SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 12

Your results are here!! for" CEHv11 Practice Test 12 "

0 of 65 questions answered correctly

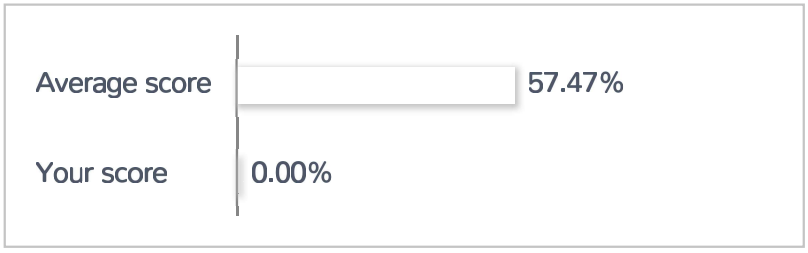
Your time: 00:00:01

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

It is the preliminary phase or "information gathering" phase of ethical hacking.

- Maintaining Access
- Clearing or Covering Tracks
- **Reconnaissance**
- Scanning and Enumeration

Unattempted

The term reconnaissance came from the military word that means to search or survey for military information in the enemy's field. In cybersecurity, reconnaissance or footprinting is the preliminary phase or "information gathering" phase of ethical hacking.

2. Question

What risk is present if a recent nmap scan shows that port 25 is open?

- Unauthenticated access
- Weak SSL version
- Clear text authentication
- **Active mail relay**

Unattempted

Port 25 is SMTP or Simple Mail Transfer Protocol.

3. Question

Which of the following types of Nmap scan is the most reliable but can be easily picked up by IDS?

- SYN scan
- FIN scan
- ACK scan
- **Connect scan**

Unattempted

The TCP full connect (-sT) scan is the most reliable scan but it involves sending a significant number of packets to each port which can be picked up by IDS.

4. Question

Which of the following can be used as a basic vulnerability scanner which can cover several vectors such as FTP, SMB, and HTTP?

- Nessus scripting engine
- SAINT scripting
- Metasploit scripting engine
- **NMAP scripting engine**

Unattempted

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It is designed for network discovery, version detection, backdoor detection, and vulnerability detection and exploitation.

5. Question

Amanda was tasked to check the quality of a program. Before the program reaches her end, it needs to pass a restricted OS first. What do you call this step?

- None of the above
- Quality checking the code
- Sandboxing the code
- **Fuzzy-testing the code**

Unattempted

Fuzz testing is a quality and assurance checking technique that is used to identify coding errors and security loopholes in a targeted web applications.

6. Question

A server with an IP address of 10.10.0.6 was compromised by Paul, a penetration tester from SIA Global Security. Which of the following Nmap commands must he use to quickly list all the machines in the same network?

- **nmap -T4 -F 10.10.0.0/24**
- nmap -T4 -r 10.10.1.0/24
- nmap -T4 -q 10.10.0.0/24
- nmap -T4 -O 10.10.0.0/24

Unattempted

The command "nmap -T4 -F" is used to scan faster than a normal scan because it uses the aggressive timing template and scans fewer ports.

7. Question

This is a global information security standard by "PCI Security Standards Council" that handles cardholders' data for debit, credit, prepaid, e-purse, ATM, and POS cards. This offers a comprehensive and robust standard and supporting materials to improve payment card information security.

- Center for Disease Control (CDC)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Security Industry Organization (ISIO)
- **Payment Card Industry (PCI)**

Unattempted

Payment Card Industry Data Security Standard (PCI DSS) is a global information security standard by "PCI Security Standards Council" that handles cardholders' data for debit, credit, prepaid, e-purse, ATM, and POS cards.

8. Question

Jane conducted a security assessment at SIA Global Security. She discovered that the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and another Domain Name Server (DNS) on the internal network. What do you call this type of DNS configuration?

- Split DNS
- DynDNS
- DNSSEC
- DNS Scheme

Unattempted

A split DNS infrastructure uses two zones for the same domain. One zone is used by the internal network, while the other is used by the external network. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution.

9. Question

This tool is used on a Linux-based system to detect WLANs using 802.11a, 802.11b, 802.11g, and 802.11n WLAN standards.

- Nessus
- Netstumbler
- Kismet
- Abel

Unattempted

Kismet is a wireless network detector, packet sniffer, and intrusion detection system (IDS) that works with any wireless card supporting raw monitoring (rfmon) mode. It can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic and works on Linux, Mac OSX, and Windows 10 under the WSL framework.

10. 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-headers
- http-num
- http-all

Unattempted

http-methods returns all the available methods on the server

11. Question

It is the simplest way of gaining unauthorized access to a targeted system rather than breaking it?

- Packet sniffing
- Port Scanning
- Eavesdropping
- **Social engineering**

Unattempted

Social engineering is an act of using an individual to compromise an information system or to give access to a sensitive resource. It exploits human psychology that aims to manipulate the victim into divulging confidential information in the interest of cybercriminals.

12. Question

Which of the following does not describe Broken Authentication vulnerability?

- **This vulnerability can be mitigated by using the default credentials.**
- This vulnerability allows hackers to compromise account credentials, keys, and session tokens, leading to identity theft.
- It happens when applications related to authentication and session management are incorrectly implemented in the system.
- It is one of the OWASP Top 10 Application Security Risks – 2017

Unattempted

Broken Authentication vulnerabilities can be mitigated by using authentication methods such as multi-factor authentication (MFA) or two-factor authentication (2FA). Another way is by not using the default credentials

and by not allowing repeated invalid login attempts.

13. Question

Which of the following best describes a NULL scan?

- A type of TCP scan where all the flags are turned on.
- A type of UDP scan where all the flags are turned off.
- **A type of TCP scan where all the flags are turned off.**
- A type of TCP scan where the packet size is set to zero.

Unattempted

Null scan is a type of scan that is used to identify listening TCP port. In a null scan, a series of packet is sent to a TCP port with zero bits or no flags set. If the target port is open, a null scan will result to a no response since the host will ignore the packet. If the target port is closed, it will respond a RST packet.

14. Question

Which of the following is a security threat posed by backups?

- Backups can be used to hide usernames and passwords.
- **Stolen un-encrypted backup can be used by cybercriminals for personal gain.**
- Misplaced backups are hard to find.
- Backups can't be used for data recovery.

Unattempted

Ensure that the data in the backup has been properly encrypted to avoid being accessed by unauthorized person.

15. Question

Which of the following open-source tool is best for scanning a network to check for potential targets.

- **Nmap**
- Cain

- Abel
- John the ripper

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.

16. Question

Which of the following protocol and port number is needed in sending log messages to a log analysis tool residing behind a firewall?

- **UDP 514**
- UDP 451
- UDP 415
- UDP 545

Unattempted

UDP 514 is used for system logging.

17. Question

What type of attack happens when a cybercriminal forces the victim's browser to send an authenticated request to the server?

- Cross-site scripting
- Server side request forgery
- **Cross-site request forgery**
- Session hijacking

Unattempted

Cross-site request forgery, also known as CSRF is a type of malicious exploit that allows an attacker to trick users to perform actions that they do not intend to perform. Some examples are changing the email address and/or password, or making a funds transfer. Depending on the nature of the action, the attacker might be able to gain full control over the user's account.

18. Question

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

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

Unattempted

Payment Card Industry Data Security Standard (PCI DSS) is a global information security standard by "PCI Security Standards Council" that handles cardholders' data for debit, credit, prepaid, e-purse, ATM, and POS cards. This include an outline of specifications, tools, measurements, and support resources to help organizations protect the cardholder's information.

19. Question

Network Time Protocol (NTP) uses which of the following UDP port as its primary means of communication?

- 69
- 113
- 161
- **123**

Unattempted

NTP is a UDP-based service. NTP servers use well-known port 123 to talk to each other and to NTP clients.

20. Question

A black hat hacker is trying to compromise a school's computer system. What technique should be used to know the operating system of the computer to launch further attacks?

- SSDP Scanning
- **Banner Grabbing**

- UDP Scanning
- IDLE/IPID Scanning

Unattempted

Banner grabbing, or "OS fingerprinting," is a technique used to determine the running operating system (OS) on a remote target system. The attacker can then formulate an attack strategy based on the OS of the target system.

21. Question

Given an nmap command with host specification of 202.176.56-57.* It will scan how many number of hosts?

- 128
- 10000
- **512**
- 256

Unattempted

256 multiplied by 2 is 512.

22. Question

A deeply upset employee wants to send top-secret information to her current company's competitor. To successfully send these data, she plans to hide this information in a normal message. Which of the following technique is being used in this scenario?

- Cryptography
- RSA
- **Steganography**
- Encryption

Unattempted

Steganography is simply the technique of hiding information from unwanted eyes. It is the practice of hiding information within an ordinary file or message to avoid suspicion. Hackers often use steganography to embed malicious code inside a WAV audio file.

23. Question

This is known as the successor of Secure Sockets Layer (SSL)?

- TLS
- RSA
- GRE
- IPSec

Unattempted

Transport Layer Security (TLS) is the successor protocol of Secure Sockets Layer (SSL). TLS is an improved version of SSL. It works in much the same way as the SSL, using encryption to protect the transfer of data and information.

24. Question

Which protocol is most commonly used for LAN connections and remote access enterprise VPN solutions?

- Internet Protocol Security (IPsec)
- Point-to-Point Protocol (PPP)
- File Transfer Protocol (FTP)
- Secure Electronic Transaction (SET) protocol

Unattempted

Most IPsec based VPNs use ISAKMP (Internet Security Association Key Management Protocol), a part of IKE, to establish, negotiate, modify and delete Security Associations (SA) and cryptographic keys in a VPN environment.

25. Question

A security analyst is encountering a lot of noisy alerts in their security monitoring system. What should be her best approach in this scenario?

- Close all false-negative alerts.
- Close all false positive alerts,

- Continue raising a ticket for all alerts.
- **Tune false positives and false negatives alerts.**

Unattempted

Tuning false positives and false negatives can help identify legitimate threats in the network.

26. Question

Which of the following Intrusion Detection System (IDS) is ideal for checking sensitive network segments. This is also designed to help large organizations detect network-based threats.

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

Unattempted

Network-based intrusion detection system (NIDS) is used to protect a system from network-based threats by monitoring and analyzing network traffic. NIDS scan all inbound packets and hunt for any suspicious patterns. When threats are discovered, the system takes action based on its severity. This includes notifying administrators, or blocking the source IP address from accessing the network.

27. Question

This vulnerability happens when certain applications related to authentication and session management are incorrectly implemented in the system.

- **Broken authentication**
- SQL injection
- Cross site scripting
- Session management

Unattempted

The second security risk as per OWASP Top 10 Application Security Risks 2017 is Broken Authentication. A broken authentication vulnerability allows hackers to compromise an account that can be used to take control of the system. This happens when certain applications related to authentication and session management

are incorrectly implemented in the system. This will allow hackers to compromise account credentials, keys, and session tokens, leading to identity theft.

28. Question

Athena is currently in a work from home set up. This allows her to go anywhere while working. Which do you think is the best way of securing her laptop against data theft?

- **Data encryption on the hard drive.**
- Back up files and store it in a different place.
- Setting up a BIOS password.
- Using a strong logon password.

Unattempted

Data encryption is a securing data by converting it to encoded information, called ciphertext, that can only be decoded or decrypted with a unique decryption key.

29. Question

What software quality assurance technique is used to determine if a program can handle a wide range of invalid input?

- Mutating
- Randomizing
- **Fuzzing**
- Bounding

Unattempted

Fuzz testing is a quality and assurance checking technique that is used to identify coding errors and security loopholes in a targeted web applications. It is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.

30. Question

The Payment Card Industry Data Security Standard (PCI DSS) contains different requirements. Which of the following requirements would best fit under the objective, “Implement strong access control measures”?

- Data encryption before transmission across open and public networks.
- Regularly check for available patches for antivirus software.
- Testing the security systems and processes regularly.
- **Assigning a unique ID to each person with computer access.**

Unattempted

Payment Card Industry Data Security Standard (PCI DSS) is a global information security standard by "PCI Security Standards Council" that handles cardholders' data for debit, credit, prepaid, e-purse, ATM, and POS cards. This offers a comprehensive and robust standard and supporting materials to improve payment card information security. This include an outline of specifications, tools, measurements, and support resources to help organizations protect the cardholder's information.

31. Question

Which of the following is the result of a NULL scan on a closed port?

- **RST**
- FIN
- No response
- SYN

Unattempted

Null scan is a type of scan that is used to identify listening TCP port. In a null scan, a series of packet is sent to a TCP port with zero bits or no flags set. If the target port is open, a null scan will result to a no response since the host will ignore the packet. If the target port is closed, it will respond a RST packet.

32. Question

Which of the following is a Debian based program used for penetration testing?

- VirtualBox
- Windows 10
- **Kali Linux**
- None of the Above

Unattempted

Kali Linux is a Debian-based Linux distribution, which is one of the most popular ethical hacking operating systems. It is an operating system (OS) that specifically caters to network analysts, ethical hackers, or penetration testers.

33. Question

What technique will you use if you want to plan how a packet will move from an untrusted external host to a protected internal host behind the firewall? This method allows the hacker to identify which ports are open and check if the packets can pass through the packet-filtering of the firewall.

- Session hijacking
- Man-in-the-middle attack
- **Firewalking**
- Network sniffing

Unattempted

Firewalking is the method of determining the movement of a data packet from an untrusted external host to a protected internal host through a firewall. The idea behind fire walking is to determine which ports are open and whether packets with control information can pass through a packet filtering device.

34. Question

The equation “Risk = Threat x Vulnerability x Control” is referred to as the:

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

Unattempted

The most common way to describe risk is through Risk equation. This equation is fundamental to all information security.

Risk = Threat x Vulnerability x Control

35. Question

Which of the following US federal law orders executive officers such as the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) to sign confirmation statements regarding the reliability of financial reports?

- Payment Card Industry Data Security Standard (PCI DSS)
- General Data Protection Regulation (GDPR)
- Fair and Accurate Credit Transactions Act (FACTA)
- **Sarbanes-Oxley Act (SOX)**

Unattempted

Sarbanes Oxley Act (SOX), also known as "Public Company Accounting Reform and Investor Protection Act" aims to protect investors and the public from accounting errors and fraudulent practices in enterprises by enhancing corporate disclosures' accuracy and reliability.

36. Question

This tool is used by penetration testers and cybersecurity analysts to easily connect data and functionalities from diverse sources using Transforms.

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

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.

37. Question

SIA Global Security uses multiple layers of antivirus/anti phishing defenses to mitigate which kind of attack?

- Forensic attack
- **Social engineering attack**

- Spoofing attack
- Scanning attack

Unattempted

Social engineering is an act of using an individual to compromise an information system or to give access to a sensitive resource. This attack can be mitigated by using multiple layers of defenses such as end-user antivirus and email gateway.

38. Question

Which of the following is the most prevalent vulnerability according to the Open Web Application Security Project (OWASP) Top 10 Application Security Risks – 2017?

- Broken access control
- Broken authentication
- **Injection**
- Cross site scripting

Unattempted

The most prevalent vulnerability according to the latest (2017) OWASP Top 10 Application Security Risks is Injection.
Injection flaws are commonly found in SQL, LDAP, XPath, NoSQL, OS commands, XML parsers, SMTP headers, expression languages (EL), and Object Relational Mapping (ORM) queries.

39. Question

PUT and DELETE are two critical method. “PUT” can upload a file to the server while “DELETE” can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using what NMAP script engine?

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

Unattempted

HTTP method vulnerability can be checked using NMAP.

40. Question

To check if a certain program can properly handle a wide range of invalid input, automated testing can be done to randomly generate invalid and crash the program. What type of testing is being used here?

- **Fuzzing**
- Mutating
- Dynamic Testing
- Static Testing

Unattempted

Fuzz testing is a quality and assurance checking technique that is used to identify coding errors and security loopholes in a targeted web applications. It is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.

41. Question

A Black Hat hacker has successfully infected a server that will be used in sending and hosting spam email, and taking part in command and coordinated (C&C) attacks. Which of the following trojan infects the server?

- Banking Trojan
- Ransomware Trojan
- **Botnet Trojan**
- Turtle Trojan

Unattempted

Botnet refers to the group of hijacked or infected computers, servers, mobile devices, and IoT (Internet of Things) devices that are being controlled by a hacker. Botnets are used to carry out malicious activities such as account credential leakage, unauthorized access and clicking of ads, sending spam emails, and participating in a DDoS (Distributed Denial of Service) attacks.

42. Question

Which type of hacker is often referred to as crackers or those who exploit security vulnerabilities illegally?

- Black Hat Hacker
- Grey Hat Hacker
- Yellow Hat Hacker
- White Hat Hacker

Unattempted

Black hat hackers are often referred to as crackers. They exploit security networks and look for backdoors, even if they are not permitted to do so.

43. Question

What is SQL Injection?

- SQL Injection is an attack used to gain unauthorized access to a database.
- SQL Injection is a Denial of Service Attack.
- SQL Injection is a Man-in-the-Middle attack between your SQL Server and Web App Server.
- SQL Injection is an attack used to modify code in an application.

Unattempted

Injection flaws are commonly found in SQL, LDAP, XPath, NoSQL, OS commands, XML parsers, SMTP headers, expression languages (EL), and Object Relational Mapping (ORM) queries.
The hacker injects malicious SQL code or query into the user input form to manipulate and control the database, allowing them to access and delete modify information and change other applications' behavior.

44. Question

How would a cybercriminal list all the shares to which the victim has access by using windows CMD?

- NET FILE
- NET USE
- NET CONFIG
- NET VIEW

Unattempted

Net use command connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections.

45. Question

nmap -oX is a command line switch used for?

- Output the results in normal file
- Output the results in Grep file
- **Output the results in XML file**
- Output the results in text file

Unattempted

Nmap -oX is a command line switch used to output the results in xml.file

46. Question

This technique is used to assess whether an end-user security awareness training would be beneficial.

- **Social engineering**
- Web security testing
- Network sniffing
- Port scanning

Unattempted

Social engineering is an act of using an individual to compromise an information system or to give access to a sensitive resource. It exploits human psychology that aims to manipulate the victim into divulging confidential information in the interest of cybercriminals.
This attack can be mitigated by educating the end user on how to deal with social engineering attack.

47. Question

John, an ethical hacker from SIA Global Security, wants to check which IP addresses are currently active on a network. Which of the following should he use?

- **nmap -sP**

- nmap -P
- nmap -O
- nmap -F

Unattempted

#NAME?

48. Question

This type of malware restricts the user from accessing their files and then asks for money for the user to regain access.

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

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.

49. Question

The fastest way of scanning for open ports is by using which of the following command?

- -S
- **-T5**
- -A
- -O

Unattempted

Timing and Performance	
-T0	Paranoid (0) Intrusion Detection System evasion
-T1	Sneaky (1) Intrusion Detection System evasion
-T2	Polite (2) slows down the scan to use less bandwidth and use less target machine resources
-T3	Normal (3) which is default speed
-T4	Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network
-T5	Insane (5) speeds scan; assumes you are on an extraordinarily fast network

50. Question

Which of the following hash function produces a 160-bit message digest output?

- SHA-3
- MD4
- SHA-2
- **SHA-1**

Unattempted

Secure Hash Algorithm 1 or SHA-1 is a cryptographic hash function which produces a 160-bit (20-byte) hash value.

51. Question

Von is a security analyst from SIA Global Security. One of his tasks is to monitor and check the IDS logs. He noticed that an alert was triggered and indeed found a suspicious traffic. He can mark this alert as:

- True Negative
- **True Positive**
- False Negative
- False Positive

Unattempted

True positives are a legitimate attack which triggers a security alert. These alerts indicates that there is an on-going attack or an attack has taken place in the system. For example, an alert was triggered indicating a brute force attack. When you checked the alert, you found out that a cybercriminal was trying to break into one of your systems.

52. Question

How does the term "likelihood" connected to "threat" in Risk Assessments?

- It is the probability that a "threat" is not detected.
- It is the probability that a "threat" is ransomware.
- **It is the probability that a "threat" may occur in the system.**
- It is the probability that the system is vulnerable to threat.

Unattempted

Risk assessment is the calculation of possible consequences and the likelihood of these consequences to occur. Likelihood can be simply defined as the probability of occurrence of a threat that may affect the system, while a consequence is the impact if a threat occurs.

53. Question

A start-up company hired a penetration tester to conduct a security audit on their network. Upon investigating, there was no record of breach because the IDS has been configured properly. This is why no alarms were triggered. What type of alert is the IDS giving?

- False Negative
- False Positive
- **True Negative**
- True Positive

Unattempted

True negative event happens when no attack has taken place and no detection is made.

54. Question

The statement “All computer viruses are malware, but not all malware is a virus” is?

- Cannot be determined
- **TRUE**
- FALSE

Unattempted

There is a common misconception that all malware is a virus. A virus is a type of malware thus, all computer viruses are malware, but not all malware is a virus.

55. Question

Which of the following tools is used by security analysts and penetration testers for graphical link analysis?

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

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.

56. Question

Which of the following port number is used by the LDAP?

- 464
- **389**
- 23
- 25

Unattempted

The default port of Lightweight Directory Access Protocol (LDAP) is 389.

57. Question

Athena is a security engineer at SIA Global Security. She wants to map the company's internal network. What type of scan is being used if she enters the following nmap command:

- nmap -n -sS -P0 -p
- **Stealth scan**
- Full scan
- Scheduled scan
- Quick scan

Unattempted

#NAME?

58. Question

Which of the following tools is designed to silently copy the files and folders of any USB devices connected in your computer?

- **USB Dumper**
- USB Grabber
- USB Snoopy
- USB Sniffer

Unattempted

USB dumper is an application that runs silently as a background process once it started copying the contents of any connected USB device to the computer. The USB device owner has no indication that the files stored on the USB device are copied from the USB to the local system.

59. Question

This program can be used for remotely detecting the operating system (OS) running on the host.

- UserInfo
- Netbus

- Nmap
- None of the above

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.

60. Question

Which of the following special character is sent to web application to check for SQL Injection vulnerability.

- Exclamation point
- Backlash
- **Single quotation**
- Semicolon

Unattempted

Injection attacks can be prevented by doing a source code validation or review. This will allow you to determine the injection flaws and mitigate them before deploying the code into production.

61. Question

An IT Security Analyst from SIA Global Security received an intrusion detection system (IDS) alert due to an abnormal number of packets coming into the network over ports 20 and 21. During investigation, there were no signs of attack on the FTP servers. This alert can be marked as:

- False negatives
- **False positives**
- True positives
- True negatives

Unattempted

False positives are mislabeled security alerts. These alerts indicates that there is a threat when in reality no attack has taken place.

62. Question

Which of the following statements are not true?

- **Viruses spread faster than the worms.**
- Worms can be remotely controlled.
- Viruses spread slower than the worms.
- Viruses cannot be controlled remotely.

Unattempted

Computer viruses can spread across the network only with the help of human intervention while worms do it independently.

63. Question

This command line switch in nmap allows you to determine which IP protocols are supported by target machines:

- #NAME?
- #NAME?
- **#NAME?**
- #NAME?

Unattempted

#NAME?

64. Question

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

- 11001100
- **10100110**
- 1011001
- 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.

65. Question

As a security engineer at SIA Global Security, part of your work is to deploy a secure remote access solution that will allow your colleagues to connect to the company's internal network. Which of the following must be implemented to mitigate man-in-the-middle attack?

- SSL
- **IPSec**
- Static IP addresses
- Mutual authentication

Unattempted

IPsec is the most commonly implemented technology for both gateway-to-gateway (LAN-to-LAN) and host to gateway (remote access) enterprise VPN solutions. IPsec provides data security by employing various components like ESP (Encapsulation Security Payload), AH (Authentication Header), and IKE (Internet Key Exchange) to secure communication between VPN end-points.

Click Below to go to Next Practice Set

We help you to succeed in your certification exams

We have helped over thousands of working professionals to achieve their certification goals with our practice tests.

Skillcertpro

Quick Links

ABOUT US
FAQ
BROWSE ALL PRACTICE TESTS
CONTACT FORM

Important Links

REFUND POLICY
REFUND REQUEST
TERMS & CONDITIONS
PRIVACY POLICY

Privacy Policy