SALE IS ON | BUY 2 & GET ADDITIONAL 25% OFF | Use Coupon - FLASHSALE

SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 5

Your results are here!! for" CEHv11 Practice Test 5 "

0 of 55 questions answered correctly

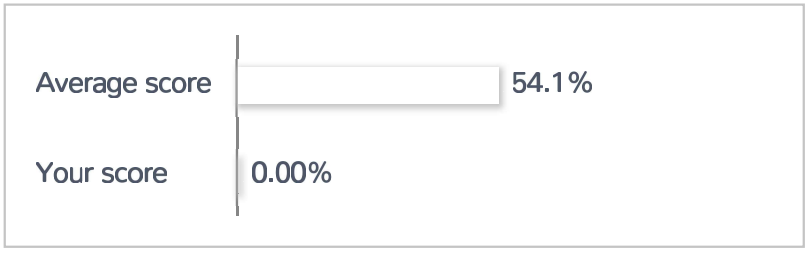
Your time: 00:00:02

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

Correct Incorrect

Review Question Summary

1. Question

Which of the following threats can policies, procedures, and end-user training help to effectively mitigate?

- Man-in-the-middle attacks
- Attempted DDoS attacks
- Zero-day attacks
- **Social engineering attempts**

Unattempted

OBJ-4.2: Social engineering attempts occur when someone uses something like: phishing (they are attempting to receive your personal information and look legitimate), pretexting (basically they give you a scenario and expect you to react quickly), tailgating (following too closely into a door they aren't allowed in), and many other situations. Proper policies, procedures, and educating your users on the dangers posed by social engineering could prevent them from becoming a victim of a phishing attack, as well as many other attacks.

2. Question

Which of the following might be exploited on a Linux server to conduct a privilege escalation?

- DLL hijacking
- **Insecured sudo**
- Cpassword
- Kerberoasting

Unattempted

OBJ-5.2: An insecure sudo vulnerability could allow an attacker to circumvent protections and execute commands that would normally require a password, resulting in privilege escalation. Kerberoasting,

Cpassword, and DLL hijacking are Windows-specific privilege escalation techniques.

3. Question

If you cannot ping a target because you are receiving no response or a response that states the destination is unreachable, then ICMP may be disabled on the remote end. If you wanted to elicit a response from a host using TCP, what tool would you use?

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

Unattempted

OBJ-2.2: Hping is a handy little utility that assembles and sends custom ICMP, UDP, or TCP packets and then displays any replies. It was inspired by the ping command but offered far more control over the probes sent. It also has a handy traceroute mode and supports IP fragmentation. Hping is particularly useful when trying to traceroute/ping/probe hosts behind a firewall that blocks attempts using the standard utilities. Hping also allows you to map out firewall rule sets. It is also great for learning more about TCP/IP and experimenting with IP protocols. Hping does not support IPv6, though, so the NMAP creators have created Nping to fill this gap and serve as an updated variant of Hping. Traceroute and tracert are computer network diagnostic commands for displaying the route and measuring packets' transit delays across an Internet Protocol network. Traceroute uses ICMP and not TCP. Broadcast ping is simply pinging the subnet's broadcast IP using the ping command, but if a regular ping does not work, neither will a broadcast ping. Ptunnel is an application that allows you to reliably tunnel TCP connections to a remote host using ICMP echo request and reply packets, commonly known as ping requests and replies. Ptunnel is used as a covert channel, not to elicit a response from a host using TCP.

4. Question

Which of the following types of attackers are sophisticated and highly organized people or teams typically sponsored by a nation-state?

- Ethical hacker
- Hacktivists
- Script kiddies

Advanced Persistent Threat

Unattempted

OBJ-3.3: Advanced Persistent Threat (APT) attackers are sophisticated and have access to financial and technical resources typically provided by a government. An APT is an attacker with the ability to obtain, maintain, and diversify access to network systems using exploits and malware. A hacktivist is an attacker that is motivated by a social issue or political cause. A script kiddie has little skill or sophistication and uses publicly available tools and techniques. An ethical hacker specializes in penetration testing and in other testing methodologies that ensure the security of an organization's information systems. An ethical hacker is also known as a white hat hacker.

5. Question

A penetration tester wants to install an integrated platform for testing web applications. The software should allow them to capture, analyze, and manipulate HTTP traffic. Which of the following tools should they install?

SET

Kismet

Proxychains

Burp suite

Unattempted

OBJ-5.2: Burp Suite is an integrated platform included for testing web applications' security by acting as a local proxy so that the attacker can capture, analyze, and manipulate HTTP traffic. SET (Social Engineer Toolkit) is an open-source penetration testing framework included with Kali Linux that supports social engineering to penetrate a network or system. Kismet is an 802.11 Layer 2 wireless network detector, sniffer, and intrusion detection system included with Kali Linux. Proxychains is a command-line tool that enables pen testers to mask their identity and/or source IP address by sending messages through intermediary or proxy servers. Censys is a search engine that returns information about the types of devices connected to the Internet.

6. Question

During her login session, Sally is asked by the system for a code sent to her via text (SMS) message. Which of the following concerns should she raise to her organization's AAA services manager?

SMS should be paired with a third factor

- SMS is a costly method of providing a second factor of authentication
- SMS should be encrypted to be secure
- **SMS messages may be accessible to attackers via VoIP or other systems**

Unattempted

OBJ-4.1: NIST's SP 800-63-3 recommends that SMS messages be deprecated as a means of delivering a second factor for multifactor authentication because they may be accessible to attackers. SMS is unable to be encrypted (at least without adding additional applications to phones). A third factor is typically not a user-friendly recommendation and would be better handled by replacing SMS with the proposed third factor. SMS is not a costly method since it can be deployed for less than $20/month at scale.

7. Question

Which of the following threats to a SaaS deployment would be the responsibility of the consumer to remediate?

- SQL injections
- **An endpoint security failure**
- Cross-site scripting
- Unpatched operating systems on the server

Unattempted

OBJ-8.1: In a SaaS model, the consumer has to ensure that the endpoints being used to access the cloud are secure. Since the consumer owns the endpoint (laptop, desktop, tablet, smartphone, etc.), they are responsible for securing it. The entire concept behind using a SaaS product is that the service provider will patch the servers' underlying operating systems, create secure software that isn't vulnerable to SQL injection or cross-site scripting attacks, and ensure proper operations and maintenance of the backend systems.

8. Question

An analyst reviews a triple-homed firewall configuration that connects to the internet, a private network, and one other network. Which of the following would best describe the third network connected to this firewall?

- NIDS
- Subnet
- GPO

DMZ

Unattempted

OBJ-4.5: A triple-homed firewall connects to three networks internal (private), external (internet/public), and the demilitarized zone (DMZ). The demilitarized zone (DMZ) network hosts systems that require access from external hosts. Group Policy Object (GPO) is a collection of Group Policy settings that defines what a system looks like and how it behaves for a defined group of users. A network intrusion detection system (NIDS) is a system that attempts to detect hacking activities, denial of service attacks, or port scans on a computer network or a computer itself. A subnet is a logical subdivision of an IP network.

9. Question

You are planning an engagement with a new client. Which target type should be selected to simulate an APT?

External

On-site

Third-party hosted

Internal

Unattempted

OBJ-3.3: An advanced persistent threat (APT) is a threat that uses multiple attack vectors to gain unauthorized access to sensitive resources. APTs are often funded by nation-states and used for intelligence-gathering operations against the government, military, and commercial networks. In general, APT attacks as an external target type.

10. Question

You are logged into the Windows command prompt and want to find what systems are alive in a portion of a Class B network (172.16.0.0/24) using ICMP. What command would best accomplish this?

for /L %X in (1 1 254) do PING -n 1 172.16.0.%X | FIND /I "Reply"

ping 172.16.0.255

for %X in (1 1 255) do PING 172.16.0.%X

ping 172.16.0.0

Unattempted

OBJ-3.2: The Windows command line does support some fundamental scripting, as shown in this answer. Use an iterative variable to set the starting value (start#) and then step through a set range of values until the value exceeds the set ending value (end#). /L will execute the iterative by comparing start# with end#. If start# is less than end#, the command will execute. When the iterative variable exceeds end#, the command shell exits the loop. You can also use a negative step# to step through a range in decreasing values. For example, (1,1,5) generates the sequence 1 2 3 4 5 and (5,-1,1) generates the sequence (5 4 3 2 1). The syntax is: "for /L %variable in (start# step# end#) do command [CommandLineOptions]."

11. Question

An analyst reviews the logs from the network and notices that there have been multiple attempts from the open wireless network to access the networked HVAC control system. The open wireless network must remain openly available so that visitors can access the internet. How can this type of attack be prevented from occurring in the future?

- Enable WPA2 security on the open wireless network
- Enable NAC on the open wireless network
- Install an IDS to protect the HVAC system
- **Implement a VLAN to separate the HVAC control system from the open wireless network**

Unattempted

OBJ-7.2: A VLAN is useful to segment out network traffic to various parts of the network and stop someone from the open wireless network from logging to the HVAC controls. By utilizing NAC, each machine connected to the open wireless network could be checked for compliance and determine if it is a 'known' machine, but they would still be given access to the entire network. Also, since this is a publicly usable network, using NAC could prevent users from accessing all the network features. An IDS would be a good solution to detect the attempted logins, but it won't prevent them. Instead, an IPS would be required to prevent logins.

12. Question

Which protocol relies on mutual authentication of the client and the server for its security?

- Two-factor authentication
- CHAP
- **LDAPS**

RADIUS

Unattempted

OBJ-2.3: The Lightweight Directory Access Protocol (LDAP) uses a client-server model for mutual authentication. LDAP is used to enable access to a directory of resources (workstations, users, information, etc.). TLS provides mutual authentication between clients and servers. Since Secure LDAP (LDAPS) uses TLS, it provides mutual authentication.

13. Question

Which of the following techniques does a vulnerability scanner use to detect a vulnerability on a specific service?

Analyzing the response received from the service when probed

Banner grabbing

Port scanning

Fuzzing

Unattempted

OBJ-3.1: When a vulnerability scanner analyzes the response received from services during a scan or probe, it can determine if the vulnerability exists on the given service on a particular host. Port Scanning is the name for the technique used to identify open ports and services available on a network host. Fuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports.

14. Question

You are installing a new wireless network in your office building and want to ensure it is secure. Which of the following configurations would create the MOST secure wireless network?

WEP and TKIP

WPA2 and AES

WPA2 and RC4

WPA and MAC filtering

Unattempted

OBJ-6.1: The most secure wireless network configuration utilizes WPA2 with AES encryption. WPA2 is the most secure wireless encryption standard, as it has replaced both WPA and WEP. AES is a robust encryption algorithm that is used by default in the WPA2 standard.

15. Question

During a recent penetration test, it was discovered that your company's wireless network could be reached from the parking lot. The Chief Security Officer has submitted a change request to your network engineering team to solve this issue because he wants to ensure that the wireless network is only accessible from within the building. Based on these requirements, which of the following settings should be changed to ensure the wireless signal doesn't extend beyond your building's interior while maintaining a high level of availability to your users?

- **Power level**
- Frequency
- Channel
- Encryption

Unattempted

OBJ-6.1: The power level should be reduced for the radio transmitter in the wireless access points. With a reduced power level, the signal will not travel as far, which can ensure the signal remains within the building's interior only. The other options, if changed, would affect the availability of the network to the currently configured users and their devices.

16. Question

You are conducting a wireless penetration test against an organization. During your attack, you created an evil twin of their wireless network. Many of the organization's laptops are now connected to your evil twin access point. Which of the following exploits should you utilize next to gather credentials from the victims browsing the internet through your access point?

- Karma attack
- Fragmentation attack
- **Downgrade attack**
- Deauthentication attack

Unattempted

OBJ-6.1: A downgrade attack forces a client to use a weaker SSL version that the attacker can crack. Since the devices are connected through your access point, you can establish a weaker SSL-based HTTPS connection between their web browser and the actual web server they wanted. This forcing of the client to use a weaker version is known as a downgrade attack, and it allows the attacker to capture the packets and later crack them offline since SSL-based HTTPS is weak enough to crack due to vulnerabilities in its design.

17. Question

An independent cybersecurity researcher has contacted your company to prove a buffer overflow vulnerability exists in one of your applications. Which technique would have been most likely to identify this vulnerability in your application during development?

- Static code analysis
- Manual Peer Review
- Pair programming
- Dynamic code analysis

Unattempted

OBJ-5.1: Buffer overflows are most easily detected by conducting a static code analysis. Manual peer review or pair programming methodologies might have been able to detect the vulnerability. Still, they do not have the same level of success as a static code analysis using proper tools. DevSecOps methodology would also improve the likelihood of detecting such an error but still rely on human-to-human interactions and human understanding of source code to detect the fault. Dynamic code analysis also may have detected this if the test found exactly the right condition. Still, again, a static code analysis tool is designed to find buffer overflows more effectively.

18. Question

Which of the following secure coding best practices ensures special characters like <, >, /, and ‘ are not accepted from the user via a web form?

- Input validation
- Error handling
- Session management

Output encoding

Unattempted

OBJ-5.3: Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering a malfunction of various downstream components. Input validation should happen as early as possible in the data flow, preferably as soon as the data is received from the user. Improper error handling can introduce various security problems where detailed internal error messages such as stack traces, database dumps, and error codes are displayed to an attacker. The session management implementation defines the exchange mechanism that will be used between the user and the web application to share and continuously exchange the session ID. Output encoding involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example, translating the < character into the < string when writing to an HTML page.

19. Question

What system contains a publicly available set of databases with registration contact information for every domain name on the Internet?

IETF

IANA

WHOIS

CAPTCHA

Unattempted

OBJ-2.1: WHOIS is a query and response protocol widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. WHOIS also is used for a broader range of information. The protocol stores and delivers database content in a human-readable format and is publicly available for use. The Internet Assigned Numbers Authority is a standards organization that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System, media types, and other Internet Protocol-related symbols and Internet numbers. A CAPTCHA is a type of challenge-response test used in computing to determine whether the user is human. The Internet Engineering Task Force (IETF) is an open standards organization that develops and promotes voluntary Internet standards, particularly the standards that comprise the Internet protocol suite.

20. Question

Your organization has recently migrated to a SaaS provider for its enterprise resource planning (ERP) software. Before this migration, a weekly port scan was conducted to help validate the on-premise systems' security. Which of the following actions should you take to validate the security of the cloud-based solution?

- Utilize a different scanning tool
- Utilize a VPN to scan inside the vendor's security perimeter
- **Utilize vendor testing and audits**
- Utilize a third-party contractor to conduct the scans

Unattempted

OBJ-8.1: The best option is to utilize vendor testing and audits in a cloud-based environment. Most SaaS providers will not allow customers to conduct their own port scans or vulnerability scans against the SaaS service. This means you cannot scan using a VPN connection, utilize different scanning tools, or hire a third-party contractor to scan on your behalf.

21. Question

Which of the following a characteristic of a Blind SQL Injection vulnerability?

- Application properly filters the user input but it is still vulnerable to code injection in a blind attack
- Administrator of the vulnerable application cannot see the request to the webserver
- **An attacker cannot see any of the display errors with information about the injection during a blind attack**
- Administrator of the affected application does not see an error message during a successful attack

Unattempted

OBJ-5.3: Blind SQL injection is a type of SQL injection attack that asks the database true or false questions and determines the answer based on the application's response. This attack is often used when the web application is configured to show generic error messages but has not mitigated the code that is vulnerable to SQL injection.

22. Question

Which of the following are valid concerns when migrating to a serverless architecture? (SELECT THREE)

- **Dependency on the cloud service provider**

- [ ] Management of physical servers
- [ ] Management of VPC offerings
- [ ] **Protection of endpoint security**
- [ ] Patching of the backend infrastructure
- [ ] Limited disaster recovery options

Unattempted

OBJ-8.1: Serverless is a modern design pattern for service delivery. With serverless, all the architecture is hosted within a cloud, but unlike "traditional" virtual private cloud (VPC) offerings, services such as authentication, web applications, and communications aren't developed and managed as applications running on servers located within the cloud. Instead, the applications are developed as functions and microservices, each interacting with other functions to facilitate client requests. There is a heavy dependency on the cloud service provider in a serverless architecture system since all of the back-end infrastructure's patching and management functions are done by them. An organization using such an architecture would still need to prevent compromise of the user endpoints, though the cloud service provider does not manage these. Another concern with serverless architectures is that there are limited options for disaster recovery if service provisioning fails. Patching of backend infrastructure is eliminated because the infrastructure is eliminated with serverless architectures. Once migration is complete, there are no physical servers to manage, which reduces the workload on your system administration teams.

23. Question

Which of the following types of attacks are usually used as part of a man-in-the-middle attack?

- ○ Tailgating
- ○ **Spoofing**
- ○ Brute force
- ○ DDOS

Unattempted

OBJ-4.1: A man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. One example of a MITM attack is active eavesdropping. The attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection. In fact, the entire conversation is controlled by the attacker. The attacker

must intercept all relevant messages passing between the two victims and inject new ones. Spoofing is often used to inject the attacker into the conversation path between the two parties.

24. Question

Which of the following open source tools a penetration tester to conduct vulnerability scans against a company's infrastructure?

- Peach
- **OpenVAS**
- CeWL
- Wireshark

Unattempted

OBJ-3.1: OpenVAS (Open Vulnerability Assessment System) is an open-source software framework for vulnerability scanning and management that can scan for vulnerabilities, misconfigurations, default passwords, and susceptibility to denial of service (DoS) attacks. Wireshark is an open-source network protocol analyzer used to sniff many traffic types, re-create entire TCP sessions, and capture copies of files transmitted on the network. Peach is a dynamic application security testing tool used to conduct fuzzing. CeWL is a Ruby app that crawls websites to generate word lists that can be used with password crackers such as John the Ripper.

25. Question

Jason is conducting a physical penetration test against a company. His objective is to enter the server room that is protected by a lock using a fingerprint reader. Jason attempts to use his finger to open the lock several times without success. He then turns his finger 45 degrees to the left, and the lock authenticates him. What is MOST likely the reason the lock opened?

- The biometric lock is set to fail closed after five invalid attempts
- **The crossover error rate is tuned towards false positives**
- The crossover error rate is tuned towards true negatives
- The biometric lock is set to fail open after five invalid attempts

Unattempted

OBJ-3.2: A biometric lock is difficult to bypass unless the installer incorrectly configures it. If the biometric lock has a high false acceptance rate, it will allow unauthorized people to open the door. The crossover error rate (CER) is the point where the false acceptance and false rejection rates are equal. When charted on a graph, this point can lean more towards accepting false positives or rejecting true positives. If it leans more towards accepting false positives, the sensitivity has decreased to allow less frustration for its users.

26. Question

During scanning and enumeration, you have identified that a port 69 is open on a server. Which fo the following risks exist on this server?

- Unauthenticated access to the server
- Web portal informationn disclosure
- Weak SSL cipher implementation
- Cleartext log ins are accepted

Unattempted

OBJ-2.3: Trivial File Transfer Protocol (TFTP) uses port 69. TFTP allows a client to get a file from or put a file onto a remote host. TFTP has no login or access control mechanisms, therefore if it is used it could allow unauthenticated access to the server.

27. Question

Which of the following provides accounting, authorization, and authentication via a centralized privileged database, as well as challenge/response and password encryption?

- TACACS+
- ISAKMP
- Network access control
- Multi-factor authentication

Unattempted

OBJ-1.1: TACACS+ is a AAA (accounting, authorization, and authentication) protocol to provide AAA services for access to routers, network access points, and other networking devices.

28. Question

Which attack utilizes a wireless access point made to look as if it belongs to the network to eavesdrop on the wireless traffic?

- Evil twin
- WEP attack
- Rogue access point
- Wardriving

Unattempted

OBJ-6.1: An evil twin is meant to mimic a legitimate hotspot provided by a nearby business, such as a coffee shop that provides free Wi-Fi access to its patrons. The evil twin is the wireless LAN equivalent of the phishing scam. This type of attack may be used to steal the passwords of unsuspecting users by monitoring their connections or phishing, which involves setting up a fraudulent web site and luring people there.

29. Question

Which of the following is the MOST dangerous type of threat when using virtualization?

- VM escape
- Rogue VM
- VM sprawl
- Virtual NIC duplication

Unattempted

OBJ-8.1: VM escape refers to malware running on a guest OS jumping to another guest or the host. As with any other software type, it is vital to keep the hypervisor code up-to-date with patches for critical vulnerabilities. VM escape is the biggest threat to virtualized systems.

30. Question

Your team is developing an update to a piece of code that allows customers to update their billing and shipping addresses in the web application. The shipping address field used in the database was designed with a limit of 75 characters. Your team's web programmer has brought you some algorithms that may help prevent an attacker from trying to conduct a buffer overflow attack by submitting invalid input to the shipping address field. Which pseudo-code represents the best solution to prevent this issue?

- if (shippingAddress = 75) {update field} else exit
- if (shippingAddress >= 75) {update field} else exit
- **if (shippingAddress <= 75) {update field} else exit**
- if (shippingAddress != 75) {update field} else exit

Unattempted

OBJ-5.2: To ensure that the field is not overrun by an input that is too long, input validation must occur. Checking if the shipping address is less than or equal to 75 characters before updating the field will prevent a buffer overflow from occurring in this program. If the input is 76 characters or more, then the field will not be updated, and the algorithm will exit the function.

31. Question

Which of the following is the biggest weakness with ICS and SCADA systems in a network?

- ICS/SCADA must be connected to the internet to function
- **These systems are difficult to retofit with modern security**
- They are patched using standard vendor OS patches
- Cybersecurity experts don't know how to secure ICS/SCADA

Unattempted

OBJ-7.2: Industrial control system (ICS) and supervisory control and data acquisition (SCADA) systems were developed many years before security standards were established and integrated into their design. Many of these older systems date back to the 1970s and are still in use today. Over time, these systems were incorporated into the organization's TCP/IP data networks, which provides a huge exploitation area by penetration testers and attackers alike. Many ICS and SCADA vendors are slow to implement security measures since they cannot be easily retrofitted with the newer security required. Therefore, ICS and SCADA systems should ALWAYS be isolated from production networks and segmented into their own logical network. For example, some ICS/SCADA systems use a proprietary operating system. More modern ICS/SCADA operates using a version of Windows. However, many still use Windows XP, making them much more vulnerable since they cannot be upgraded to Windows 10 without hardware replacement.

32. Question

Mallory is unhappy with her job at a large beverage company. She decides to steal sensitive information about the company's proprietary formula for a new energy drink. She installs a keylogger onto some of the product

team's workstations, which then emails out the information to her personal email account each evening so she can post the information to WikiLeaks. How would you best classify Mallory and her actions?

- DoS
- **Insider threat**
- Logic bomb
- Social engineering

Unattempted

OBJ-4.2: Mallory is considered an insider threat in this scenario. An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data, and computer systems. Regardless of her method of stealing the information, the key to this question resides in the fact that she is an employee of the company doing something malicious.

33. Question

Which of the following port or ports does SIP use?

- **5060/5061**
- 389/636
- 443
- 135/139/445

Unattempted

OBJ-2.3: SIP works with other protocols over 5060/5061. 443 is HTTPS, 389/636 is LDAP, and 135/139/445 is NetBIOS and SMB.

34. Question

You want to exploit the NETBIOS name service on a Windows-based network. Which of the following tools should you use?

- Arpspoof
- **Responder**

- Nessus
- John the Ripper

Unattempted

OBJ-4.4: Responder provides a fake server and relay tool that is included with Kali Linux. It responds to LLMNR, NBT-NS (NETBIOS), POP, IMAP, SMTP, and SQL queries to recover sensitive information such as user names and passwords. Responder is configured to listen for LLMNR/NBNS queries and respond with itself as the desired destination. When the client then tries to connect, it prompts the user to log on based on the client's protocol, thus harvesting the user's credentials.

35. Question

Riaan's company runs critical web applications. During a vulnerability scan, Riaan found a serious SQL injection vulnerability in one of their web applications. The system cannot be taken offline to remediate the vulnerability. Which of the following compensating controls should Riaan recommend using until the system can be remediated?

- IPS
- Vulnerability scanning
- **WAF**
- Encryption

Unattempted

OBJ-5.3: WAF (web application firewall) is the best option since it can serve as a compensating control and protect against web application vulnerabilities like an SQL injection until the application can be fully remediated. Vulnerability scanning could only be used to detect the issue. Therefore, it is a detective control, not a compensating control. Encryption would not be effective in stopping an SQL injection. An IPS is designed to protected network devices based on ports, protocols, and signatures. It would not be effective against an SQL injection and is not considered a compensating control for this vulnerability.

36. Question

As a cybersecurity analyst conducting vulnerability scans, you have just completed your first scan of an enterprise network comprising over 10,000 workstations. As you examine your findings, you note that you have less than 1 critical finding per 100 workstations. Which of the following statement does BEST explain these results?

- The scanner was not compatible with the devices on your network
- **An uncredentialed scan of the network was performed**
- The scanner failed to connect with the majority of workstations
- The network has an exceptionally strong security posture

Unattempted

OBJ-3.1: Uncredentialed scans are generally unable to detect many vulnerabilities on a device. When conducting an internal assessment, you should perform an authenticated (credentialed) scan of the environment to most accurately determine the network's vulnerability posture. In most enterprise networks, if a vulnerability exists on one machine, it also exists on most other workstations since they use a common baseline or image. If the scanner failed to connect to the workstations, an error would have been generated in the report.

37. Question

What type of cloud service would provide you with a complete development and deployment environment in the cloud for you to create customized cloud-based apps?

- SaaS
- IaaS
- **PaaS**
- DaaS

Unattempted

OBJ-8.1: Platform as a service (PaaS) is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications. You purchase the resources you need from a cloud service provider on a pay-as-you-go basis and access them over a secure Internet connection. PaaS includes infrastructure (servers, storage, and networking) and middleware, development tools, business intelligence (BI) services, database management systems, and more. PaaS allows you to avoid the expense and complexity of buying and managing software licenses, the underlying application infrastructure and middleware, container orchestrators, or the development tools and other resources. You manage the applications and services you develop, and the cloud service provider typically manages everything else.

38. Question

Which of the following vulnerability scans would provide the best results if you want to determine if the target's configuration settings are correct?

- Credentialed scan
- External scan
- Internal scan
- Non-credentialed scan

Unattempted

OBJ-3.1: Credentialed scans log into a system and retrieve their configuration information. Therefore, it should provide you with the best results. Non-credentialed scans rely on external resources for configuration settings that can be altered or incorrect. The scanner's network location does not directly impact the ability to read the configuration information, so it would not make a difference if you conducted an external or internal scan.

39. Question

Your smartphone begins to receive unsolicited messages while eating lunch at the restaurant across the street from your office. What might cause this to occur?

- Geotagging
- Bluesnarfing
- Packet sniffing
- Bluejacking

Unattempted

OBJ-6.1: Bluejacking sends unsolicited messages over Bluetooth to Bluetooth-enabled devices such as smartphones and tablets. On the other hand, Bluesnarfing involves taking data from a smartphone or tablet over Bluetooth without permission. Bluetooth has a limited range, so the attacker is likely within 10 meters of the victimized device. Geotagging involves embedded the geolocation coordinates into a piece of data (normally a photo or video). Packet sniffing is a passive method of collecting network traffic for follow-on analysis at a later time.

40. Question

Jennifer decided that the licensing cost for a piece of video editing software was too expensive. Instead, she decided to download a keygen program to generate her own license key and install a pirated version of the editing software. After she runs the keygen, a license key is created, but her system performance becomes very sluggish, and her antimalware suite begins to display numerous alerts. Which type of malware might her computer be infected with?

- Trojan
- Logic bomb
- Adware
- Worm

Unattempted

OBJ-3.3: A trojan is a program in which malicious or harmful code is contained inside an apparently harmless program. In this example, the harmless program is the key generator (which does create a license key). It also has malicious code inside it (causing the additional alerts from the antimalware solution). Likely, this keygen has an embedded virus or remote access trojan (RAT) in its programming.

41. Question

Keith wants to validate the application file that he downloaded from the vendor of the application. Which of the following should he compare against the file to verify the integrity of the downloaded application?

- MD5 or SHA1 hash digest of the file
- File size and file creation date
- Public key of the file
- Private key of the file

Unattempted

OBJ-9.1: Keith should conduct a hash of the downloaded file and compare it against the MD5 hash digest listed on the server of this file. This file needs to be a verifiable MD5 hash file to validate the file integrity has not been compromised during the download. This is an important step to ensure the file was not modified in transit during the download. The other options are insufficient to guarantee the integrity of the downloaded file since integrity checking relies on comparing hash digests. A public or private key would not be assigned solely to a single file, nor do they provide integrity on their own. Public and private keys are used to ensure data confidentiality, whereas a hash digest ensures integrity. The file size and file creation date are additional

forms of metadata that could help validate a file's integrity. Still, they of a much lower quality and trust factor than using a hash digest. Therefore MD5 or SHA1 is a better choice.

42. Question

Which of the following ports are used to provide secure remote connection sessions over the Internet?

- 22
- 23
- 25
- 80

Unattempted

OBJ-2.2: Port 22 is used by Secure Shell (SSH) to securely create communication sessions over the Internet for remote access to a server or system. Telnet used to be used over port 23, but it is insecure and doesn't provide an encrypted tunnel like SSH does. Port 25 is for SMTP, and Port 80 is for HTTP, neither of which provide an encrypted tunnel, either.

43. Question

You have been contracted to conduct a wireless penetration test for a corporate client. Which of the following should be documented and agreed upon in the scoping documents before you begin your assessment?

- The make and model of the wireless access points used by the client
- **The frequencies of the wireless access points and devices used by the client**
- The number of wireless access points and devices used by the client
- The network diagrams with the SSIDs of the wireless access points used by the client

Unattempted

OBJ-6.1: To ensure you are not accidentally targeting another organization's wireless infrastructure during your penetration test, you should have the frequencies of the wireless access points and devices used by the client documented in the scoping documents. This would include whether your clients use Wireless A, B, G, N, or AC and if they are using the 2.4 GHz or 5.0 GHz spectrum if they are using Wireless N or AC.

44. Question

A client is concerned about a hacker compromising a network to gain access to confidential research data. What could be implemented to redirect any attackers on the network?

- Honeypot
- Botnet
- DMZ
- Content filter

Unattempted

OBJ-4.5: A honeypot is a computer security mechanism set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data that appears to be a legitimate part of the site but is actually isolated and monitored and seems to contain information or a resource of value to attackers, who are then blocked.

45. Question

Which device actively defends the network by detecting threats and shutting down ports or changing configurations to prevent attacks?

- IPS
- Firewall
- IDS
- Honeypot

Unattempted

OBJ-4.5: Intrusion Protection Systems (IPS) can reconfigure themselves based on the threats experienced. Firewalls maintain a static configuration.

46. Question

You are conducting a penetration test and planning to use a cross-site scripting attack. During your reconnaissance, you determined that the system performs input validation using REGEX to prevent any strings that contain the term "[Ss][Cc][Rr][Ii][Pp][Tt]" in the input. To bypass this input validation, which of the following variations of the script tag should you utilize?

- <SCRIPT>

- <script>
- **<%53CRIPT>**
- <$cript>

Unattempted

OBJ-4.5: Since cross-site scripting (XSS) relies on the HTML tags to launch, the system administrators had a good idea of creating input validation using a REGEX for those keywords. Unfortunately, they forgot to include a more inclusive version of this REGEX to catch all variants. For example, simply using [Ss][Cc][Rr][Ii][Pp][Tt] would have been much more secure, but even this would miss %53CRIPT would evade this filter. To catch all the letter S variants, you would need to use [%53%%73Ss], which includes the capital S in hex code, the lower case s in hex code, the capital S, and the lowercase s. As a penetration tester, it is important to remember that you can evade weak input validation using ASCII encoded characters, like %53 for the S character. As a cybersecurity analyst, you must build good input validations into your systems to prevent these types of attacks.

47. Question

An employee contacts the service desk because they cannot open an attachment they receive in their email. The service desk agent conducts a screen sharing session with the user and investigates the issue. The agent notices that the attached file is named Invoice1043.pdf, and a black pop-up window appears and then disappears quickly when the attachment was double-clicked. Which of the following is most likely causing this issue?

- **The attachment is using a double file extension to mask its identity**
- The user doesn't have a PDF reader installed on their computer
- The email is a form of spam and should be deleted
- The file contains an embedded link to a malicious website

Unattempted

OBJ-3.3: The message contains a file attachment hoping that the user will execute or open it. The attachment's nature might be disguised by formatting tricks such as using a double file extension, such as Invoice1043.pdf.exe, where the user only sees the first extension since .exe is a known file type in Windows. This would explain the black popup window that appears and then disappeared, especially if the exe file was running a command-line tool. This file is most likely not a PDF, so there is no need for a PDF reader. Additionally, most modern web browsers, such as Chrome and Edge, can open PDF files by default for the user. The file would not contain an embedded link since an embedded link is another popular attack

vector that embeds a link to a malicious site within the email body, not within the file. This email is likely not spam and would be better categorized as a phishing attempt instead.

48. Question

A penetration test tester conducts an ACK scan using nmap against the external interface of a DMZ firewall. Nmap reports port 80 as "unfiltered". What type of packet inspection is the firewall performing?

- Host inspection
- Stateful inspection
- Application-level inspection
- **Stateless inpsection**

Unattempted

OBJ-2.2: The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed. Only the ACK scan, which is used to map firewall rulesets, classifies ports into this state. Based on the unfiltered port state, the firewall must be performing stateless inspection. Stateless firewalls watch network traffic, and restrict or block packets based on source and destination addresses or other static values. They are not 'aware' of traffic patterns or data flows. A stateless firewall uses simple rule-sets with ACLs.

49. Question

You are conducting a penetration test against an organization. You have captured the legitimate authentication handshake between a client and a server. Later in the day, you retransmit that session while spoofing your MAC address to that of the client. Which of the following exploits are you using?

- Fragementation attack
- **Replay attack**
- Downgrade attack
- Relay attack

Unattempted

OBJ-4.1: A replay attack repeats a legitimate transmission in a malicious context. For example, a user might send their authentication information to a client or system; the attacker who eavesdrops on this communication can use the authentication in a later transmission, essentially impersonating the victim. In

wireless networking, replaying transmissions can be used to enable several different attacks. Do not confuse a replay attack with a relay attack. In a replay attack, a legitimate network packet or frame is retransmitted repeatedly. In a relay attack, an attacker inserts themselves man-in-the-middle style between two devices, intercepting and forwarding traffic between them.

50. Question

An attacker uses the nslookup interactive mode to locate information on a Domain Name Service (DNS). What command should they type to request the appropriate records for only name servers?

- **set type=ns**
- request type=ns
- locate type=ns
- transfer type=ns

Unattempted

OBJ-2.1: The “set type=ns” tells nslookup only reports information on name servers. If you used “set type=mx” instead, you would receive information only about mail exchange servers.

51. Question

You have just conducted an automated vulnerability scan against a static webpage without any user input fields. You have been asked to adjudicate the scanner's findings in the automated report. Which of the following is MOST likely to be a false positive?

- **Version disclosure of server information**
- Missing secure flag for the site's cookies
- Supports weak cipher suites
- Unencrypted transfer of data

Unattempted

OBJ-5.1: The disclosure of internal server information, such as its version, is a common vulnerability on both static webpages and dynamic webpages. This disclosure can occur during banner grabber or by reviewing the source course of the webpage.

52. Question

Your company has decided to move all of its data into the cloud. Your company is concerned about the privacy of its data due to some recent data breaches that have been in the news. Therefore, they have decided to purchase cloud storage resources that will be dedicated solely for their use. Which of the following types of clouds is your company using?

- **Private**
- Hybrid
- Community
- Public

Unattempted

OBJ-8.1: Private cloud refers to a cloud computing model where IT services are provisioned over private IT infrastructure for the dedicated use of a single organization. A private cloud is usually managed via internal resources. The terms private cloud and virtual private cloud (VPC) are often used interchangeably.

53. Question

Rick is upset that he was passed over for a promotion. He decides to take revenge on his nemesis, Mary, who got the job instead of him. Rick sets up a man-in-the-middle attack against Mary's computer by redirecting any layer 2 traffic destined for the gateway to his own computer first. Rick is careful only to affect the traffic associated with Mary's computer and not the entire network. Which type of man-in-the-middle attack is Rick conducting against Mary?

- Evil twin
- IP spoofing
- **ARP cache poisoning**
- MAC spoofing

Unattempted

OBJ-4.1: Based on the scenario, we can eliminate evil twin (focused on wireless access points) and IP spoofing (since this affects layer 3 traffic). While MAC spoofing the gateway's address might work, it would also affect every computer on this subnet. By conducting an ARP cache poisoning attack, Rick can poison the cache and replace Mary's computer's MAC association with his own, allowing him to become the man-in-the-middle between Mary and the default gateway.

54. Question

Which of the following type of threats did the Stuxnet attack rely on to cross an airgap between a business and an industrial control system network?

- Cross-site scripting
- Session hijacking
- Directory traversal
- **Removable media**

Unattempted

OBJ-7.2: Airgaps are designed to remove connections between two networks to create a physical segmentation between them. The only way to cross an airgap is to have a physical device between these systems, such as using a removable media device to transfer files between them. A directory traversal is an HTTP attack that allows attackers to access restricted directories and execute commands outside of the web server's root directory. Cross-Site Scripting (XSS) attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. A session hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server. A directory traversal, cross-site scripting, or session hijacking attack cannot by itself cross an airgap.

55. Question

During your annual cybersecurity awareness training in your company, the instructor states that employees should be careful about what information they post on social media. According to the instructor, if you post too much personal information on social media, such as your name, birthday, hometown, and other personal details, it is much easier for an attacker to conduct which type of attack to break your passwords?

- Birthday attack
- Brute force attack
- **Cognitive password attack**
- Rainbow table attack

Unattempted

OBJ-3.2: A cognitive password is a form of knowledge-based authentication that requires a user to answer a question, presumably something they intrinsically know, to verify their identity. If you post a lot of personal information about yourself online, this password type can easily be bypassed. For example, during the 2008 elections, Vice Presidential candidate Sarah Palin's email account was hacked because a high schooler used

the “reset my password” feature on Yahoo’s email service to reset her password using the information that was publically available about Sarah Palin (like her birthday, high school, and other such information).

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 →

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

Privacy Policy