Section 1.

Footprinting is the process of identifying and understanding the security risks present in an organization. Like reconnaissance, it involves gathering as much information about the target as possible, including information that may not be readily available online. This information can then be used to build a profile of the organization's security posture and identify potential vulnerabilities.

There are two main types of footprinting: passive and active.

- Passive footprinting: Gathering information from publicly available sources such as websites, news articles, and company profiles
- Active footprinting: Using more intrusive methods to access sensitive data, such as hacking into systems or applying social engineering techniques

The type of footprinting approach you use will depend on what information you want to collect and how much access you have to the target. For example, if you're going to collect information about an organization's network infrastructure, you may need to use active footprinting methods such as port scanning and vulnerability assessment. However, passive footprinting will suffice if you want to gather publicly available information, such as the names of employees and their contact details.

Reconnaissance is the information-gathering stage of ethical hacking, where you collect data about the target system. This data can include anything from network infrastructure to employee contact details. The goal of reconnaissance is to identify as many potential attack vectors as possible.

Data collected from reconnaissance may include:

- **Security policies**. Knowing an organization's security policies can help you find weaknesses in their system.
- **Network infrastructure**. A hacker needs to know what type of network the target is using (e.g., LAN, WAN, MAN), as well as the IP address range and subnet mask.
- **Employee contact details**. Email addresses, phone numbers, and social media accounts can be used to launch social engineering attacks.
- **Host information**. Information about specific hosts, such as operating system type and version, can be used to find vulnerabilities.

Steps in Footprinting

Several steps need to be followed during footprinting to collect all relevant information.

1. Identifying Targets
The first step is to identify which systems or organizations to footprint by scanning networks for open ports or performing reconnaissance using Google searches and tools like Shodan.

2. Gathering Information
After the target has been identified, the next step is to gather as much information about it as possible using tools like Nmap, Netcat, and Whois to identify open ports and services, usernames and passwords, web server information, and more.

3. Analyzing Results

After all relevant data has been collected, it needs to be analyzed to determine the most vulnerable points. This is done by identifying common weaknesses across multiple systems or comparing results against known exploits.

4. Planning Attacks

The final step is to use the information gathered during footprinting to plan a successful attack against the target’s systems, networks, and devices. This may involve developing custom exploits or choosing a suitable attack vector based on the data collected.

Section 2:

Vulnerability scanning is the process of identifying security weaknesses and flaws in systems and software running on them. It's part of a vulnerability management program that protects organizations from data breaches.

IT departments or third-party security service providers scan for vulnerabilities using vulnerability scanning tools. Doing so helps predict how effective countermeasures are in case of a threat or attack.

In this article we'll define vulnerability scanning, the six step process for how it works, why it's important in your cyber strategy, common vulnerabilities detected, best practices and top tools.

Security scanning vs. vulnerability scanning

Vulnerability scanning is a specific type that focuses on identifying security flaws and vulnerabilities in systems and software. But security scanning is a broader term encompassing vulnerability and other types of scans, such as:

- Port scanning
- Network mapping
- Web application scanning

Vulnerability and security scanning are components of a comprehensive security strategy and can help organizations identify and address potential security risks before attackers can exploit them.

How vulnerability scanning works

Vulnerability scanning is an ongoing process, and regular scanning helps organizations stay ahead of emerging threats and new vulnerabilities. Here is a step-by-step explanation of how it works:

1. **Creates an asset inventory**: The vulnerability scanner identifies and creates an inventory of all systems connected to a network. It identifies each device's operating system, software, open ports, and user accounts.
2. **Scans the attack surface**: Next, the scanner scans the networks, hardware, software, and systems to identify potential risk exposures and attack vectors.

3. **Compares with vulnerability databases**: The vulnerability scanner checks for known flaws, like CVEs, and potential paths to sensitive data on the target attack surface.
4. **Detects and classifies**: The scanner detects and classifies system weaknesses, identifying vulnerabilities attackers could exploit.
5. **Reports**: The scanner then creates reports on vulnerabilities and how to fix them to help organizations prioritize their efforts.
6. **Acts to remediate**: Based on the vulnerability scan reports, organizations can take action to address the identified vulnerabilities. This can involve applying patches, updating software, reconfiguring systems, or implementing other security measures.

