Certified Ethical Hacker v12 Exam

1. Topic #: 1
Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server.

A. Which of the following tools is used by Jack to perform vulnerability scanning?

Answer(s): C

---

2. Question #: 219
Topic #: 1
You have been hired as an intern at a start-up company. Your first task is to help set up a basic web server for the company's new website. The team leader has asked you to make sure the server is secure from common threats. Based on your knowledge from studying for the CEH exam, which of the following actions should be your priority to secure the web server?

A. A. Limiting the number of concurrent connections to the server

B. B. Installing a web application firewall

C. C. Regularly updating and patching the server software

D. D. Encrypting the company's website with SSL/TLS

Answer(s): D

---

3. Question #: 159
Topic #: 1
A certified ethical hacker is conducting a Whois footprinting activity on a specific domain. The individual is leveraging various tools such as Batch IP Converter and Whois Analyzer Pro to retrieve vital details but is unable to gather complete Whois information from the registrar for a particular set of data. As the hacker, what might be the probable data model being utilized by the domain's registrar for storing and looking up Whois information?

A. A. Thin Whois model working correctly

B. B. Thin Whois model with a malfunctioning server

C. C. Thick Whois model with a malfunctioning server

D. D. Thick Whois model working correctly

Answer(s): A

---

4. Question #: 144
Topic #: 1
You are a cybersecurity consultant for a major airport that offers free Wi-Fi to travelers. The management is concerned about the possibility of “Evil Twin” attacks, where a malicious actor sets up a rogue access point that mimics the legitimate one. They are looking for a solution that would not significantly impact the user experience or require travelers to install additional software. What is the most effective security measure you could recommend that fits these constraints, considering the airport’s unique operational environment?

A. A. Regularly change the SSID of the airport’s Wi-Fi network

B. B. Use MAC address filtering on the airport’s Wi-Fi network

C. C. Implement WPA3 encryption for the airport’s Wi-Fi network

D. D. Display a captive portal page that warns users about the possibility of Evil Twin attacks

Answer(s): D

---

5. Question #: 35
Topic #: 1
Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.bank.com, the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different.
What type of attack he is experiencing?

A. A. DHCP spoofing

B. B. DoS attack

C. C. ARP cache poisoning

D. D. DNS hijacking

Answer(s): D

---

6. Question #: 180
Topic #: 1
During a reconnaissance mission, an ethical hacker uses Maltego, a popular footprinting tool, to collect information about a target organization. The information includes the target's Internet infrastructure details (domains, DNS names, Netblocks, IP address information). The hacker decides to use social engineering techniques to gain further information. Which of the following would be the least likely method of social engineering to yield beneficial information based on the data collected?

A. A. Dumpster diving in the target company's trash bins for valuable printouts

B. B. Impersonating an ISP technical support agent to trick the target into providing further network details

C. C. Shoulder surfing to observe sensitive credentials input on the target's computers

D. D. Eavesdropping on internal corporate conversations to understand key topics

Answer(s): A

---

7. Question #: 18
Topic #: 1
Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process, Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.
What is the attack performed by Robin in the above scenario?

A. A. ARP spoofing attack

B. B. STP attack

C. C. DNS poisoning attack

D. D. VLAN hopping attack

Answer(s): B

---

8. Question #: 120
Topic #: 1
Which of the following protocols can be used to secure an LDAP service against anonymous queries?

A. A. NTLM

B. B. RADIUS

C. C. WPA

D. D. SSO

Answer(s): A

---

9. Question #: 17
Topic #: 1
Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection.
What is the APT lifecycle phase that Harry is currently executing?

A. A. Initial intrusion

B. B. Persistence

C. C. Cleanup

D. D. Preparation

Answer(s): A

---

10. Question #: 278
Topic #: 1
Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

A. A. Union SQL injection

B. B. Error-based injection

C. C. Blind SQL injection

D. D. Boolean-based blind SQL injection

Answer(s): A

---

11. Question #: 30
Topic #: 1
Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials.
Which of the following tools is employed by Clark to create the spoofed email?

A. A. Evilginx

B. B. Slowloris

C. C. PLCinject

D. D. PyLoris

Answer(s): A

---

12. Question #: 92
Topic #: 1
Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks.
What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

A. A. Allow the transmission of all types of addressed packets at the ISP level

B. B. Disable TCP SYN cookie protection

C. C. Allow the usage of functions such as gets and strcpy

D. D. Implement cognitive radios in the physical layer

Answer(s): D

---

13. Question #: 283
Topic #: 1
An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption. The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages.

A. What is the attack performed in the above scenario?

Answer(s): C

---

14. Question #: 297
Topic #: 1
Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request.

A. Which of the following techniques is employed by Dayn to detect honeypots?

Answer(s): C

---

15. Question #: 260
Topic #: 1
John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the IoT devices connected in the target network that are using default credentials and are vulnerable to various hijacking attacks. For this purpose, he used an automated tool to scan the target network for specific types of IoT devices and detect whether they are using the default, factory-set credentials.

A. What is the tool employed by John in the above scenario?

Answer(s): C

---

16. Question #: 54
Topic #: 1
Jude, a pen tester, examined a network from a hacker’s perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network.
What is the type of vulnerability assessment that Jude performed on the organization?

A. A. Application assessment

B. B. External assessment

C. C. Passive assessment

D. D. Host-based assessment

Answer(s): B

---

17. Question #: 290
Topic #: 1
In an attempt to damage the reputation of a competitor organization, Hailey, a professional hacker, gathers a list of employee and client email addresses and other related information by

using various search engines, social networking sites, and web spidering tools. In this process, she also uses an automated tool to gather a list of words from the target website to further perform a brute-force attack on the previously gathered email addresses.

A. What is the tool used by Hailey for gathering a list of words from the target website?

Answer(s): A

---

18. Question #: 307
Topic #: 1
Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the information, he successfully performed an attack on the target government organization without being traced.

A. Which of the following techniques is described in the above scenario?

Answer(s): B

---

19. Question #: 69
Topic #: 1
Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.
Identify the behavior of the adversary in the above scenario.

A. A. Unspecified proxy activities

B. B. Use of command-line interface

C. C. Data staging

D. D. Use of DNS tunneling

Answer(s): A

---

20. Question #: 106
Topic #: 1
Attacker Simon targeted the communication network of an organization and disabled the security

controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic. He then extracted all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks.
What is the type of attack performed by Simon?

A. A. Combinator attack

B. B. Dictionary attack

C. C. Rainbow table attack

D. D. Internal monologue attack

Answer(s): D
