: Identifying known vulnerabilities in the system by using automated tools.
3. **Family Tree of Scans:**
    - **Active Scans**: Directly interacting with the target, such as ping scans or port scans.
    - **Passive Scans**: Monitoring traffic or using indirect methods, such as looking for exposed services without directly engaging with the target system.
4. **OS Fingerprinting:**
    - OS fingerprinting is the process of determining the operating system of a target system by analyzing network traffic and responses to probes. This helps attackers choose the best method of attack based on the target's OS.
5. **Countermeasures:**
    - **Firewall Configuration**: Setting up firewalls to block unauthorized scans.
    - **Intrusion Detection Systems (IDS)**: Detecting and blocking suspicious scanning activity.
    - **Obfuscation**: Changing or disguising network responses to make fingerprinting harder.
6. **Vulnerability Scanning:**
    - **Automated Tools** like Nessus, OpenVAS, and Qualys are used to scan systems for vulnerabilities, such as outdated software or security flaws.
7. **Using Proxies for Scanning:**
    - Proxies act as intermediaries between the user and the target system, masking the user's identity and making scanning activities harder to trace. They are commonly used in anonymity and evasion techniques.

# Important MCQ

**Footprinting**

1. **What is the primary goal of footprinting?**
    - a) To launch an attack
    - **b) To gather information about a target system**
    - c) To encrypt sensitive data
    - d) To monitor network traffic
2. **Which of the following is an example of passive footprinting?**
    - a) Sending pings to a target system
    - **b) Collecting data from publicly available sources**
    - c) Scanning a network for open ports
    - d) Attempting to brute-force passwords
3. **What does Google hacking refer to?**
    - a) Hacking into Google accounts
    - **b) Using Google search operators to find sensitive data**
    - c) Cracking Google's encryption systems
    - d) Hacking Google servers
4. **Which of the following is a threat introduced by footprinting?**
    - **a) Privacy violations**
    - b) Speed degradation of network
    - c) Unauthorized data encryption
    - d) Increased bandwidth usage
5. **What is an example of a search engine used for footprinting?**
    - a) Yahoo
    - **b) Google**
    - c) Bing
    - d) All of the above

6. **Which of these is NOT a form of social engineering in footprinting?**
    - a) Scanning public social media profiles
    - b) Phishing
    - **c) Directly hacking a network**
    - d) Reviewing company websites for employee information
7. **What type of information can you gather through social networking footprinting?**
    - a) IP addresses
    - **b) Employee names, roles, and company details**
    - c) System vulnerabilities
    - d) DNS configurations
8. **What is considered a public resource for financial services footprinting?**
    - a) Internal network logs
    - **b) Public financial reports and filings**
    - c) Encrypted communications
    - d) Private email addresses
9. **In footprinting, which technique is used to gather information indirectly without directly contacting the target?**
    - a) Active footprinting
    - **b) Passive footprinting**
    - c) Social engineering
    - d) Vulnerability scanning
10. **Which of the following can be considered a legal risk when conducting footprinting?**
    - a) Discovering weak encryption protocols
    - b) Discovering network configuration details
    - **c) Unauthorized access to private data**
    - d) Verifying network uptime

**Scanning**

11. **What is the main goal of scanning in ethical hacking?**
    - a) To attack a system
    - **b) To identify open ports and vulnerabilities**
    - c) To delete files from a system
    - d) To encrypt network traffic
12. **Which type of scan is used to discover live hosts in a network?**
    - a) OS fingerprinting
    - **b) Network scanning**
    - c) Vulnerability scanning
    - d) Social engineering
13. **What is port scanning used for?**
    - a) To determine the operating system of a target
    - **b) To identify open ports on a system**
    - c) To check for malware
    - d) To track internet usage
14. **Which of these is a type of active scan?**
    - a) Packet sniffing
    - **b) Ping scan**
    - c) DNS lookup
    - d) WHOIS query
15. **What is OS fingerprinting?**
    - **a) Determining the operating system of a target**
    - b) Identifying the IP address of a target
    - c) Scanning for open ports
    - d) Detecting malware on a system
16. **Which of these is a countermeasure to prevent scanning?**
    - a) Open-source intelligence gathering
    - **b) Configuring firewalls to block unauthorized scans**
    - c) Using weak encryption
    - d) Installing proxies for external access

17. **Which tool is commonly used for vulnerability scanning?**
    - a) Nmap
    - **b) Nessus**
    - c) Burp Suite
    - d) Wireshark
18. **What is the main purpose of vulnerability scanning?**
    - a) To collect information on a target system
    - **b) To identify security weaknesses in a system**
    - c) To bypass firewalls
    - d) To scan encrypted communications
19. **Which scanning technique can be used to determine the operating system of a target machine?**
    - **a) OS fingerprinting**
    - b) Ping scan
    - c) Port scanning
    - d) Network scanning
20. **Which type of scan is passive and does not interact with the target system?**
    - a) Port scanning
    - b) OS fingerprinting
    - **c) DNS lookup**
    - d) Ping sweep

---

**Proxies and Advanced Techniques**

21. **What is the main function of a proxy in network scanning?**
    - a) To scan the target system’s vulnerabilities
    - **b) To mask the attacker's IP address**
    - c) To protect against malware attacks
    - d) To monitor network traffic

22. **Which of these is an example of a vulnerability scanning tool?**
    - a) Wireshark
    - b) Metasploit
    - **c) OpenVAS**
    - d) Nmap
23. **Which type of scan helps detect weaknesses like outdated software or missing patches?**
    - a) Port scan
    - **b) Vulnerability scan**
    - c) OS fingerprinting
    - d) Ping sweep
24. **What can be identified by network scanning?**
    - a) Open ports and running services
    - **b) Vulnerabilities in services**
    - c) OS details
    - d) All of the above
25. **What type of scan is typically used to identify specific services running on a system?**
    - a) OS fingerprinting
    - b) Network scanning
    - **c) Port scanning**
    - d) Ping scanning
26. **Which tool is commonly used for OS fingerprinting?**
    - a) Nessus
    - b) **Nmap**
    - c) Burp Suite
    - d) Snort
27. **What does a DNS lookup scan reveal?**
    - **a) Domain name information and associated IP addresses**
    - b) Vulnerabilities in a system
    - c) Open ports on a system
    - d) The operating system of a target

28. **What is the main risk of using proxies during scanning?**
    - a) Proxy servers may introduce lag
    - **b) Proxies may log and reveal your identity**
    - c) Proxies cannot be used for network scanning
    - d) Proxies may interfere with the firewall
29. **Which of the following methods can be used to mitigate the risk of scanning?**
    - **a) Installing firewalls**
    - b) Increasing bandwidth usage
    - c) Disabling proxy servers
    - d) Monitoring DNS queries
30. **Which of the following tools is used to mask your IP address during a scan?**
    - a) Nmap
    - **b) Proxy server**
    - c) Nessus
    - d) Wireshark