SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 10

Your results are here!! for" CEHv11 Practice Test 10 "

0 of 65 questions answered correctly

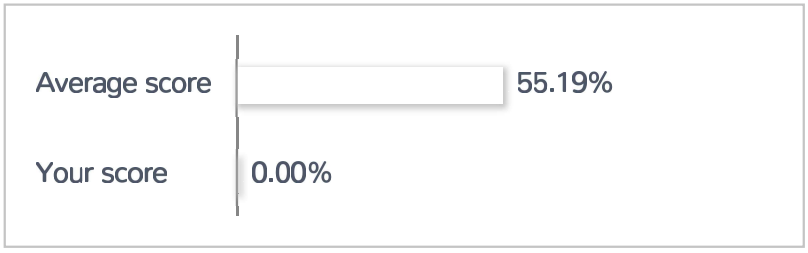
Your time: 00:00:01

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 41 42 43 44 45 46 47 48 49 50 51
52 53 54 55 56 57 58 59 60 61 62 63 64 65

Correct Incorrect

Review Question Summary

1. Question

Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He is determined that the application is vulnerable to SQL injection and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?

- Error-based SQL injection
- **Blind SQL injection**
- NoSQL injection
- Union-based SQL injection

Unattempted

2. Question

What is the purpose of DNS AAAA record?

- Authorization, Authentication and Auditing record
- Address database record
- **IPv6 address resolution record**
- Address prefix record

Unattempted

3. Question

Which system consists of a publicly available set of databases that contain domain name registration contact information?

- IANA
- CAPTCHA
- **WHOIS**
- IETF

Unattempted

4. Question

Which of the following is not a Bluetooth attack?

- Bluesnarfing
- **Bluedriving**
- Bluejacking
- Bluesmacking

Unattempted

5. Question

Which of the following is assured by the use of a hash?

- **Integrity**
- Availability
- Confidentially
- Authentication

Unattempted

6. Question

>NMAP “”sn 192.168.11.200-215 The NMAP command above performs which of the following?

- An operating system detect

- A port scan
- A trace sweep
- **A ping scan**

Unattempted

7. Question

Risks=Threats x Vulnerabilities is referred to as the:

- Threat assessment
- BIA equation
- **Risk equation**
- Disaster recovery formula

Unattempted

8. Question

Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message. The technique provides "Ëœsecurity through obscurity'. What technique is Ricardo using?

- **Steganography**
- Encryption
- RSA algorithm
- Public-key cryptography

Unattempted

9. Question

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

- Voice
- Fingerprints
- Iris patterns
- **Height and Weight**

Unattempted

10. Question

Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: -Verifies success or failure of an attack "" Monitors system activities "" Detects attacks that a network-based IDS fails to detect. "" Near real-time detection and response "" Does not require additional hardware "" Lower entry cost. Which type of IDS is best suited for Tremp's requirements?

- **Host-based IDS**
- Network-based IDS
- Open source-based IDS
- Gateway-based IDS

Unattempted

11. Question

The "Gray-box testing" methodology enforces what kind of restriction?

- Only the external operation of a system is accessible to the tester.
- The internal operation of a system is completely known to the tester.
- Only the internal operation of a system is known to the tester.
- **The internal operation of a system is only partly accessible to the tester.**

Unattempted

12. Question

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?

- True positive
- **False positive**
- True negative
- False negative

Unattempted

13. Question

Which command can be used to show the current TCP/IP connections?

- Net use
- **Netstat**
- Netsh
- Net use connection

Unattempted

14. Question

You have successfully gained access to your client's internal network and successfully comprised a Linux server which is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled. Which port would you see listening on these Windows machines in the network?

- **445**
- 3389
- 161
- 1433

Unattempted

15. Question

Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occuring during non-business hours. After further examination of all login activities, it is notices that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realized the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux serves to synchronize the time has stopped working?

- PPP
- OSPF
- **NTP**
- TimeKeeper

Unattempted

16. Question

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

- Jack the ripper
- Nessus
- **Tcpdump**
- Ethereal

Unattempted

17. Question

Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?

- **Network-based intrusion detection system (NIDS)**
- Honeypots
- Firewalls
- Host-based intrusion detection system (HIDS)

Unattempted

18. Question

Which of these is capable of searching for and locating rogue access points?

- HIDS
- NIDS
- **WIPS**
- WISS

Unattempted

19. Question

Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?

- **Userland Exploit**
- Sandbox Exploit
- iBoot Exploit
- Bootrom Exploit

Unattempted

20. Question

You are analyzing a traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs. “” 192.168.8.0/24. What command you would use?

- **wireshark ""capture ""local ""masked 192.168.8.0 ""range 24**
- tshark ""net 192.255.255.255 mask 192.168.8.0
- wireshark ""fetch "192.168.8/*"
- sudo tshark ""f "net 192.168.8.0/24"

Unattempted

21. Question

Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

- **Accept the risk**
- Avoid the risk
- Mitigate the risk
- Introduce more controls to bring risk to 0%

Unattempted

22. Question

A common cryptographical tool is the use of XOR. XOR the following binary values: 10110001 00111010

- 11011000
- **10001011**
- 10111100
- 10011101

Unattempted

23. Question

What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

- **Meet-in-the-middle attack**
- Man-in-the-middle attack

- Replay attack
- Traffic analysis attack

Unattempted

24. Question

Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

- **Nikto**
- Snort
- John the Ripper
- Dsniff

Unattempted

25. Question

Which protocol is used for setting up secure channels between two devices, typically in VPNs?

- SET
- PEM
- **IPSEC**
- PPP

Unattempted

26. Question

Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP). Which of the following is an incorrect definition or characteristics of the protocol?

- **Only compatible with the application protocol HTTP**
- Provides a structured model for messaging

- Based on XML
- Exchanges data between web services

Unattempted

27. Question

The change of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?

- $100
- $1,320
- **$146**
- $440

Unattempted

28. Question

Which of these options is the most secure procedure for storing backup tapes?

- In a cool dry environment
- **In a climate controlled facility offsite**
- On a different floor in the same building
- Inside the data center for faster retrieval in a fireproof safe

Unattempted

29. Question

When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

- At least once every three years or after any significant upgrade or modification
- At least once every two years and after any significant upgrade or modification
- At least twice a year or after any significant upgrade or modification
- **At least once a year and after any significant upgrade or modification**

Unattempted

30. Question

WPA2 uses AES for wireless data encryption at which of the following encryption levels?

- 128 bi and TKIP
- 128 bit and CRC
- **128 bit and CCMP**
- 64 bit and CCMP

Unattempted

31. Question

Your company was hired by a small healthcare provider to perform a technician assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?

- Use the built-in Windows Update tool
- Check MITRE.org for the latest list of CVE findings
- **Use a scan tool like Nessus**
- Create a disk image of a clean Windows installation

Unattempted

32. Question

From the following table, identify the wrong answer in terms of Range (ft).

Standard	Range (ft)
802.11a	150-150
802.11b	150-150
802.11g	150-150
802.16(WiMax)	30 miles

- 802.11g
- **802.11a**
- 802.11b
- 802.16(WiMax)

Unattempted

33. Question

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes. Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

- Black Hat
- White Hat
- **Gray Hat**
- Suicide Hacker

Unattempted

34. Question

You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

- ICMP
- **TCP**
- UPD

UPX

Unattempted

35. Question

Why containers are less secure than virtual machines?

A compromise container may cause a CPU starvation of the host.

Containers are attached to the same virtual network.

Host OS on containers has a larger surface attack.

Containers may fulfill disk space of the host.

Unattempted

36. Question

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, smallsized 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?

Hydra

tcpsplice

Whisker

Burp

Unattempted

37. Question

You are monitoring the network of your organizations. You notice that: 1. There are huge outbound connections from your Internal Network to External IPs 2. On further investigation, you see that the external IPs are blacklisted 3. Some connections are accepted, and some are dropped 4. You find that it is a CnC communication Which of the following solution will you suggest?

Clean the Malware which are trying to Communicate with the External Blacklist IP's

- **Block the Blacklist IP's @ Firewall as well as Clean the Malware which are trying to Communicate with the External Blacklist IP's.**
- Block the Blacklist IP's @ Firewall
- Update the Latest Signatures on your IDS/IPS

Unattempted

38. Question

While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: nmap “”Pn “”p “”sl kiosk.adobe.com http://www.riaa.com kiosk.adobe.com is the host with incremental IP ID sequence. What is the purpose of using “-sl” with Nmap?

- Conduct ICMP scan
- Conduct silent scan
- Conduct stealth scan
- **Conduct IDLE scan**

Unattempted

39. Question

What is the process of logging, recording, and resolving events that take place in an organization?

- Security Policy
- Internal Procedure
- **Incident Management Process**
- Metrics

Unattempted

40. Question

During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is

inspecting outbound traffic?

- Application
- Stateful
- Circuit
- Packet Filtering

Unattempted

41. Question

A pen-tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

- Winprom
- Winpsw
- Libpcap
- Winpcap

Unattempted

42. Question

Which of the following statements regarding ethical hacking is incorrect?

- Testing should be remotely performed offsite.
- Ethical hacking should not involve writing to or modifying the target systems.
- An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services
- Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems

Unattempted

43. Question

You are doing an internal security audit and intend to find out what ports are open on all the servers. What is the best way to find out?

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

Unattempted

44. Question

Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned. Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

- "GET/restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.com"
- **"GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com"**
- "GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"
- "GET/restricted/bank.getaccount("ËœNed') HTTP/1.1 Host: westbank.com"

Unattempted

45. Question

What is a “Collision attack” in cryptography?

- **Collision attacks try to find two inputs producing the same hash**
- Collision attacks try to get the public key
- Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key
- Collision attacks try to break the hash into three parts to get the plaintext value

Unattempted

46. Question

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

- Broadcast ping
- TCP ping
- **Hping**
- Traceroute

Unattempted

47. Question

Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

- SHA-0
- SHA-3
- SHA-2
- **SHA-1**

Unattempted

48. Question

DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

- Layer 2 Attack Prevention Protocol (LAPP)
- **Dynamic ARP Inspection (DAI)**
- Port security

Spanning tree

Unattempted

49. Question

Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

STARTTLS

OPPORTUNISTICTLS

UPGRADETLS

FORCETLS

Unattempted

50. Question

You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration? alert tcp any any -> 192.168.100.0/24 21 (msg:""FTP on the network!"";)

An Intrusion Detection System

FTP Server rule

A Router IPTable

A firewall IPTable

Unattempted

51. Question

Which of the following is a component of a risk assessment?

Logical interface

- Administrative safeguards
- DMZ
- Physical security

Unattempted

52. Question

What would you enter, if you wanted to perform a stealth scan using Nmap?

- nmap -sU
- nmap -sM
- nmap -sT
- nmap -sS

Unattempted

53. Question

During the security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

- Create a procedures document
- Terminate the audit
- Conduct compliance testing
- Identify and evaluate existing practices

Unattempted

54. Question

User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

- **Presentation**
- Transport
- Application
- Session

Unattempted

55. Question

Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server? The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

- Stacheldraht
- **R-U-Dead-Yet? (RUDY)**
- MyDoom
- LOIC

Unattempted

56. Question

When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?

- http enum
- **http-methods**
- http-git
- http-headers

Unattempted

57. Question

What is the minimum number of network connections in a multihomed firewall?

- 5
- 3
- 4
- **2**

Unattempted

58. Question

You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

- SET
- **CHNTPW**
- John the Ripper
- Cain & Abel

Unattempted

59. Question

Analyst is investigating proxy logs and found out that one of the internal user visited website storing suspicious java scripts. After opening one of them, he noticed that it is very hard to understand the code and that all codes differ from the typical java script. What is the name of this technique to hide the code and extend analysis time?

- Encryption
- **Obfuscation**
- Steganography

Code encoding

Unattempted

60. Question

The “white box testing” methodology enforces what kind of restriction?

The internal operation of a system is completely known to the tester.

Only the external operation of a system is accessible to the tester.

The internal operation of a system is only partly accessible to the tester.

Only the internal operation of a system is known to the tester.

Unattempted

61. Question

A company’s policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?

tcp port = = 21

tcp.port ! = 21

tcp. port = 23

tcp.port = = 21 | | tcp.port = =22

Unattempted

62. Question

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet 10.1.4.0/23. Which of the following IP addresses could be leased as a result of the new configuration?

10.1.255.200

- **10.1.5.200**
- 10.1.4.156
- 10.1.4.254

Unattempted

63. Question

Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

- Cain & Abel
- Wireshark
- Metasploit
- **Maltego**

Unattempted

64. Question

Which utility will tell you in real time which ports are listening or in another state?

- Loki
- Nmap
- **TCPView**
- Netsat

Unattempted

65. Question

Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library? This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

- POODLE

- Heartbleed Bug
- SSL/TLS Renegotiation Vulnerability
- Shellshock

Unattempted

Click Below to go to Next Practice Set

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 →

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy