SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 16

Your results are here!! for" CEHv11 Practice Test 16 "

0 of 65 questions answered correctly

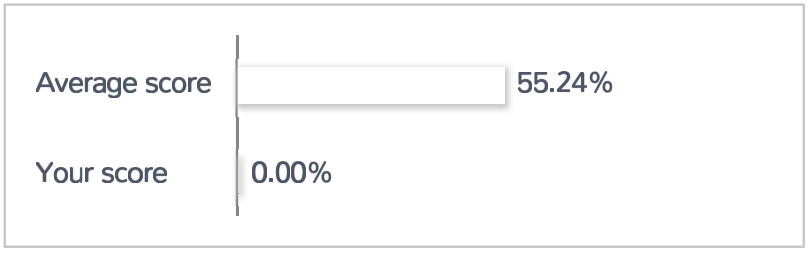
Your time: 00:00:02

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 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

While Athena is accessing her bank account using a web browser, she receives an email containing a link that says "awesome cats". She clicks on the link and shows a video of dancing cats. The next day, she receives an email notification from her bank, asking to verify the transactions made outside of the country. What web browser-based vulnerability was exploited?

- Webform input validation
- Cross-Site Scripting
- **Cross-Site Request Forgery**
- Clickjacking

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. 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.

2. Question

Jane is a Security Analyst from a large financial company. One of her tasks is to analyze IDS logs. While checking the alerts, she noticed that an alert was triggered and wants to know if it's true positive or false positive. Below are the basic details of the log:

Source IP: 192.168.11.107

Source port: 80

Destination IP: 192.168.10.205

Destination port: 63221

We can say that the alert is?

- This is most probably true negative.

- This is most probably false-positive because an alert triggered on reversed traffic.
- This is most probably false-positive because IDS is monitoring one-direction traffic.
- This is most probably true positive which triggered secure communication between client and server.

Unattempted

False positives are mislabeled security alerts. These alerts indicate that there is a threat when in reality no attack has taken place. For example, an alert was triggered indicating a brute force attack, but later on, found out that it was just the user who mistyped the password a lot of times.

3. Question

This programming language is the most vulnerable to buffer overflow attacks because it lacks a built-in-bounds checking mechanism?

- C++
- C#
- Python
- Java

Unattempted

Programming languages such as C#, Java, Python have built-in inbound checking.

4. Question

To show improvement of security over time, what must be developed?

- Metrics
- Testing tools
- Taxonomy of vulnerabilities
- Reports

Unattempted

The management demands metrics to get a clearer view of security. Metrics measures participation, effectiveness, and window of exposure. It provides information the organization can use to make plans and improve programs.

5. Question

Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch. What happens when the CAM table becomes full due to a MAC flooding attack?

- Every packet is dropped and the switch sends out SNMP alerts to the IDS port.
- The switch replaces the outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF
- **Switch then acts as a hub by broadcasting packets to all machines on the network**
- The CAM overflow table will cause the switch to crash causing Denial of Service

Unattempted

When the CAM table becomes full, the switch acts as a hub by broadcasting packets to all machines on the network. This gives an advantage to the attacker and can sniff all packets coming from the switch.

6. Question

What does GINA stand for?

- Global Internet National Authority (G-USA)
- **Graphical Identification and Authentication**
- Gateway Interface Network Application
- GUI Installed Network Application CLASS

Unattempted

GINA stands for Graphical Identification and Authentication. Graphical Identification and Authentication (GINA) is a component of Windows 2000, Windows XP, and Windows Server 2003 that provides secure authentication and interactive logon services.

7. Question

Theon logged in as an admin account. He wants to know what to type on the windows command line to launch the Computer Management Console.

- c:\services.msc
- c:\ncpa.cpl

c:\gpedit

c:\compmgmt.msc

Unattempted

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

8. Question

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

Clear text authentication

Weak SSL version

Unauthenticated access

Active mail relay

Unattempted

Port 25 is SMTP or Simple Mail Transfer Protocol.