Common vulnerabilities detected by scanning

Vulnerabilities vary depending on the scanning tool used and the configuration of the scanning process. And by doing so, you can detect:

- **Misconfigured systems** that may have default or weak settings, which attackers can exploit.
- **Outdated software** with known vulnerabilities should be updated with the latest patches and security fixes.
- **Weak passwords** that attackers use to gain unauthorized access to systems or accounts.
- **Missing patches** that are vulnerable to known exploits.
- **Open ports and services** that may be potential entry points for attackers.
- **Insecure configurations** in systems that may expose sensitive data or allow unauthorized access.
- **Default credentials** enabled devices that help attackers to carry out exploitations.
- **Systems that use insecure network protocols** like outdated versions of SSL/TLS.

Best practices for vulnerability scanning

Here are some best practices for vulnerability scanning:

- **Establish a framework** that covers the six steps of the process, documents it, and uses it to execute the vulnerability scanning process.
- **Consistent scanning** helps identify and address potential security flaws before they can be exploited.

- **Scan every device** that connects your ecosystem, including systems behind firewalls within secure internal networks.
- **Assign owners to critical assets** to help ensure vulnerabilities are identified and addressed promptly.
- **Prioritize the patching process** based on the severity of the vulnerabilities identified.
- **Document all results** to ensure that vulnerabilities are tracked and addressed in a timely manner.
- **Use multiple tools**, such as at least two scanners with different approaches, to get cross-vendor results and better coverage.
- **Use instrumentation tools** to provide the most accurate and actionable results and lessen the triage burden on security teams.
- **Identify your different attack vectors** to find a suitable scanner for your business.

Top vulnerability scanning tools in cybersecurity

Vulnerability scanning tools help improve your organization's security posture by providing automated scanning capabilities, detailed reporting, and integration with other security tools. They save time and effort for security teams.

Selecting the right tool depends on the specific requirements, budget, and complexity of the organization's infrastructure. So here are a few top vulnerability scanning tools in cybersecurity to help you out:

- **Nessus** is a versatile vulnerability scanner with an extensive database and frequent updates.
- **OpenVAS** is a flexible and cost-effective open-source vulnerability scanner that offers tests for common security issues.
- **Burp Suite** is a web application security testing tool that identifies common vulnerabilities and offers interactive scanning and features like proxying and session analysis.

Section 3:

Introduction of Firewall in Computer Network

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic. **Accept :** allow the traffic **Reject :** block the traffic but reply with an “unreachable error” **Drop :** block the traffic with no reply A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

Types of Firewall

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Advantages of using Firewall

1. **Protection from unauthorized access:** Firewalls can be set up to restrict incoming traffic from particular IP addresses or networks, preventing hackers or other malicious actors from easily accessing a network or system. Protection from unwanted access.
2. **Prevention of malware and other threats:** Malware and other threat prevention: Firewalls can be set up to block traffic linked to known malware or other security concerns, assisting in the defense against these kinds of attacks.
3. **Control of network access:** By limiting access to specified individuals or groups for particular servers or applications, firewalls can be used to restrict access to particular network resources or services.
4. **Monitoring of network activity:** Firewalls can be set up to record and keep track of all network activity. This information is essential for identifying and looking into security problems and other kinds of shady behavior.
5. **Regulation compliance:** Many industries are bound by rules that demand the usage of firewalls or other security measures.

Organizations can comply with these rules and prevent any fines or penalties by using a firewall.

6. **Network segmentation:** By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.

Honeypot

Honeypot is a network-attached system used as **a trap for cyber-attackers** to detect and study the tricks and types of attacks used by hackers. It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system. Honeypots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of attacks used by attackers. It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information.

Cryptography

Cryptography in computer network security is the process of protecting sensitive information from unauthorized access when it is at rest or in transit by rendering it unreadable without a key. Leveraging encryption, cryptography helps users secure data transmission over networks, ensuring that only individuals with designated keys can access encrypted data.