SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 21

Your results are here!! for" CEHv11 Practice Test 21 "

0 of 40 questions answered correctly

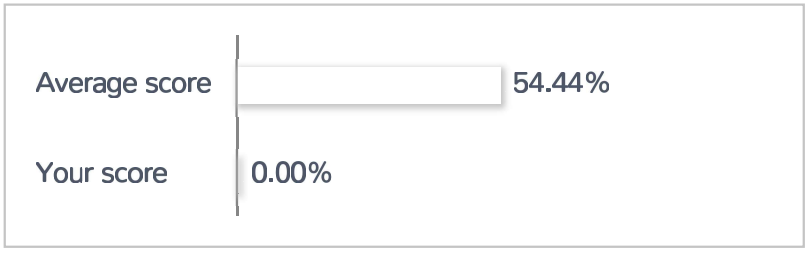
Your time: 00:00:02

Your Final Score is : 0

You have attempted : 0

Number of Correct Questions : 0 and scored 0

Number of Incorrect Questions : 0 and Negative marks 0



You can review your answers by clicking view questions.

Important Note : Open Reference Documentation Links in New Tab (Right Click and Open in New Tab).

Restart Test | View Answers

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34

35 36 37 38 39 40

Correct Incorrect

Review Question Summary

1. Question

This Nmap command allows hackers to scan fewer ports.

- -sP
- -r
- **-P**
- -F

Unattempted

-P command line switch is used for scanning fewer ports other than the default scanning using the Nmap tool. For example, nmap -p 80 192.168.1.1 will scan port 80.

2. Question

This Nmap command is used for detecting the operating system used by the targeted machine?

- -r
- -F
- **-O**
- -sP

Unattempted

-O is a command-line switch used for OS detection in Nmap.

For example, nmap -O 192.168.1.1.

3. Question

This type of hacker doesn't have enough knowledge or skills to perform hacking.

- Hacktivist
- Ethical Hacker
- Suicide Hacker
- **Script Kiddies**

Unattempted

Script kiddies are hackers who are new to hacking and don't have much knowledge or skills to perform hacks. Instead, they use tools and scripts developed by more experienced hackers.

4. Question

How is sniffing broadly categorized?

- Unmanaged and managed
- **Active and passive**
- Broadcast and unicast
- Filtered and unfiltered

Unattempted

There are two types of sniffing: Passive Sniffing and Active Sniffing.

5. Question

XOR is a common cryptographical tool. What will be the result if you apply XOR in the following binary values: 11001100, 01101010?

- **10100110**
- 1011001
- 11001100
- 1101010

Unattempted

XOR (eXclusive OR) is a boolean logic operation that is widely used in cryptography. It is used in generating parity bits for error checking and fault tolerance. The output is True (or 1) if and only if the two inputs are

different. The output is false (or 0) if the two inputs have the same value.

6. Question

Which of the following is being described when two pieces of data resulted in the same hash value?

- **Collision**
- Polymorphism
- Escrow
- Collusion

Unattempted

A collision attack is an attempt to find two input strings of a hash function that produce the same hash result.

7. Question

This is greatly affected by Smurf attacks on the Internet?

- Mail servers
- SPAM filters
- **IRC servers**
- IDS devices

Unattempted

In a Smurf attack, a large amount of ICMP echo request (ping) traffic is sent to an IP broadcast address, with a spoofed source IP address of the intended victim. IRC servers are commonly used to prolong thus making them the primary victim of this attack.

8. Question

Penetration testers and cybersecurity analysts use this tool to easily connect data and functionalities from diverse sources using Transforms.

- **Maltego**
- Wireshark

- Cain & Abel
- Metasploit

Unattempted

Maltego is an open-source intelligence and forensics software application developed by Paterva. It is a comprehensive tool for graphical link analysis that offers real-time data mining and information gathering which can be presented in a graph format.

9. Question

Which of the following command is used to launch the Computer Management Console from the command line?

- c:\services.msc
- c:\ncpa.cpl
- **c:\compmgmt.msc**
- c:\gpedit

Unattempted

To open the Computer Management Console from the command line just type compmgmt.msc in your run box or at the command line.

10. Question

This type of malicious software aims to restrict the user from using the system rather than to steal confidential information.

- Trojan
- Logic Bomb
- Botnet
- **Ransomware**

Unattempted

Ransomware is a form of malware that restricts the user from accessing their infected computer system or files and then asks for a ransom payment to regain user access. The main goal of a ransomware attack is to extort money from its victims.

11. Question

This attack is used by cybercriminals to crack passwords by using a precomputed table of hashed passwords.

- Dictionary Attack
- Hybrid Attack
- **Rainbow Table Attack**
- Brute Force Attack

Unattempted

A rainbow table attack is a hacking method that involves the use of a rainbow hash table. This table contains the values used to encrypt the passwords before adding them to the database.

12. Question

A Certified Ethical Hacker aspirant wants to explore HTTP methods such as GET, POST, HEAD, PUT, DELETE, and TRACE. Which of the following Nmap script should he use?

- **HTTP-methods**
- HTTP-all
- HTTP-headers
- HTTP-num

Unattempted

HTTP-methods returns all the available methods on the server.

13. Question

Which of the following is/are an example of Active sniffing?

- Hub-based networks
- **DHCP attacks**
- **Mac flooding**
- **DNS poisoning**

Unattempted

Active sniffing involves sending out multiple network probes to identify access points. The following are examples of different active sniffing techniques: ⁎ MAC flooding ⁎ DNS poisoning ⁎ ARP poisoning ⁎ DHCP attacks ⁎ Switch port stealing ⁎ Spoofing attack

14. Question

Public keys are shared during the process of encryption and decryption. (True or False)

- FALSE
- **TRUE**

Unattempted

In an asymmetric key system, public keys are shared or available to anyone, while private keys are held only by the key owner.

15. Question

This is commonly used in performing a security audit on various forms of network systems?

- Port scanning
- Intrusion Detection System
- **Vulnerability scanning**
- Protocol analyzer

Unattempted

Vulnerability scanning is a method used in checking whether a system is exploitable or not by identifying its vulnerabilities.

16. Question

Which type of access control is used on a router or firewall to limit network activity?

- **Rule-based**
- Role-based

- Mandatory
- Discretionary

Unattempted

With rule-based access control, when a request is made for access to a network or network resource, the controlling device, e.g. firewall, checks properties of the request against a set of rules. A rule might be to block an IP address or a range of IP addresses.

17. Question

An ethical hacker was hired to perform penetration testing and security assessments for a small company in the local area. While conducting a routine security assessment, the ethical hacker discovered that the client is involved in fraudulent activities. What should the ethical hacker do?

- Copy the data to removable media and keep it in case you need it.
- Ignore the data and continue the assessment until completed as agreed
- **Immediately stop work and contact the proper legal authorities.**
- Respectfully confront the client and ask her about the data.

Unattempted

You must report your client immediately if they are involved in any illegal activities.

18. Question

Operating System (OS) Fingerprinting helps a cracker because:

- It defines exactly what software you have installed
- **It informs the cracker of which vulnerabilities he may be able to exploit on your system**
- It doesn't depend on the patches that have been applied to fix existing security holes
- It opens a security-delayed window based on the port being scanned

Unattempted

OS fingerprinting is the process a hacker goes through to determine the type of operating system being used on a targeted computer. This is beneficial because it gives the hacker useful information about any security vulnerabilities of the operating system that can be exploited to launch an attack.

19. Question

Which of the following best describes the polymorphic shellcode?

- Polymorphic shellcode converts the shellcode into Unicode.
- Polymorphic shellcode compresses the shellcode into normal instructions, uncompressed the shellcode using loader code, and then executes the shellcode.
- Polymorphic shellcode reverses the order of working instructions by masking the IDS signatures.
- **Polymorphic shellcode changes by using the XOR process to encrypt and decrypt the shellcode.**

Unattempted

Polymorphic shellcode encrypts the shellcode by XORing values over the shellcode, using loader code to decrypt the shellcode, and then executing the decrypted shellcode.

20. Question

Joshua has been working as a network security administrator on a large electric company for more than 15 years. Unfortunately, due to the ongoing pandemic, his company is downsizing and he is one of those who will be laid off in a few weeks. Joshua felt betrayed and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. He doesn't care if this will land him in jail. Joshua can be tagged as?

- Black Hat Hacker
- Hacktivist Hacker
- **Suicide Hacker**
- White Hat Hacker

Unattempted

Suicide hackers are those who hack for some purpose and even don't bother to suffer long-term jail due to their activities.

21. Question

A type of penetration testing where the internal operation of a system is completely known to the tester.

- Gray box testing

- White box testing
- Black box testing
- Red box testing

Unattempted

A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application. A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.

22. Question

Which of the following asymmetry cipher is based on factoring the product of two large prime numbers?

- SHA
- MD5
- RSA
- RC5

Unattempted

RSA is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

23. Question

This is a non-profit organization dedicated to providing unbiased, practical, and cost-effective information about application security

- PCIDSS
- HIPAA
- OWASP
- GDPR

Unattempted

Open Web Application Security Project or OWASP is a non-profit organization dedicated to providing unbiased, practical, and cost-effective information about application security. OWASP's Top 10 Security Vulnerabilities provides a ranking of the top ten most prevalent security vulnerabilities which also serves as a guideline for developers and security professionals.

24. Question

Jane, a network engineer from SIA Global Security, is conducting an internal security audit. What is the best way for her to find all the open ports on all of the servers?

- **Scan servers with Nmap**
- Telnet to every port on each server
- Scan servers with MBSA
- Physically go to each server

Unattempted

Nmap or network mapper is a powerful reconnaissance tool. It is a free, open-source Linux command-line tool that can be used to gather lots of information about the target. This program can be used in finding active hosts on a network, perform port scanning, ping sweeps, and, OS and version detection.

25. Question

This is a type of malware that replicates, executes, and spreads across network connections without the help of human interaction.

- **Worms**
- Virus
- Trojan

Unattempted

A worm is a type of malware that replicates, executes, and spreads across network connections, but unlike a computer virus, it does not need the help of human interaction. It is designed to consume all available computing resources causing network, web, and individual computer systems to become overloaded and stop responding.

26. Question

A Linux administrator was hired by XYZ company to investigate the recent incidents on their Linux server that is occurring during non-business hours. During the investigation, the Linux admin realizes that the time on the Linux server was not synchronized. What protocol has stopped working on Linux servers which affected the synchronization of time?

- Network Time Protocol
- Time Keeper
- Point-to-Point Protocol
- Operating System Protection Protocol

Unattempted

Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network.

27. Question

Spacefiller virus is most commonly known as:

- Cavity virus
- Tunneling virus
- Stealth virus
- Polymorphic virus

Unattempted

Cavity virus known as spacefiller virus is a rare type of computer virus that installs itself by filling in empty sections of a file. By only using empty sections of a file, the virus can infect a file without the size of the file changing, making it more difficult to detect.

28. Question

Which of the following is a symmetric cryptographic standard?

- 3DES
- DSA
- RSA
- PKI

Unattempted

In cryptography, Triple DES (3DES or TDES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block.

29. Question

What is the result of the following command:

```
nmap -sS -O -p 150 to 160 192.168.111.107
```

- Stealth scan, checking all open ports excluding ports 150 to 160
- **Stealth scan, determine operating system, and scanning ports 150 to 160.**
- Stealth scan, opening port 150 and 160
- Stealth scan, checking open ports 150 to 160

Unattempted

-sS = Stealth scanning

-O = Operating System (OS) checking

-p = Scan fewer ports

-p 150 to 160 = Scanning ports 150 to 160

30. Question

It is a regulation that requires businesses to ensure the protection of personal data and privacy of European citizens.

- Digital Millennium Copyright Act (DMCA)
- **General Data Protection Regulation (GDPR)**
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)

Unattempted

General Data Protection Regulation or GDPR is a regulation that requires businesses to ensure the protection of personal data and privacy of European citizens. It establishes one law across the continent and a single set

of rules which applies to companies doing business within EU member states.

31. Question

DHCP snooping is an excellent solution in preventing rogue DHCP servers on your network. Which of the following security feature on switches leverages the DHCP snooping database to help mitigate man-in-the-middle attacks?

- A Layer 2 Attack Prevention Protocol (LAPP)
- Port security
- Spanning tree
- **Dynamic ARP inspection (DAI)**

Unattempted

Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors.

32. Question

In order to keep the access and maintain undetected for a longer time, the ethical hacker must remain invisible to the host system to avoid getting caught. The ethical hacker is in which phase of ethical hacking?

- Covering Tracks
- Gaining Access
- **Maintaining Access**
- Scanning and Enumeration

Unattempted

The fourth phase of ethical hacking is maintaining access. In this phase, the hacker will secure his or her access to the system to maintain it for a longer time for future exploitation and additional attack purposes. To keep the access and maintain undetected for a longer time, the hacker must remain invisible to the host system to avoid getting caught.

33. Question

Which of the following is known as a detective control?

- Audit trail
- Security policy
- Continuity of operations plan
- Smart card authentication

Unattempted

An audit trail is a step-by-step record by which accounting or trade data can be traced to its source.

34. Question

Which of the following is/are examples of Worms?

- Morris
- Code Red
- WannaCry
- Stuxnet

Unattempted

Worms are designed to consume all available computing resources causing network, web, and individual computer systems to become overloaded and stop responding. Some popular examples are Stuxnet, Morris worm, and Code red worm.

35. Question

This type of hacker uses their skills to promote political or social agenda.

- Hacktivist
- Ethical Hacker
- Suicide Hacker
- Script Kiddies

Unattempted

Hacktivists break into government agencies or big corporate systems out of protest. They use their skills to promote a political or social agenda.

36. Question

A security audit of network systems must be performed to determine compliance with security policies. Which of the following tools would most likely be used in such an audit?

- **Vulnerability scanner**
- Port scanner
- Protocol analyzer
- Intrusion Detection System

Unattempted

Vulnerability scanning is a method used to check whether a system is exploitable by identifying its vulnerabilities. A vulnerability scanner consists of a scanning engine and a catalog. These tools generally target vulnerabilities that secure host configurations can fix easily, updated security patches, and a clean Web document.

37. Question

Which of the following describes the Connection Stream Parameter Pollution (CSPP) attack?

- Addition of multiple parameters with the same name in HTTP requests.
- Insertion of malicious Javascript code into input parameters.
- Setting the user's SID to an explicit known value.
- **Injection of parameters into a connection string using semicolons as a separator.**

Unattempted

The so-called Connection String Parameter Pollution (CSPP) attack exploits poorly secured dynamic connections between Web apps and databases, namely ones that still use semicolons as separators between data such as the data source, user ID, and password associated with a connection to the database, for instance.

38. Question

XYZ company recently discovered that their new product was released by one of their competitor before their release date. They hired an investigator to know how this happened. The investigator discovered that the maid threw away papers with confidential information about the new product and it is possible that their competitor found it in the garbage. Which technique is being described in this scenario?

- Hack attack
- Spying
- **Dumpster diving**
- Sniffing

Unattempted

Dumpster diving (or searching for useful information through a potential victim's garbage dump). This is an often-used method of social engineering. In the corporate world, a lot of valuable data, such as employees' names, phone numbers, organizational charts, as well as user credentials and passwords written in notes, can be found in the company's trash.

39. Question

Which of the following keys are shared during the process of encryption and decryption?

- Public and private keys
- Private keys
- **Public keys**
- User passwords

Unattempted

In an asymmetric key system, public keys are shared or available to anyone, while private keys are held only by the key owner.

40. Question

This device enables the capture of all traffic when using a Wireshark to acquire packet capture on a network?

- Application firewall
- Layer 3 switch

Network tap

Network bridge

Unattempted

Network TAPs are a purpose-built hardware device that sits in a network segment, between two appliances (router, switch or firewall), and allows you to access and monitor the network traffic.

Click Below to go to Master Cheat Sheet

Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

← Previous Post

Next Post →

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy