SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 18

Your results are here!! for" CEHv11 Practice Test 18 "

0 of 65 questions answered correctly

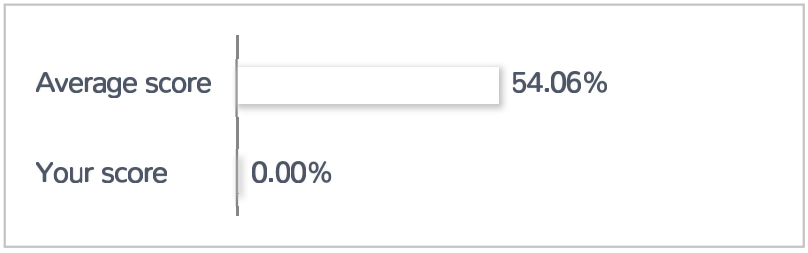
Your time: 00:00:01

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

Which of the following configuration allows a wired or wireless network interface controller to pass all traffic it receives to the central processing unit (CPU), rather than passing only the frames that the controller is intended to receive?

- WEM
- **Promiscuous mode**
- Multi-cast mode
- Port forwarding

Unattempted

Promiscuous mode refers to the special mode of Ethernet hardware that allows a NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.

2. Question

You were hired to perform a penetration testing and security assessments for small company in the local area. While conducting a routine security assessment, you discovered that your client is involved in human trafficking. What should you do?

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

Unattempted

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

3. Question

Using a smart card and a PIN as a two-factor authentication satisfies which of the following?

- Something you know and something you are
- **Something you have and something you know**
- Something you are and something you remember
- Something you have and something you are

Unattempted

Smart card = Something you have

PIN = Something you know

4. Question

David was hired to do penetration testing in a bank. He was able to gain access to the system via a buffer overflow exploit. Upon further investigation, he found a folder filled with usernames and passwords. This includes the administrator's bank account password and login information to his bitcoin account. What should David do?

- Do not transfer the money but steal the bitcoins.
- Do not report it and continue the penetration test.
- Transfer money from the administrator's account to another account.
- **Report immediately to the administrator**

Unattempted

Immediately report the findings to the administrator to avoid future damages.

5. Question

Which of the following tools can be used in password cracking of Server Message Block (SMB)?

- [ ] Pwddump2
- [ ] L0phtCrack
- [ ] KrbCrack
- [ ] SMBRelay

Unattempted

L0phtCrack is a Windows password recovery tool that can be used by cybercriminals with the dictionary, brute force, and hybrid password-cracking attacks. SMBRelay is a Server Message Block (SMB) server that is used to grab usernames and password hashes from inbound SMB traffic.

6. Question

Which of the following does not belong to the group?

- ( ) Reconnaissance
- ( ) Blocking
- ( ) Gaining Access
- ( ) Scanning and Enumeration

Unattempted

Phases of Ethical Hacking

1. Reconnaissance
2. Scanning and Enumeration
3. Gaining Access
4. Maintaining Access
5. Clearing and Covering Tracks

7. Question

Which of the following is the best way to prevent network sniffing?

- ( ) Register all machines MAC Address in a Centralized Database
- ( ) Restrict Physical Access to Server Rooms hosting Critical Servers
- ( ) Use Static IP Address

- Using encryption protocols to secure network communications

Unattempted

Aside from refraining from using public networks, encryption is the best bet for protecting the network from potential packet sniffers.

8. Question

Which type of security document is written with specific step-by-step details?

- Paradigm
- **Procedure**
- Policy
- Process

Unattempted

A security procedure is a set sequence of necessary activities that performs a specific security task or function. Procedures are normally designed as a series of steps to be followed as a consistent and repetitive approach or cycle to accomplish a result.

9. Question

Which of the following is/are known weaknesses of Windows LAN Manager (LM)?

- [ ] Makes use of only 32-bit encryption.
- [ ] **The effective length is 7 characters.**
- [ ] **Converts passwords to uppercase.**
- [ ] **Hashes are sent in clear text over the network.**

Unattempted

The LM hash is computed as follows.

1. The user's password as an OEM string is converted to uppercase.
2. This password is either null-padded or truncated to 14 bytes.
3. The "fixed-length" password is split into two 7-byte halves.
4. These values are used to create two DES keys, one from each 7-byte half.
5. Each of these keys is used to DES-encrypt the constant ASCII string "KGS!@#$%", resulting in two 8-byte

ciphertext values.

6. These two ciphertext values are concatenated to form a 16-byte value, which is the LM hash. The hashes themself are sent in clear text over the network instead of sending the password in cleartext.

10. Question

This type of IDS (Intrusion Detection System) can monitor and automatically defend against attacks.

- Passive
- **Active**
- Reactive
- Detective

Unattempted

An active Intrusion Detection System (IDS) is also known as Intrusion Detection and Prevention System (IDPS). It is configured to automatically block suspected attacks without any intervention required by an operator.

11. Question

Brian is working as a Security Analyst in a large manufacturing company. The company owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8. While monitoring the data, he discovered a high number of outbound connections from one of the company's internal IP to a blacklisted public IP. Upon further investigating, the internal communicating devices are already compromised. What kind of attack is being described in the scenario?

- Spear Phishing Attack
- **Botnet Attack**
- Rootkit Attack
- Advanced Persistent Threats

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 DDoS (Distributed Denial of Service) attacks.

12. Question

This has been used by government authorities before as their methods of information discovery?

- Wiretapping
- Spoofing
- **Wiretapping**
- SMB signing

Unattempted

Wiretapping is a form of electronic eavesdropping accomplished by seizing or overhearing communications through a concealed recording or listening device connected to the transmission line.

13. Question

Which of the following provides the difference between an anomaly-based IDS over a signature-based IDS?

- Requires vendor updates for a new threat
- Produces fewer false positives
- **Can identify unknown attacks**
- Cannot deal with encrypted network traffic

Unattempted

A signature-based IDS can only detect known attacks for which a signature has previously been created.

14. Question

A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a password for the forms or a new document, the student decides to write a script that pulls passwords from a list of commonly used passwords instead. He will use this to try against the secured PDF until the correct password is found or the list is exhausted. Which cryptography attack is the student attempting?

- **Dictionary attack**
- Brute-force attack

- Man-in-the-middle attack
- Session hijacking

Unattempted

A dictionary attack is a brute-force technique where attackers run through common words and phrases, such as those from a dictionary, to guess passwords.

15. Question

Which of the following is/are types of honeypot deployments?

- **Pure honeypots**
- Mixed honeypots
- **High-interaction honeypots**
- **Low-interaction honeypots**

Unattempted

Pure, low-interaction, and high-interaction are types of honeypot deployments.

16. Question

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

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

Unattempted

A null scan is a type of scan that is used to identify a listening TCP port. In a null scan, a series of packets is sent to a TCP port with zero bits or no flags set. If the target port is closed, it will respond a RST packet.

17. Question

This type of IDS (Intrusion Detection System) can monitor and alert on attacks, but cannot stop them.

- Passive
- Detective
- Reactive
- Active

Unattempted

A passive IDS is a system that's configured to only monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. A passive IDS is not capable of performing any protective or corrective functions on its own.

18. Question

Which of the following does not below to the group?

- Injection
- Encryption
- Broken Authentication
- Cross-site scripting

Unattempted

Cross-site scripting, Broken Authentication, and Injection belong to the OWASP Top 10 Web Application Security Risks.

19. Question

Rick works as a penetration tester at SIA University. Which type of virus detection method is used if he uses a detection method where the anti-virus executes the malicious codes on a VM to simulate CPU and memory activities?

- Heuristic Analysis
- Integrity checking
- Code Emulation
- Scanning

Unattempted

The code emulation method of malware detection scans a file's behavior by emulating its execution in a virtual (emulated) environment.

20. Question

This type of attack poses as an authorized AP by beaconing the WLAN's SSID to lure users.

- Session Hijacking
- Cracking WEP key
- **Evil Twin AP**
- Eavesdropping

Unattempted

Evil Twin is a wireless AP that pretends to be a legitimate AP by imitating another network name. It poses a clear and present danger to wireless users on private and public WLANs.

21. Question

John received a distraught call from his company's security team. They told him that they are under a denial of service attack. Coincidentally, John is performing a ping scan into a target network and when he stopped his scan, the smurf attack event stops showing too on the IDS monitor. What should John do to avoid triggering this event in the IDS?

- Only scan the Windows systems.
- **Avoid scanning the broadcast IP.**
- Try scanning more slowly.
- Spoof the source IP address.

Unattempted

Scanning the broadcast address makes the scan target all IP addresses on that subnet at the same time.

22. Question

This security policy defines the use of VPN for gaining access to an internal corporate network.

- Access control policy
- Information protection policy
- **Remote access policy**
- Network security policy

Unattempted

Remote-Access Policy (RAP) contains a set of rules that define authorized connections. It defines who can have remote access, the access medium, and remote access security controls. This policy is essential in larger organizations since most employees are now working from home.

23. Question

Which of the following types of FTP allows a user to access a certain directory and its contents (even without permission) as long as the user knows the correct path and file name.

- Hidden FTP
- Secure FTP
- Passive FTP
- **Blind FTP**

Unattempted

Blind FTP, also known as anonymous FTP, allows users to go directly to a specific directory as long as they use the correct path and file name.

24. Question

This risk will remain even after applying all the theoretically possible safety measures?

- Inherent risk
- **Residual risk**
- Deferred risk
- Impact risk

Unattempted

According to ISO 27001, residual risk is “the risk remaining after risk treatment”.

25. Question

This tool is used by cybercriminals in achieving a connection to a remote computer and then executing a Trojan on it?

- **PsExec**
- Hk.exe
- RemExec
- GetAdmin.exe

Unattempted

PsExec or psexec.exe is a command-line utility built for Windows. It allows administrators to run programs on local and more commonly remote computers.

26. Question

Which of the following is/are NOT an example of a Denial of Service (DoS) attack?

- Smurf
- ICMP flood
- SYN flood
- **Prometei**

Unattempted

Denial of service, or DoS, is an attack on a computer or network which makes it inaccessible to the user. Some popular DoS attacks are SYN flood, ICMP flood, and smurf.

27. Question

Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 15?

- **3072 bit key**
- 2048 bit key

1536 bit key

1025 bit key

Unattempted

· DH Group 1: 768-bit group
· DH Group 2: 1024-bit group
· DH Group 5: 1536-bit group
· DH Group 14: 2048-bit group
· DH Group 15: 3072-bit group

28. Question

Janine is a Linux administrator from SIA Global Security. She was hired by a large financial company to investigate the recent suspicious logins on a Linux server occurring during non-business hours. After further checking, Janine realizes the system time on the Linux server is wrong by more than twelve hours. What protocol has stopped working on Linux servers which affected the synchronization of time?

Time Keeper

NTP

PPP

OSPP

Unattempted

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

29. Question

Which of the following tool can be used in performing session splicing attacks?

TCPsplice

Hydra

Whisker

Burp

Unattempted

A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. A whisker is an evasion tool that crafts packets with small payloads referred to as session splicing.

30. Question

Which of the following is the phase where the actual ethical hacking takes place. This involves attacking one device and controlling it to perform another attack on another device connected in the same network.

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

Unattempted

The third phase of ethical hacking known as Gaining access. This is the phase where the actual ethical hacking takes place. The system weaknesses or vulnerabilities found in phases one and two were exploited by the hacker to obtain access to the system.

31. Question

Which of the following encryption levels does WPA2 use AES for wireless data encryption?

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

Unattempted

WPA2 is an updated version of WPA that uses AES encryption and long passwords to create a secured network. CCMP, also known as AES CCMP is the security standard used with WPA2 wireless networks. CCMP employs 128-bit keys and a 48-bit initialization vector that minimizes vulnerability to replay attacks.

32. Question

Which of the following belongs to OWASP Top 10 Web Application Security Risks?

- [ ] Cross-site scripting
- [ ] Injection
- [ ] Encryption
- [ ] Broken Authentication

Unattempted

Cross-site scripting, Broken Authentication, and Injection belong to the OWASP Top 10 Web Application Security Risks.

33. Question

Which of the following can be used by cybercriminals to hide secret data within a text file?

- ( ) Snow.exe
- ( ) Image hide
- ( ) Fpipe
- ( ) SARA

Unattempted

Snow.exe is a steganography tool that can be used to embed and mask secret data within simple text files. Since spaces and tabs are usually not visible in text viewers, where the file will likely open, messages can be effectively sneaked in without cluing in an unguarded observer.

34. Question

This tool is specifically designed to find potential exploits in Microsoft Windows products?

- ( ) Microsoft Baseline Security Analyzer
- ( ) Retina
- ( ) Core Impact
- ( ) Microsoft Security Baseline Analyzer

Unattempted

Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed for IT professionals and helps small and medium-sized businesses determine their security state per Microsoft security recommendations and offers specific remediation guidance. It is a standalone security and vulnerability scanner designed to provide a streamlined method for identifying common security misconfigurations and missing security updates.

35. Question

Which of the following are characteristics of a strong password commonly found in a password policy? Select all that applies.

- [ ] Password must use only words found in a dictionary or including their street address or other personal information.
- [ ] **Password must include one or more special characters.**
- [ ] **Password must include one or more numerical digits.**
- [ ] **Password must make use of both upper- and lower-case letters.**

Unattempted

A password policy encourages users to use strong passwords and update them properly to enhance a web server's security.

36. Question

This security policy ensures that updates to policies, procedures, and configurations are controlled and documented.

- ○ Regulatory compliance
- ○ Peer review
- ○ **Change management**
- ○ Penetration testing

Unattempted

Change Management Policy refers to a process of making changes to IT, software development, and security services or operations. This policy aims to increase the awareness and understanding of proposed changes across an organization and ensure these changes are conducted methodically to minimize any unfavorable impact on services and customers.

37. Question

Password stealing is a cyberattack that allows cybercriminals to utilize user credentials that can cause significant data losses from the system. Which of the following is/are NOT a type of password attack?

- Phishing
- Visual Hacking
- Shoulder surfing
- **Password hashing**

Unattempted

Password hashing is a password encryption method done before its storage so that the system password databases cannot easily be decrypted.

38. Question

Theon logged in as a local admin on a Windows 7 system and needs to launch the Services Manager from command line. Which of the following command will he use?

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

Unattempted

To open the Services Manager from command line just type services.msc in your run box or at the command line.

39. Question

This happens when an application fails to secure the stored or in-transit sensitive information or personally identifiable information (PII) against hackers.

- Injection
- Broken Authentication

- Sensitive data exposure
- Cross-site scripting

Unattempted

Sensitive data exposure happens when an application fails to secure the stored or in-transit sensitive information such as account credentials, credit card numbers, Social Security Numbers, financial and healthcare information, and other personally identifiable information (PII) against hackers.

40. Question

This is an extremely common IDS evasion technique in the web world?

- Spyware
- Subnetting
- Port knocking
- Unicode characters

Unattempted

Unicode attacks can be effective against applications that understand them. Unicode evasion is also referred to as UTF-8 evasion. Non-Unicode character encodings are known as overlong characters, and may be signs of an attempted attack.

41. Question

Which access control mechanism uses a central authentication server (CAS) that permits users to authenticate only once but gain access to multiple systems?

- Single sign-on
- Role-Based Access Control (RBAC)
- Windows authentication
- Discretionary Access Control (DAC)

Unattempted

Single sign-on (SSO) is an authentication method that allows users to securely authenticate with multiple applications and websites by using just one set of credentials.

42. Question

Which of the following can be used in protecting a router from potential smurf attacks?

- Enabling port forwarding on the router.
- Installing the router outside of the network's firewall.
- **Disabling the router from accepting broadcast ping messages.**
- Placing the router in broadcast mode.

Unattempted

To prevent smurf attacks, you can:

1. Disable IP-directed broadcasts on your router.
2. Reconfigure your operating system to disallow ICMP responses to IP broadcast requests.
3. Reconfigure the perimeter firewall to disallow pings originating from outside your network.

43. Question

While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?

- **The port will ignore the packets**
- The port will send an RST
- The port will send an ACK
- The port will send a SYN

Unattempted

TCP XMAS scan is used to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with all possible flags set in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out-of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.

44. Question

Which of the following is/are NOT an example of active reconnaissance?

- Traceroute
- Ping
- **Spyse**
- Nmap

Unattempted

Active reconnaissance is the opposite of passive reconnaissance wherein the information is gathered by directly engaging with the potential target. This may be done via manual testing or automated scanning using tools such as Nmap, ping, traceroute, and netcat.

45. Question

What style of attack is discussed in this scenario: Cybercriminals discover vulnerabilities and hold on to them until they want to launch a sophisticated attack.

- zero-hour
- zero-sum
- **zero-day**
- no-day

Unattempted

A zero-day attack (also referred to as Day Zero) is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of. The software developer must rush to resolve the weakness as soon as it is discovered in order to limit the threat to software users.

46. Question

This scanning method splits the TCP header into several packets which makes it difficult for packet filters to detect the purpose of the packet?

- ICMP Echo scanning
- **SYN/FIN scanning using IP fragments**
- ACK flag probe scanning

IPID scanning

Unattempted

IP fragmentation occurs when packets are broken up into smaller pieces (fragments) so they can pass through a link at a smaller maximum transmission unit than the original or larger packet size. IP fragmentation can cause problems when fragments are affected by packet loss and cause excessive retransmissions. This can cause performance issues. To recover the loss of a fragment, protocols, like TCP, retransmit fragments in order to reassemble them. Fragmented traffic can also be crafted to evade intrusion detection systems and be used maliciously.

47. Question

A firewall checks which of the following to prevent particular ports and applications from getting packets into an organization?

Headers of presentation layer and port numbers of the session layer.

Port numbers of application layer and headers of the transport layer.

Port numbers of Transport layer and headers of the application layer.

Headers of presentation layer and port numbers of the session layer.

Unattempted

Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or transport layer port, destination services like WWW or FTP. They can filter based on protocols, TTL values, netblock of the originator, of the source, and many other attributes. Application layer firewalls are responsible for filtering at 3, 4, 5, 7 layers. Because they analyze the application layer headers, most firewall control and filtering are performed actually in the software.

48. Question

Which of the following tools can be used for passive OS fingerprinting?

Tcpdump

Nmap

Ping

Tracert

Unattempted

The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools.

49. Question

Which of the following is the correct process for the TCP three-way handshake connection establishment?

- ACK, ACK-SYN, SYN
- ACK, ACK-FIN, FIN
- **SYN, SYN-ACK, ACK**
- FIN, ACK-FIN, ACK

Unattempted

Connection Establishment: SYN, SYN-ACK, ACK

Connection Termination: FIN, ACK-FIN, ACK

50. Question

The Open Web Application Security Project or OWASP Foundation addresses the need to secure web applications by providing which of the following services?

- Web application patches
- **List of web application security flaws and how to mitigate them**
- Extensible security framework named COBIT
- Security certification for hardened web applications

Unattempted

The Open Web Application Security Project or OWASP is a non-profit foundation 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 critical web application security risks. It offers insights to developers and security professionals on the most prevalent vulnerabilities that are commonly found in web applications so they may incorporate the report's findings and recommendations into their security practices.

51. Question

This process can determine the potential impacts when some of the critical business processes of the company interrupt its service.

- Emergency Plan Response (EPR)
- **Business Impact Analysis (BIA)**
- Risk Mitigation
- Disaster Recovery Planning (DRP)

Unattempted

A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment.

52. Question

Password cracking software applications can reverse the hashing process to recover passwords.

- **FALSE**
- TRUE

Unattempted

Hash functions are not reversible.

53. Question

This is a critical procedure that an ethical hacker must perform after being brought into an organization?

- **Sign a formal contract with non-disclosure.**
- Turn over deliverables.
- Assess what the organization is trying to protect.
- Begin security testing.

Unattempted

A contract and non-disclosure agreement (NDA) is usually signed between the ethical hacker and the organization. This ensures the legality of what they are doing and that both parties are protected.

54. Question

This type of antenna is used in wireless communication.

- Bi-directional
- Parabolic
- Uni-directional
- **Omnidirectional**

Unattempted

An omnidirectional antenna is a wireless transmitting/receiving antenna that radiates or intercepts radio-frequency (RF) electromagnetic fields equally well in all horizontal directions in a flat, two-dimensional (2D) geometric plane. Omnidirectional antennas are used in most consumer RF wireless devices, including cellular telephone sets and wireless routers.

55. Question

Which type of sniffing technique is generally referred to as Man-in-The-Middle (MiTM) attack?

- **ARP Poisoning**
- DHCP Sniffing
- Password Sniffing
- Mac Flooding

Unattempted

ARP poisoning, also known as ARP flooding is a technique used to attack a local-area network (LAN). It allows an attacker to intercept data frames on a LAN, modify the traffic, or stop the traffic altogether. The attack can only be used on networks that make use of the Address Resolution Protocol (ARP) and not another method of address resolution.

56. Question

Which IPsec mode should you implement when your utmost priority is security and confidentiality of data within the same LAN?

- AH promiscuous

- AH Tunnel mode
- **ESP confidential**
- ESP transport mode

Unattempted

Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload.

57. Question

What tool can crack Windows SMB passwords simply by listening to network traffic?

- **L0phtcrack**
- Netbus
- This is not possible
- NTFSDOS

Unattempted

L0phtCrack 7 is a state-of-the-art tool for password auditing and recovery that serves to guide organizational policies and procedures. uses a variety of sources and methods to retrieve passwords from the operating system.

58. Question

Which element of security testing is being assured by using hash?

- Availability
- Confidentiality
- Authentication
- **Integrity**

Unattempted

Cryptography plays a major role in ensuring data integrity. Commonly used methods to protect data integrity include hashing the data you receive and comparing it with the hash of the original message.

59. Question

This TCP/IP protocol is used in matching an IP address to MAC addresses on a network interface card (NIC).

- PIM
- **ARP**
- RARP
- DHCP

Unattempted

Address Resolution Protocol (ARP) is one protocol of the TCP/IP protocol suite that is used to resolve an IP address to its matching MAC address.

60. Question

Which of the following account authentications is/are supported by SSH-2 protocol?

- Rhosts (RSH-style) authentication
- Kerberos authentication
- **Password-based authentication**
- TIS authentication

Unattempted

SSH-2 protocol supports Publickey, Host-based, and Password-based authentication types. SSH-1 supports a wider range of account authentication types, including RSA only, RhostsRSA, Rhosts (RSH-style), TIS, and Kerberos authentication types.

61. Question

This is a client-server tool used to evade firewall inspection?

- hping
- Nikto
- **TCP-over-DNS**
- kismet

Unattempted

Tcp-over-DNS is a tool that can be utilized in evading firewall inspection.

62. Question

Which of the following is an example of two-factor authentication?

- Fingerprint and Smartcard ID
- Username and Password
- Digital Certificate and Hardware Token
- PIN Number and Birth Date

Unattempted

Two-factor authentication (2FA) is a security process in which users provide two out of three different authentication factors to verify themselves. The three authentication factors are something you have (smartcard ID), something you know, and something you are (Fingerprint).

63. Question

Which of the following is/are an example of a Denial of service (DoS) attack?

- ICMP flood
- SYN flood
- Smurf
- Prometei

Unattempted

Denial of service, or DoS, is an attack on a computer or network which makes it inaccessible to the user. Some popular DoS attacks are SYN flood, ICMP flood, and smurf.

64. Question

A cybercriminal wishes to use a netbus Trojan on the Windows program to break into the targeted machine. Which of the following tools will help the cybercriminal execute his plan?

- Cover

- Wrapper
- Tripwire
- Binder

Unattempted

A wrapper is a tool used to combine a harmful executable file with a harmless executable file.

65. Question

Jacob is a network administrator at SIA University. He realized that most of the students are connecting their laptops in the wired network to have Internet access. Ethernet ports in the campus are available for professors and authorized visitors only. He discovered this when the IDS alerted for malware activities in the network. What should he do to mitigate this problem?

- Disable the unused ports in the switches
- Ask the students to use the wireless network instead
- Separate the students in a different VLAN
- **Use the 802.1x protocol**

Unattempted

802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network.

Click Below to go to Next Practice Set

← Previous Post

Next Post →

Skillcertpro

Quick Links

ABOUT US

FAQ

BROWSE ALL PRACTICE TESTS

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy