**Sample MCQ**

**CEH**

1. **Identify a tool that can be used for passive OS fingerprinting?**
2. **Nmap**
3. **Tracert**
4. **Ping**
5. **Tcpdump**
6. **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**
   2. **Scan servers with Nmap**
   3. **Scan servers with MBSA**
   4. **Manual scan on each server**
7. **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**
   2. **Rubber hose attack**
   3. **Man-in-the-middle attack**
   4. **Chosen-key attack**
8. **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**
   2. **DMZ**
   3. **Split tunnelling**
   4. **VPN**
9. **Identify a low-tech way of gaining unauthorized access to information?**
   1. **Sniffing**
   2. **Scanning**
   3. **Eavesdropping**
   4. **Social engineering**
10. 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**
    2. **DNSSEC zone walking**
    3. **DNS zone walking**
    4. **DNS cache poisoning**
11. **Which of the following components of public key infrastructure acts as a verifier for the certificate authority?**
    1. **Authentication authority**
    2. **Registration authority**
    3. **Certificate management system**
    4. **Validation authority**
12. **Which one of the following Google search operators allows restricting results to those from a specific website?**
    1. **[link:]**
    2. **[cache:]**
    3. **[site:]**
    4. **[inurl:]**
13. **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**
14. 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**
  2. **HTTPS**
  3. **DTLS**
  4. **IPsec**