**Define what network scanning is as a method of penetration testing.**

Network scanning is a technique used in penetration testing to identify open ports, active hosts, and other network infrastructure details. It involves systematically scanning a target network for vulnerabilities an attacker could exploit.

Network scanning tools can perform various types of scans, including port scans, operating system detection, service discovery, and vulnerability scans. These scans can be either passive, where the scanning tool listens for responses from the network, or active, where the tool sends packets to the web to elicit a response.

The goal of network scanning in penetration testing is to identify potential vulnerabilities in the target network that attackers could exploit. This information can then be used to strengthen the network's security posture and mitigate any potential risks.

**Explain how network scanning works and why cybercriminals use it**

**Include statistics on web application testing as a form of penetration testing**.

Network scanning identifies active hosts, open ports, and other network infrastructure details. It works by sending packets to a network and analyzing the responses to determine the state of various network resources. There are different types of network scanning techniques, including:

1. Ping Scanning: This technique detects active hosts on a network. It sends an Internet Control Message Protocol (ICMP) echo request to a range of IP addresses and waits for a response. If a response is received, the host is considered active.
2. Port Scanning: This technique detects open ports on a network. It sends packets to a range of ports on a host to determine which ones are open and accepting connections.
3. Service Scanning: This technique detects services running on a network. It sends packets to a host to determine which services are running and what versions they are.
4. Cybercriminals use network scanning for reconnaissance purposes. By reviewing a network, attackers can gather information about the network's infrastructure, including the operating systems, software versions, and potential vulnerabilities. This information can be used to launch targeted attacks against the network, such as exploiting a known vulnerability in a specific software version or gaining unauthorized access to a system.
5. Cybercriminals may also use network scanning to identify potential targets for attack. For example, they may scan for open ports or poorly secured wireless networks for remote access. Once a target has been identified, the attacker can launch a more targeted attack to gain access to the network and steal data or cause damage.
6. Network scanning is a valuable tool for penetration testers and cyber criminals. It helps identify vulnerabilities and potential attack vectors and enables attackers to gather reconnaissance on a target network for their attack.

**What is the most commonly used tool for web scanning?**

Several web scanning tools are available in the market, each with features and capabilities. The choice of a web scanning tool often depends on the project's specific requirements, such as the application's size, the application, the complexity of the application, and the level of testing required.

However, some of the most popular and widely used web scanning tools are:

1. Burp Suite: Burp Suite is a comprehensive web application testing tool with features like a proxy server, scanner, and intruder. It is widely used by penetration testers, security researchers, and web developers.
2. OWASP ZAP: OWASP ZAP (Zed Attack Proxy) is a free, open-source web application security testing tool. It is easy to use and provides a range of features, including a proxy server, scanner, and spider.
3. Acunetix: Acunetix is a commercial web application testing tool with a scanner, vulnerability assessment, and management capabilities. It is widely used by security professionals, compliance auditors, and web developers.
4. Nessus: Nessus is a vulnerability scanner that can scan web applications and identify vulnerabilities. It includes various features, including a web application scanner, compliance checking, and remediation guidance.
5. Nikto: Nikto is a free, open-source web application scanner that checks for common vulnerabilities and misconfigurations. It is easy to use and provides a range of output formats.

Choosing a web scanning tool depends on the project's specific requirements, and each device has strengths and weaknesses.

**Discuss what BurpSuite is and how it is used, Or discuss another web application tool used in pen testing. You can explain how it is used within and outside of AWS.**

**Technical documentation - steps that clearly show how to download, install and use a web application testing tool.**

Burp Suite is a popular web application security testing tool widely used by security professionals, web developers, and penetration testers. It includes a range of features, including a proxy server, scanner, intruder, and repeater, which can be used to identify and exploit vulnerabilities in web applications.

Burp Suite can intercept and modify HTTP/HTTPS traffic between the client and server, allowing users to analyze and adjust requests and responses. The scanner feature can automatically identify vulnerabilities in web applications, such as SQL injection, cross-site scripting, and file inclusion vulnerabilities. The intruder feature can automate attacks against web applications, such as brute force attacks and parameter manipulation.

Burp Suite can be installed on Windows, Linux, and macOS outside of AWS. To download and install Burp Suite, follow these steps:

1. Go to the PortSwigger website and download the appropriate installer for your operating system.
2. Install Burp Suite by following the on-screen instructions.
3. Once installed, open Burp Suite and configure your browser to use Burp Suite as a proxy server. This can be done by setting the proxy server settings in your browser to utilize the IP address and port number of the Burp Suite proxy.
4. Browse to the web application you want to test, and Burp Suite will intercept the traffic.
5. Use the various features of Burp Suite, such as the scanner, intruder, and repeater, to test the web application's security.
6. Within AWS, several web application security testing tools can be used to test web applications deployed on AWS infrastructure. Some of these tools include:
7. Amazon Inspector: Amazon Inspector is an automated security assessment service that can test the security of EC2 instances and applications running on them. It includes pre-built rules packages that can be used to test for common vulnerabilities, such as missing patches, open ports, and weak passwords.
8. AWS Security Hub: AWS Security Hub is a security management service that provides a comprehensive view of security alerts and compliance status across AWS accounts. It integrates with various third-party security tools, including web application scanners, to provide a centralized view of security posture.
9. AWS WAF: AWS WAF is a web application firewall that can protect web applications from common attacks, such as SQL injection and cross-site scripting. It includes pre-built rules and can be customized to fit the specific requirements of the web application.
10. To use these tools within AWS, follow the documentation AWS provides for each device. Typically, these tools are available through the AWS Management Console and can be configured and managed from there.