**Sample MCQ**

**CEH**

1. **Identify a tool that can be used for passive OS fingerprinting?**
2. **Nmap**

**nmap is a network scanning tool that is commonly used for active OS fingerprinting by sending probes and analyzing responses from target systems to determine their operating systems. While nmap is a powerful tool for network reconnaissance, it is not typically used for passive OS fingerprinting.**

1. **Tracert**

**tracert is a network diagnostic tool used to trace the route that packets take from one networked device to another. It is not typically used for passive OS fingerprinting as it does not analyze network traffic to determine the operating system of a target system.**

1. **Ping**

**ping is a network utility used to test the reachability of a host on an IP network. It sends ICMP echo request packets to the target host and waits for an ICMP echo reply. Ping is not suitable for passive OS fingerprinting as it does not analyze network traffic to determine the operating system of a target system.**

1. **Tcpdump**

**tcpdump is a packet analyzer that captures and analyzes network traffic. It can be used for passive OS fingerprinting by capturing packets and analyzing the characteristics of the network traffic to determine the operating system of the target system without actively sending probes or packets.**

**https://www.geeksforgeeks.org/linux-unix/tcpdump-command-in-linux-with-examples/**

1. **Ahmed, a pentester, has been assigned to perform an internal audit for the company. One of his tasks is to identify open ports on servers. Which of the following methods is the most effective solution for this task?**
   1. **Telnet to every port on each server**

**Telnetting to every port on each server manually is a time-consuming and inefficient method for identifying open ports. It requires manual effort to connect to each port individually, which can be impractical and may not provide comprehensive results compared to automated scanning tools like Nmap.**

* 1. **Scan servers with Nmap**

**Nmap is a powerful network scanning tool commonly used by pentesters to identify open ports, services running on those ports, and other network information. It provides detailed information about the servers' network configuration and is considered one of the most effective solutions for identifying open ports during an internal audit.**

**nmap 192.168.1.1-20**

**nmap 192.168.1.0/24 (CIDR notation)**

**This scans all 256 addresses in the subnet 192.168.1.0 to 192.168.1.255**

**Specify port range while scanning IP range**

**nmap -p 20-100 192.168.1.1-20**

**This checks ports 20 through 100 on all IPs from 192.168.1.1 to 192.168.1.20.**

* 1. **Scan servers with MBSA**

**MBSA (Microsoft Baseline Security Analyzer) is primarily used for scanning Windows-based systems for security vulnerabilities and misconfigurations.**

* 1. **Manual scan on each server**

**Performing a manual scan on each server is a labor-intensive and error-prone process, especially when dealing with a large number of servers. Manual scanning may lead to overlooking open ports or misconfigurations, making it less effective and reliable compared to automated scanning tools like Nmap.**

1. **Which of the following is an attack where an attacker intercepts the communication between a client and server, negotiates cryptographic parameters to decrypt the encrypted content, and obtains confidential information such as system passwords?**
   1. **Chosen-ciphertext attack**

**A Chosen-ciphertext attack is a type of cryptanalysis where the attacker can choose a piece of ciphertext and obtain the corresponding plaintext.**

* 1. **Rubber hose attack**

**A Rubber hose attack is a physical attack where an individual is physically coerced or threatened to reveal sensitive information, such as system passwords.**

* 1. **Man-in-the-middle attack**

**A Man-in-the-middle attack is when an attacker intercepts the communication between a client and server, allowing them to eavesdrop on the encrypted content, negotiate cryptographic parameters, and obtain confidential information such as system passwords. This type of attack is a common method used to steal sensitive information during data transmission.**

* 1. **Chosen-key attack**

**A Chosen-key attack is a type of cryptanalysis where the attacker can choose a key and obtain the corresponding plaintext.**

1. **You've been tasked with setting up remote work for employees. However, their remote connections could be vulnerable to session hijacking, and you want to prevent this risk. You decide to implement a technology that establishes a secure and encrypted tunnel over a public network to safely transmit sensitive data, preventing hackers from intercepting or decrypting the information. Which technology would you choose?**
   1. **Bastion host**

**A Bastion host is a highly secured server that acts as a gateway between the internal network and an external network, such as the internet.**

* 1. **DMZ**

**DMZ (Demilitarized Zone) is a network segment that sits between the internal network and an external network, such as the internet.**

* 1. **Split tunnelling**

**Split tunneling is a technique that allows remote users to access both the company's network and the internet simultaneously, by splitting the traffic between the two.**

* 1. **VPN**

**VPN (Virtual Private Network) establishes a secure and encrypted tunnel over a public network, such as the internet, to securely transmit data. By using a VPN, remote employees can access the company's network and resources securely, preventing session hijacking and eavesdropping by encrypting the data transmitted over the network.**

1. **Identify a low-tech way of gaining unauthorized access to information?**
   1. **Sniffing**

**Sniffing is a technical method that involves intercepting and capturing network traffic to obtain sensitive information such as passwords or data.**

* 1. **Scanning**

**Scanning is a technical method that involves actively probing a network or system for vulnerabilities and open ports.**

* 1. **Eavesdropping**

**Eavesdropping is a low-tech method that involves listening in on conversations or communications to gather sensitive information. .**

* 1. **Social engineering**

**Social engineering is a low-tech method that involves manipulating individuals into divulging confidential information or performing actions that compromise security. It relies on human interaction and psychological manipulation rather than technical exploits to gain unauthorized access to information.**

1. Scammers can probe the DNS server to see if a particular DNS record is stored in the cache, allowing them to track your organization’s browsing patterns. This could expose sensitive information like recently visited financial websites or other private sites that a company would prefer to keep confidential.Which attack type matches this scenario?
   1. **DNS cache snooping**

**DNS cache snooping is the correct attack type for this scenario. It involves probing the DNS server to see if a specific DNS record is stored in the cache, which can expose sensitive information about an organization's browsing patterns and visited websites. This attack allows attackers to track and monitor the DNS cache to gather information that should be kept confidential.**

* 1. **DNSSEC zone walking**

**DNSSEC zone walking is a technique used to extract information from a DNSSEC-protected zone by following the chain of trust. It does not directly involve probing the DNS server to track an organization's browsing patterns or expose sensitive information stored in the cache.**

* 1. **DNS zone walking**

**DNS zone walking is a technique used to enumerate all the resource records in a DNS zone by following the links between the records. It does not specifically involve probing the DNS server to track an organization's browsing patterns or expose sensitive information stored in the cache.**

* 1. **DNS cache poisoning**

**This attack involves corrupting the DNS cache with false information to redirect users to malicious websites. It does not specifically involve probing the DNS server to track an organization's browsing patterns or expose sensitive information.**

1. **Which of the following components of public key infrastructure acts as a verifier for the certificate authority?**
   1. **Authentication authority**

This is not a standard PKI component. However, it might be referred to in some contexts but is not typically part of the standard PKI architecture.

* 1. **Registration authority**

The RA acts as an intermediary between the user and the CA. It verifies the user's identity before requesting a digital certificate from the CA.

It does not verify the certificate's validity; that's the VA's job

* 1. **Certificate management system**

This system is used to **manage the lifecycle** of certificates (issuance, renewal, revocation) but does not validate certificates.

It assists in managing certificates rather than verifying their status.

* 1. **Validation authority**

**The Validation Authority (VA) in a Public Key Infrastructure (PKI) acts as the verifier for the Certificate Authority (CA). It is responsible for validating whether a digital certificate issued by a CA is still valid and whether the certificate chain is trusted. The VA checks for certificate revocation using methods like CRLs (Certificate Revocation Lists) or OCSP (Online Certificate Status Protocol).**

1. **Which one of the following Google search operators allows restricting results to those from a specific website?**
   1. **[link:]**

**The [link:] operator in Google search is used to find pages that link to a specific URL.**

* 1. **[cache:]**

**The [cache:] operator in Google search is used to view a cached version of a webpage.**

* 1. **[site:]**

**The [site:] operator in Google search allows users to restrict search results to a specific website or domain. By using [site:], you can filter search results to only show pages from the specified website, making it a useful tool for targeted searches.**

* 1. **[inurl:]**

**The [inurl:] operator in Google search is used to search for specific keywords within the URL of a webpage.**

1. **The attacker shared a message and an image on the forum, containing a hidden malicious link. When the victim clicks the link, their browser automatically sends an authenticated request to a server. What kind of attack is this?**
   1. **Cross-site scripting**
   2. **SQL injection**
   3. **Cross-site request forgery**
   4. **Session hijacking**
2. Lewis, an attacker, performed sniffing on a target organization’s network and found that one of the protocols used by the target organization is vulnerable as it allows a client to access and manipulate the emails on a server. Lewis exploited that protocol to obtain the data and employee credentials that are transmitted in cleartext.

Which of the following protocols was exploited by Lewis in the above scenario?

* 1. **IMAP**

**IMAP** (Internet Message Access Protocol) is a protocol used by email clients to retrieve and manipulate messages stored on a mail server. If **IMAP** is not properly secured (i.e., using **IMAP over SSL/TLS**), the communication between the client and the server could occur in **cleartext**, making it vulnerable to **sniffing** and data interception.

In the scenario, Lewis performed sniffing and exploited a protocol to access emails and credentials transmitted in **cleartext**. **IMAP** (if not encrypted) is vulnerable to this type of attack.

* 1. **HTTPS**
  2. **DTLS**
  3. **IPsec**