9. Question

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

Parabolic grid antenna

Omnidirectional antenna

Dipole antenna

Yagi antenna

Unattempted

Yagi antennas can be used in the frequency range from about 3 – 3000 MHz, with the best operating range below about 1500 MHz.

10. Question

Which of the following attacks exploits web age vulnerabilities that allow the cybercriminal to control and send malicious requests from an unsuspecting user's browser without the victim's knowledge?

- File Injection Attack
- **Cross-Site Request Forgery (CSRF)**
- Command Injection Attacks
- Hidden Field Manipulation Attack

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. 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.

11. Question

This network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack.

- SYN flood
- **Teardrop**
- Ping of death
- Smurf attack

Unattempted

The teardrop attack uses overlapping packet fragments to confuse a target system and cause the system to reboot or crash.

12. Question

What does the following command "nc -l -u -p55555 < /etc/passwd?" in netcat do?

- logs the incoming connections to /etc/passwd file
- loads the /etc/passwd file to the UDP port 55555
- deletes the /etc/passwd file when connected to the UDP port 55555

grabs the /etc/passwd file when connected to UDP port 55555

Unattempted

The command "nc -l -u -p55555 < /etc/passwd" will grab the passwd file once connected to UDP port 55555.

13. Question

It is an act of gathering information without engaging with the system or the individual itself.

Enumeration

Network Mapping

Active Reconnaissance

Passive Reconnaissance

Unattempted

Passive reconnaissance is the process of gaining valuable information without alerting the potential victim. It is also an act of gathering information without engaging with the system or the individual. An example of passive reconnaissance is reviewing or checking the targeted company's website.

14. Question

This describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

Recovery agent

Directory

Key registry

Key escrow

Unattempted

Key escrow is a cryptographic key exchange process in which a key is held in escrow, or stored, by a third party. A key that is lost or compromised by its original user(s) may be used to decrypt encrypted material, allowing restoration of the original material to its unencrypted state.

15. Question

Which of the following describes a covert channel?

- Covert channel transfers information over, within a computer system, or network that is encrypted.
- Covert channel transfers information via a communication path within a computer system or network for the transfer of data.
- **Covert channel transfers information over, within a computer system, or network that is outside of the security policy.**
- Covert channel transfers information over, within a computer system, or network that is within the security policy.

Unattempted

An Internet covert channel is the digital equivalent of a briefcase with a secret compartment that a spy might use to slip sensitive documents past security guards into or out of a secure facility. An attacker can use Internet covert channels to transmit sensitive documents unobserved, bypassing network security measures.

16. Question

What service is required to run before starting metasploit console (msfconsole)?

- Mysql
- Mssql
- Meterpreter
- **Postgresql**

Unattempted

To run the Metasploit, the user must first start postgresql server. The user may type “sudo service postgresql start” and enter his/her credentials when prompted.

17. Question

Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

- Social engineering
- **Penetration testing**

- Access control list reviews
- Vulnerability scanning

Unattempted

Penetration testing is a methodological approach to security assessment that encompasses the security audit and vulnerability assessment and demonstrates if the vulnerabilities in the system can be successfully exploited by attackers.

18. Question

This tool is used to analyze the files produced by packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

- Tcptraceroute
- **Tcptrace**
- OpenVAS
- Nessus

Unattempted

Tcptrace is a tool for the analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump/WinDump/Wireshark, snoop, EtherPeek, and Agilent NetMetrix.

19. 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 5?

- 768 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

20. Question

Which of the following is an effect of having high humidity in a data center?

- Static electricity
- Airborne contamination
- **Corrosion**
- Heat

Unattempted

High humidity in data servers causes corrosion while low humidity causes static electricity.

21. Question

Mark is s recently hired network security associate at SIA Global Security. One of his tasks is to look for unauthorized devices by performing daily scans of the internal network. To make things easier for him, he wrote a script that will scan the network for unauthorized devices every six in the morning. Which of the following programming languages would allow him to do this?

- **Python**
- PHP
- C#
- ASP.NET

Unattempted

Python allows you to write programs that can automate tasks you usually do for hours.

22. Question

Which of the following device will enable the capture of all traffic when using a Wireshark to acquire packet capture on a network?

- Layer 3 switch

- **Network tap**
- Application firewall
- 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.

23. Question

Which of the following describes a “white box testing?”

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

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.

24. Question

Which of the following protocol is being used by smart cards to transfer the certificate securely?

- Point to Point Protocol (PPP)
- Layer 2 Tunneling Protocol (L2TP)
- **Extensible Authentication Protocol (EAP)**
- Point to Point Tunneling Protocol (PPTP)

Unattempted

Extensible Authentication Protocol (EAP) is an authentication protocol that was originally designed for Point-to-Point connections. It is used as an alternative to CHAP and PAP authentication protocols as it is more

secure and supports different authentication mechanisms such as passwords, smart tokens, OTPs (one-time passwords), Secure ID cards, digital certificates, and public-key encryption mechanisms.

25. Question

It is an agreement between the client and the ethical hacker wherein the latter agrees to maintain the confidentiality of the former's sensitive information.

- Contract
- Job Order
- **Non-disclosure Agreement**
- Rules of Engagement

Unattempted

As an ethical hacker, it is important to maintain the confidentiality of sensitive data. Do not disclose any sensitive information obtained from your ethical hacking to other third parties unless authorized by the owner. A non-disclosure agreement (NDA) can be issued to gain the trust of your clients.

26. Question

It is the practice of hacking a certain system or network without malicious intent.

- Hacking
- Ethical Exposing
- Exposing
- **Ethical Hacking**

Unattempted

Ethical hacking is the practice of hacking without malicious intent. The goal of ethical hacking is to expose known security vulnerabilities of a certain system or network to help the owners address and fix these before being discovered by malicious hackers.

27. Question

Which of the following belongs to the requirements of PCI DSS? (Select all that apply.)

- [ ] Regularly conduct a vulnerability scanning and penetration testing
- [ ] Scan and update the antivirus software regularly.
- [ ] Avoid using default passwords and settings.
- [ ] Restrict access to cardholder information by business need-to-know.

Unattempted

The 12 requirements of PCI DSS that must be complied with are:

1. Installing, maintaining, and configuring your firewall.
2. Avoid using default passwords and settings.
3. Protect the stored cardholders' information.
4. Encrypt transmission of cardholder data across open, public networks.
5. Scan and update antivirus software regularly.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder information by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder information.
10. Track and monitor all access to network resources and cardholder information.
11. Regularly conduct a vulnerability scan and do penetration testing
12. Maintain a policy that addresses information security.

28. Question

This is used to identify the weaknesses in the computer systems and network that occur due to misconfigurations.

- ○ Network Mapping
- ○ Vulnerability Scanning
- ○ Port Scanning
- ○ Enumeration

Unattempted

In ethical hacking, vulnerability scanning is used to identify the weaknesses in the computer systems and network that occur due to misconfigurations. Without this, it is not possible to determine the existing vulnerabilities within the targeted system or network that can be exploited by the hacker.

29. Question

Jane, a Certified Ethical Hacker from SIA Global Security, was contacted by a private firm to conduct an external security assessment through penetration testing.

What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

- Project Scope
- Non-Disclosure Agreement
- **Rules of Engagement**
- Service Level Agreement

Unattempted

Rules of engagement (ROE)are the formal permissions to conduct a penetration test. They provide certain rights and restrictions to the test team for performing the test and help testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.

30. Question

Therese, a penetration tester, has compromised a server and successfully gained root access. She wants to pivot and pass the traffic undetected over the network and evade any possible Intrusion Detection System.

What will be the best approach?

- Install and use Telnet to encrypt all outgoing traffic from this server.
- Use Alternate Data Streams to hide the outgoing packets from this server.
- **Install Cryptcat and encrypt outgoing packets from this server.**
- Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.

Unattempted

Cryptcat enables users to communicate between two systems and encrypts the communication between them with twofish.

31. Question

This attack occurs when the cybercriminal sends Internet Control Message Protocol (ICMP) broadcast packets to several hosts with a spoofed source Internet Protocol (IP) address that belongs to the targeted machine.

- SYN Flood
- None of the Above
- **Smurf**
- ICMP Flood

Unattempted

A Smurf attack occurs when the cybercriminal sends Internet Control Message Protocol (ICMP) broadcast packets to several hosts with a spoofed source Internet Protocol (IP) address that belongs to the targeted machine. The recipients of these spoofed packets will then respond, and the targeted host will be flooded with those responses. These responses will be sent to the victim's machine since the IP address is spoofed by the cybercriminal. This causes significant traffic to the actual victim's machine, which causes it to crash.

32. Question

Which of the following Open Web Application Security Project (OWASP) implements a web application that is full of known vulnerabilities?

- WebScarab
- WebBugs
- **WebGoat**
- VULN_HTML

Unattempted

WebGoat is a deliberately insecure application that allows interested developers just like you to test vulnerabilities commonly found in Java-based applications that use common and popular open-source components.

33. Question

Password hashes are used to prevent unauthorized access to a web based application. Which of the following cryptographic algorithms would be useful to gain access to the password hashes?

- RSA
- **SHA1**
- AES

Diffie-Helman

Unattempted

Diffie-Hellman is for key exchange while RSA and AES is for encryption and decryption. SHA1 is for hashing.

34. Question

It was reported that someone has caused an information spillage on their computer. You immediately went to the computer, disconnected it from the network, removed the keyboard and mouse, and shut it down. What step in incident handling was implemented?

Containment

Discovery

Recovery

Eradication

Unattempted

The main purpose of containment is to contain the damage and prevent further damage from occurring (as noted in step number two, the earlier incidents are detected, the sooner they can be contained to minimize damage). It's important to note that all of SANS' recommended steps within the containment phase should be taken, especially to "prevent the destruction of any evidence that may be needed later for prosecution." These steps include short-term containment, system back-up, and long-term containment.

35. Question

Which of the following should be reviewed and considered when purchasing a biometric system?

The amount of time and resources necessary to maintain a biometric system.

The amount of time it will take to either accept or reject the biometric data when a user provides identification and authentication information.

The amount of time it will take setting up individual user accounts.

The amount of time it will take to convert biometric data into a template on a smart card.

Unattempted

A biometric system should be able to either accept or reject biometric data in real-time.

36. Question

Which of the following should be reviewed and considered when purchasing a biometric system?

- The amount of time and resources necessary to maintain a biometric system.
- **The amount of time it will take to either accept or reject the biometric data when a user provides identification and authentication information.**
- The amount of time it will take setting up individual user accounts.
- The amount of time it will take to convert biometric data into a template on a smart card.

Unattempted

A biometric system should be able to either accept or reject biometric data in real-time.

37. Question

Which of the following is the role of test automation in security testing?

- **It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.**
- It is an option but it tends to be very expensive.
- Test automation is not usable in security due to the complexity of the tests.
- It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.

Unattempted

Test Automation is the best way to increase the effectiveness, efficiency, and coverage of security testing. An automated testing tool can playback pre-recorded and predefined actions, and compare the results to the expected behavior.

38. Question

Which of the following is the process of concealing information in an ordinary file or message to avoid suspicion.

- All of the Above
- **Steganography**

- Tunneling Protocols
- Altering Log Files

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.

39. Question

An incident investigator asks for a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events does not match up. Which of the following is causing this issue?

- A proper chain of custody was not observed while collecting the logs.
- The security breach was a false positive.
- **The network devices are not all synchronized.**
- The attacker altered or erased events from the logs.

Unattempted

Time synchronization is an important middleware service of distributed systems, amongst which Distributed Intrusion Detection System (DIDS) makes extensive use of time synchronization in particular.

40. Question

Which of the following is/are an example of passive reconnaissance?

- **Wireshark**
- Ping
- **Shodan**
- **Spyse**

Unattempted

Passive reconnaissance is the process of gaining valuable information without alerting the potential victim. An example of passive reconnaissance is reviewing or checking the targeted company's website. Some good

examples of passive reconnaissance are Shodan, Spyse, theHarvester, and Wireshark.

41. Question

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

- Firewall rulesets
- **Passwords**
- Usernames
- File permissions

Unattempted

John the Ripper is often used in the enterprise to detect weak passwords that could put network security at risk, as well as other administrative purposes. The software can run a wide variety of password-cracking techniques against the various user accounts on each operating system and can be scripted to run locally or remotely.

42. Question

Which of the following Nmap command must be used if you want to list all devices in the same network quickly after successfully identifying a server whose IP address is 10.10.0.5?

- nmap -T4 -r 10.10.1.0/24
- **nmap -T4 -F 10.10.0.0/24**
- 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.

43. Question

A large financial company recently hired SIA Global Security’s team of Certified Ethical Hackers to test the security of their network systems. They want to conduct the attack as realistically as possible. They only provide the name of their company. What phase of ethical hacking would the CEH team do?

- Escalation
- Scanning
- Enumeration
- **Reconnaissance**

Unattempted

Reconnaissance or footprinting is the preliminary phase or "information gathering" phase of ethical hacking. It is a crucial element of any successful cyberattack, as this is the phase in which the hacker collects all of the necessary information about the target before executing the attack.

44. Question

The following command net use \targetipc$ "" /u:"" is used for?

- **This command is used to connect as a null session**
- Grabbing the SAM
- Connecting to a Linux computer through Samba.
- Grabbing the etc/passwd file

Unattempted

The null session is one of the most debilitating vulnerabilities faced by Windows. Null sessions can be established through ports 135, 139, and 445.

45. Question

Under which of the following conditions does a secondary name server requests a zone transfer from a primary name server?

- When a primary name server has had its service restarted
- When a secondary name server has had its service restarted
- **When a primary SOA is higher than a secondary SOA**
- When a secondary SOA is higher than a primary SOA

Unattempted

Understanding DNS is critical to meeting the requirements of the CEH. When the serial number within the SOA record of the primary server is higher than the Serial number within the SOA record of the secondary DNS server, a zone transfer will take place.

46. Question

A cybercriminal with access to the inside network of a small company launches a successful STP manipulation attack. What will be the next move?

- The cybercriminal will repeat the same attack against all L2 switches of the network.
- The cybercriminal will repeat this action so that it escalates to a DoS attack.
- **The cybercriminal will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.**
- The cybercriminal will activate OSPF on the spoofed root bridge.

Unattempted

After launching a successful STP manipulation attack, the next step should be creating a SPAN entry on the spoofed root bridge and redirecting the traffic to the cybercriminal's computer.

47. Question

A cybercriminal gains access to a web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The cybercriminal did this by entering information into the Web site's user login page that the software's designers did not expect to be entered. Which of the following software design problem is being described?

- Insufficient database hardening
- **Insufficient input validation**
- Insufficient exception handling
- Insufficient security management

Unattempted

The most common web application security weakness is the failure to properly validate input coming from the client or from the environment before using it. This weakness leads to almost all of the major vulnerabilities in web applications, such as cross-site scripting, SQL injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows.

48. Question

Which of the following is an effect of having low humidity in a data center?

- Heat
- Airborne contamination
- Corrosion
- **Static electricity**

Unattempted

High humidity in data servers causes corrosion while low humidity causes static electricity.

49. Question

Which of the following does not belong to the group?

- Gaining Access
- **Blocking**
- Clearing and Covering Tracks
- Scanning

Unattempted

Phases of Ethical Hacking

1. Reconnaissance
2. Scanning and Enumeration
3. Gaining Access
4. Maintaining Access

Clearing and Covering Tracks

50. Question

In this cryptography attack method, the cybercriminal makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions?

- Ciphertext-only attack

- Chosen-plaintext attack
- Known-plaintext attack
- **Adaptive chosen-plaintext attack**

Unattempted

In Adaptive chosen-plaintext attack, the cybercriminal has a complete access to the plaintext message including its encryption, and he/she can also modify the content of the message by making series of interactive queries, choosing subsequent plaintext blocks based on the information from the previous encryption queries and functions. To perform this attack, an attacker needs to interact with the encryption device.

51. Question

In 2014, the Heartbleed bug was discovered. It is widely referred to as MITRE's Common Vulnerabilities and Exposures (CVE) as or CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520. What type of key does this bug leave making exploitation of any compromised system very easy?

- **Private**
- Root
- Public
- Shared

Unattempted

The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form of post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service. An attack may also reveal the private keys of compromised parties.

52. Question

This tool would most likely be used in performing a security audit on various forms of network systems?

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

- Protocol analyzer

Unattempted

Vulnerability scanning is a method used in checking whether a system is exploitable or not 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.

53. Question

ping -c 5 192.168.1.2 is an example of?

- Enumeration
- Gaining Access
- **Active Reconnaissance**
- Passive Reconnaissance

Unattempted

Ping is an example of active reconnaissance used to find out whether the destination host is reachable or not.

54. Question

Jane, a penetration tester from SIA Global Security, has gained physical access to a Windows 2008 R2 server which has an accessible disc drive. She tried booting the server and logging in but was unable to guess the password. Since she has an Ubuntu 9.10 Linux LiveCD, which of the following Linux-based tool can change any user's password or to activate disabled Windows accounts?

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

Unattempted

chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8, and 8.1. It edits the SAM database where Windows stores password hashes.

55. Question

Which of the following programming languages is most vulnerable to buffer overflow attacks?

- Perl
- **C++**
- Java
- Python

Unattempted

Avoid Using C and C++ Languages. C/C++ are high-level programming languages that are vulnerable to buffer overflow attacks. Use other programming languages such as Python, Java, and COBOL since these languages don't allow direct memory access.

56. Question

Paul, a penetration tester from SIA Global Security, was hired to do a penetration test from inside the network of a private company. There was no information given to him about the network. What type of test is being conducted?

- Internal Whitebox
- External, Blackbox
- External, Whitebox
- **Internal, Blackbox**

Unattempted

A blackbox testing is where the black-box tester is unaware of the internal structure of the application to be tested.

57. Question

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

- Nmap
- Traceroute

- Spyse
- Ping

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.

58. Question

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

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

Unattempted

IPsec is a group of networking protocols used for setting up secure encrypted connections, such as VPNs, across publicly shared networks.

59. Question

Which of the following statements about ethical hacking is incorrect?

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

Unattempted

Ethical hackers use the same methods and techniques, including those that have the potential of exploiting vulnerabilities, to test and bypass a system's defenses as their less-principled counterparts, but rather than

taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.

60. Question

What is the location of kernel log in Unix System?

- /message/log
- **/var/log**
- /var/lib/log
- /etc/var/log

Unattempted

In Linux, logs are stored in /var/log.

61. Question

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

- Insecure Deserialization Attack
- Injection Attack
- **Broken Authentication Attack**
- Cross-site scripting Attack (XSS)

Unattempted

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.

62. Question

It is a type of malware where it disguises itself as something that it isn't and often masquerades as a legitimate application.

- Botnet
- Worms
- **Trojan**
- Virus

Unattempted

A Trojan is a type of malware in which it disguises itself as something that it isn't. Trojans often masquerades as a legitimate application, file, or seemingly harmless program to trick its victims into installing it.

63. Question

What risk is present if a recent nmap scan shows that port 69 is open?

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

Unattempted

Trivial File Transfer Protocol (TFTP) runs on port 69. TFTP allows transferring of files without authentication.

64. Question

This is defined as the phonebook of the internet.

- SNMP
- SMTP
- NTP
- **DNS**

Unattempted

DNS or domain name server is the phonebook of the internet. DNS enumeration provides usernames, computer names, and IP addresses of the target systems.

65. Question

What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

- ISO 26029
- Blue Book
- **Common Criteria**
- The Wassenaar Agreement

Unattempted

Common Criteria (often abbreviated as CC) is an international set of standardized guidelines and specifications that were developed to evaluate information security products. Specifically, Common Criteria ensures that certified products meet an agreed-upon security standard for government deployments.

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 →

SkillCertPro

Quick Links

ABOUT US

FAQ

BROWSE ALL PRACTICE TESTS

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy