Certified Ethical Hacker (CEH) v12

1. By using a smart card and pin, you are using a two-factor authentication that satisfies

A. Something you are and something you remember

B. Something you have and something you know

C. Something you know and something you are

D. Something you have and something you are

Answer(s): B

---

2. "_____is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on thepremises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up afraudulent web site and luring people there." Fill in the blank with appropriate choice.

A. Evil Twin Attack

B. Sinkhole Attack

C. Collision Attack

D. Signal Jamming Attack

Answer(s): A

---

3. A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising

only a single server. Based on this information, what should be one of your key recommendations to the bank?

A. Place a front-end web server in a demilitarized zone that only handles external web traffic

B. Require all employees to change their anti-virus program with a new one

C. Move the financial data to another server on the same IP subnet

D. Issue new certificates to the web servers from the root certificate authority

Answer(s): A

---

4. What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Residual risk

B. Impact risk

C. Deferred risk

D. Inherent risk

Answer(s): A

---

5. Which of the following is the best countermeasure to encrypting ransomwares?

A. Use multiple antivirus softwares

B. Pay a ransom

C. Keep some generation of off-line backup

D. Analyze the ransomware to get decryption key of encrypted data

Answer(s): C

6. Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?

A. tcpsplice

B. Burp

C. Hydra

D. Whisker

Answer(s): D

---

7. You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best Nmap command you will use?

A. nmap -T4 -q 10.10.0.0/24

B. nmap -T4 -F 10.10.0.0/24

C. nmap -T4 -r 10.10.1.0/24

D. nmap -T4 -O 10.10.0.0/24

Answer(s): B

---

8. As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization’s interest and your liabilities as a tester?

A. Service Level Agreement

B. Project Scope

C. Rules of Engagement

D. Non-Disclosure Agreement

Answer(s): C

---

9. Which of the following is the BEST way to defend against network sniffing?

A. Using encryption protocols to secure network communications

B. Register all machines MAC Address in a Centralized Database

C. Use Static IP Address

D. Restrict Physical Access to Server Rooms hosting Critical Servers

Answer(s): A

---

10. Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

A. Iris patterns

B. Voice

C. Height and Weight

D. Fingerprints

Answer(s): C

---

11. Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?

A. SFTP

B. Ipsec

C. SSL

D. FTPS

Answer(s): B

---

12. To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bankweb site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?

A. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit

B. if (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit

C. if (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit

D. if (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit

Answer(s): A

---

13. Jim’s company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim’s company keeps the backup tapes in a safe in the office. Jim’s company is audited each year, and the results from this year’s audit show a risk because backup tapes are not stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

A. Encrypt the backup tapes and transport them in a lock box.

B. Degauss the backup tapes and transport them in a lock box.

C. Hash the backup tapes and transport them in a lock box.

D. Encrypt the backup tapes and use a courier to transport them.

Answer(s): A

---

14. You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.
What may be the problem?

A. Traffic is Blocked on UDP Port 53

B. Traffic is Blocked on TCP Port 80

C. Traffic is Blocked on TCP Port 54

D. Traffic is Blocked on UDP Port 80

Answer(s): A

---

15. Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a Linux platform?

A. Kismet

B. Abel

C. Netstumbler

D. Nessus

Answer(s): A

---

16. You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.
While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.
After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.
What kind of attack does the above scenario depict?

A. Botnet Attack

B. Spear Phishing Attack

C. Advanced Persistent Threats

D. Rootkit Attack

Answer(s): A

---

17. Scenario:
1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make$1000 in a day?'.
3. Victim clicks to the interesting and attractive content URL.
4. Attacker creates a transparent 'iframe' in front of the URL which the victim attempts to click, so the victim thinks that he/she clicks on the 'Do you want to make $1000 in a day?' URL but actually he/she clicks on the content or URL that exists in the transparent 'iframe' which is setup by the attacker.
What is the name of the attack which is mentioned in the scenario?

A. Session Fixation

B. HTML Injection

C. HTTP Parameter Pollution

D. Clickjacking Attack

Answer(s): D

---

18. A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named “nc.” The FTP server’s access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server’s software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?

A. File system permissions

B. Privilege escalation

C. Directory traversal

D. Brute force login

Answer(s): A

---

19. Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in bounds checking mechanism?
Code:
#include intmain(){_____char buffer[8];
strcpy(buffer, ““1111111111111111111111111111””);} Output: Segmentation fault

A. C#

B. Python

C. Java

D. C++

Answer(s): D

---

20. Internet Protocol Security IPsec is actually a suite pf protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.

A. Protect the payload and the headers

B. Encrypt

C. Work at the Data Link Layer

D. Authenticate

Answer(s): C
