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

SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 2

Your results are here!! for" CEHv11 Practice Test 2 "

0 of 50 questions answered correctly

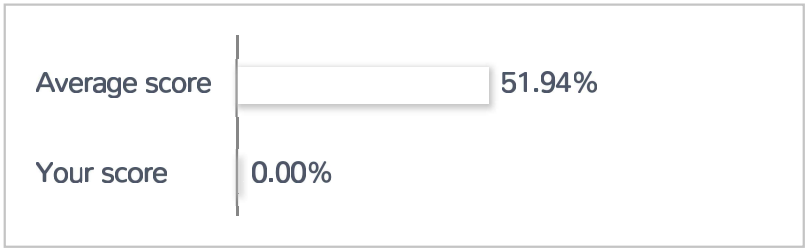
Your time: 00:00:03

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

Correct Incorrect

Review Question Summary

1. Question

A hacker successfully modified the sale price of items purchased through your company's web site. During the investigation that followed, the security analyst has verified the web server, and the Oracle database was not compromised directly. The analyst also found no attacks that could have caused this during their log verification of the Intrusion Detection System (IDS). What is the most likely method that the attacker used to change the items' sale price?

- Cross-site scripting
- SQL injection
- Buffer overflow attack
- **Changing hidden form values**

Unattempted

OBJ-5.2: Since there are no indications in the IDS logs, the database, or the server, it is most likely that the hacker changed hidden form values to change the items' price in the shopping cart. A buffer overflow is an anomaly that occurs when a program overruns the buffer's boundary and overwrites adjacent memory locations while writing data to a buffer. Cross-Site Scripting (XSS) attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in a browser side script, to a different end-user. SQL injection is a code injection technique used to attack data-driven applications. Malicious SQL statements are inserted into an entry field for execution, such as dumping the database contents to the attacker.

2. Question

You have received a laptop from a user who recently left the company. You went to the terminal in the operating system and typed 'history' into the prompt and see the following:

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

> for i in seq 255; ping -c 1 10.1.0.$i; done

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Which of the following best describes what actions were performed by this line of code?

- Attempted to conduct a SYN scan on the network
- Sequentially sent 255 ping packets to every host on the subnet
- Conducted a sequential ICMP echo reply to the subnet
- **Conducted a ping sweep of the subnet**

Unattempted

OBJ-2.2: This code is performing a ping sweep of the subnet 10.1.0.0/24. The code states that for every number in the sequence from 1 to 255, conduct a ping to 10.1.0.x, where x is the number from 1 to 255. When it completes this sequence, it is to return to the terminal prompt (done). The ping command uses an echo request and then receives an echo reply from the ping's target. A ping sweep does not use an SYN scan, which would require the use of a tool like nmap or hping.

3. Question

What type of technique does exploit chaining often implement?

- **Injecting parameters into a connection string using semicolons as a separator**
- Setting a user's session identifier (SID) to an explicit known value
- Inserting malicious JavaScript code into input parameters
- Adding multiple parameters with the same name in HTTP requests

Unattempted

OBJ-3.2: Connection String Parameter Pollution (CSPP) exploits specifically the semicolon-delimited database connection strings that are constructed dynamically based on the user inputs from web applications. CSPP, if carried out successfully, can be used to steal user identities and hijack web credentials. CSPP is a high-risk attack because of the relative ease with which it can be carried out (low access complexity) and the potential results it can have (high impact). Exploit chaining involves multiple commands and exploits being conducted in a series to fully attack or exploit a given target.

4. Question

A new piece of malware attempts to exfiltrate user data by hiding the traffic and sending it over a TLS-encrypted outbound traffic over random ports. What technology would be able to detect and block this type of traffic?

- Intrusion detection system

- Stateless packet inspection
- **Application-aware firewall**
- Stateful packet inspection

Unattempted

OBJ-4.5: A Web Application Firewall (WAF) or Application-Aware Firewall would detect both the accessing of random ports and TLS encryption and identify it as suspicious, whereas Stateless would inspect port number used by the traffic leaving. IDS only analyzes incoming traffic. Therefore it would not be able to see this activity as suspicious.

5. Question

What is not an example of a type of support resource that a pentester might receive as part of a white box assessment?

- Network diagrams
- **PII of employees**
- SOAP project files
- XSD

Unattempted

OBJ-1.1: White box support resources include architectural diagrams, sample application requests, SDK documentation, SOAP project files, Swagger documents, WSDL/WADL, and XML Scheme Definitions (XSD). The PII of employees should not be given to a penetration tester as this could violate laws and regulations regarding maintaining employee data confidentiality and privacy. White-box testing falls on the opposite end of the spectrum from black-box testing, and penetration testers are given full access to source code, architecture documentation, and so forth.

6. Question

Which technique is used with the ProxyChains command to allow a penetration tester to pivot to a new subnet?

- **Modifying routing tables**
- VPN pivoting
- Port forwarding

- SSH pivoting

Unattempted

OBJ-5.2: ProxyChains is a tool that allows a penetration tester to pivot to a new subnet, but it must be combined with the modification of the penetration tester's routing tables on their machine. For example, assume that the exploited client machine is located in the 192.168.5.0/24 subnet, but you need to access a server in the 10.0.0.0/24 subnet. You would then need to "route add 10.0.0.0 255.255.255.0 1" (1 is the ID of your Meterpreter session). Then, you can run "proxychains " to target the new subnet. For example, "proxychains nmap -sT -Pn -p21,23,25,80,443 10.0.0.5" would perform an nmap scan of the targeted server in the new subnet by chaining the connections together using a proxy on the localhost.

7. Question

A penetration tester has exploited an FTP server using Metasploit and now wants to pivot to the organization's LAN. What is the best method for the penetration tester to use to conduct the pivot?

- Set the payload to propagate through meterpreter
- **Create a route statement in meterpreter**
- Reconfigure the network settings in meterpreter
- Issue the pivot exploit and setup meterpreter

Unattempted

OBJ-5.1: Since the penetration tester has exploited the FTP server from outside the LAN, they will need to set up a route statement in meterpreter. Metasploit makes this very simple since it also has an autoroute meterpreter script that will allow us to attack this second network through our first compromised machine (the FTP server) and then create the routes needed.

8. Question

After analyzing and correlating activity from the firewall logs, server logs, and the intrusion detection system logs, a cybersecurity analyst has determined that a sophisticated breach of the company's network security may have occurred from a group of specialized attackers in a foreign country over the past five months. Up until now, these cyberattacks against the company network had gone unnoticed by the company's information security team. How would you best classify this threat?

- Insider threat
- Spear phishing

Privilege escalation

Advanced persistent threat (APT)

Unattempted

OBJ-3.3: An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. An APT attack intends to steal data rather than to cause damage to the network or organization. An APT refers to an adversary's ongoing ability to compromise network security, obtain and maintain access, and use various tools and techniques. They are often supported and funded by nation-states or work directly for a nation-states' government. Spear phishing is the fraudulent practice of sending emails ostensibly from a known or trusted sender to induce targeted individuals to reveal confidential information. An insider threat is a malicious threat to an organization 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. Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. While an APT may use spear phishing, privilege escalation, or an insider threat to gain access to the system, the scenario presented in this question doesn't specify what method was used. Therefore, APT is the best answer to select.

9. Question

Which of the following provides a cryptographic authentication mechanism to positively identify an organization as the authorized sender of email for a particular domain name?

DKIM

SMTP

SPF

DMARC

Unattempted

OBJ-2.1: DomainKeys Identified Mail (DKIM) provides a cryptographic authentication mechanism. This can replace or supplement SPF. To configure DKIM, the organization uploads a public key as a TXT record in the DNS server. Sender Policy Framework (SPF) uses a DNS record published by an organization hosting an email service. The SPF record identifies the hosts authorized to send email from that domain, and there must be only one per domain. SPF does not provide a cryptographic authentication mechanism like DKIM does, though. The Domain-Based Message Authentication, Reporting, and Conformance (DMARC) framework ensures that SPF and DKIM are being utilized effectively. DMARC relies on DKMI for the cryptographic

authentication mechanism, making it the incorrect option for this question. The simple mail transfer protocol (SMTP) is a communication protocol for electronic mail transmission, which does not utilize cryptographic authentication mechanisms by default.

10. Question

Which of the following is the LEAST secure wireless security and encryption protocol?

- WPA2
- WPA
- **WEP**
- AES

Unattempted

OBJ-6.1: Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. It is the oldest form of wireless security and the weakest form. WEP can be cracked with brute force techniques in less than 5 minutes with a normal end-user computer.

11. Question

An attacker is searching in Google for Cisco VPN configuration files by using the filetype:pcf modifier. The attacker could locate several of these configuration files and now wants to decode any connectivity passwords that they might contain. What tool should the attacker use?

- Nessus
- **Cain and Abel**
- Netcat
- Nmap

Unattempted

OBJ-3.2: Cain and Abel is a popular password cracking tool. It can recover many password types using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force, and cryptanalysis attacks. It also includes a module to conduct Cisco VPN

Client Password Decoding too. CUPP is used to create password lists. Nessus is a vulnerability scanner. The netcat tool is used to create reverse shells for remote access.

12. Question

You have determined that your client uses several networked devices that rely on an embedded operating system during your reconnaissance. Which of the following methods would MOST likely be the best method for exploiting these?

- **Use web-based exploits against the devices web interfaces**
- Use a spearphishing campaign to trick a user into installing a RAT
- Use social engineering to trick a user into opening a malicious APK
- Identify a jailbroken device for easy exploitation

Unattempted

OBJ-7.2: Most embedded operating systems use a web interface to access their configurations for setup and installation. Focusing on this web interface and using common web-based exploits is usually one of the best methods of exploiting a device with an embedded OS.

13. Question

What common technique is used by malicious individuals to perform a man-in-the-middle attack on a wireless network?

- Session hijacking
- **Creating an evil twin**
- Amplified DNS attacks
- ARP cache poisoning

Unattempted

OBJ-6.1: Evil Twin access points are the most common way to perform a man-in-the-middle attack on a wireless network. 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.

14. Question

Your organization has been receiving many phishing emails recently, and you are trying to determine why they are effective in getting your users to click on their links. The latest email consists of what looks like an advertisement that is offering an exclusive early access opportunity to buy a new iPhone at a discounted price. Still, there are only 5 phones available at this price. What type of social engineering principle is being exploited here?

- Trust
- Intimidation
- **Scarcity**
- Familiarity

Unattempted

OBJ-4.2: Scarcity is used to create a fear in a person of missing out on a special deal or offer. This technique is used in advertising all the time, such as "supplies are limited," "only available for the next 4 hours", and other such artificial limitations being used.

15. Question

An attacker has issued the following command: nc -l -p 8080 | nc 192.168.1.76 443. Based on this command, what will occur?

- Netcat will listen for a connection from 192.168.1.76 on port 443 and output anything received to port 8080
- Netcat will listen on the 192.168.1.76 interface for 443 seconds on port 8080
- Netcat will listen on port 8080 and then output anything received to local interface 192.168.1.76
- **Netcat will listen on port 8080 and output anything received to a remote connection on 192.168.1.76 port 443**

Unattempted

OBJ-3.2: The proper syntax for netcat (nc) is -l to signify listening and -p to specify the listening port. Then, the | character allows multiple commands to execute during a single command execution. Next, netcat sends the data to the given IP (192.168.1.76) over port 443. This is a common technique to bypass the firewall by sending traffic over port 443 (a secure SSL/TLS tunnel).

16. Question

What remediation strategies are the MOST effective in reducing the risk to an embedded ICS from a network-based compromise? (Select TWO)

- [ ] **Disabling unused services**
- [ ] NIDS
- [ ] **Segmentation**
- [ ] Patching

Unattempted

OBJ-7.2: Segmentation is the best method to reduce the risk to an embedded ICS system from a network-based compromise. Additionally, you could disable unused services to reduce the footprint of the embedded ICS. Many of these embedded ICS systems have a large number of default services running. So, by disabling the unused services, we can better secure these devices. By segmenting the devices off the main portion of the network, we can also better protect them. A NIDS might detect an attack or compromise, but it would not reduce the risk of the attack succeeding since it can only detect it. Patching is difficult for embedded ICS devices since they usually rely on customized software applications that rarely provide updates.

17. Question

What control provides the best protection against both SQL injection and cross-site scripting attacks?

- ( ) CSRF
- ( ) Network layer firewalls
- ( ) Hypervisors
- ( ) **Input validation**

Unattempted

OBJ-5.3: Input validation prevents the attacker from sending invalid data to an application and is a strong control against both SQL injection and cross-site scripting attacks. A network layer firewall is a device that is designed to prevent unauthorized access, thereby protecting the computer network. It blocks unauthorized communications into the network and only permits authorized access based on the IP address, ports, and protocols in use. Cross-site request forgery (CSRF) is another attack type. A hypervisor controls access between virtual machines.

18. Question

What technique is an attacker using if they review data and publicly available information to gather intelligence about the target organization without scanning or other technical information-gathering activities?

- **Passive reconnaissance**
- Patch management
- Active scanning
- Vulnerability scanning

Unattempted

OBJ-2.1: Passive reconnaissance combines publicly available data from various sources about an organization and does not use active scanning or data gathering methods. Vulnerability scanning is an inspection of the potential points of exploitation on a computer or network to identify security holes. A vulnerability scan is usually conducted to detect and classify system weaknesses in computers, networks, and communications equipment and predict the effectiveness of countermeasures. Patch management is the process that helps acquire, test, and install multiple patches (code changes) on existing applications and software tools on a computer, enabling systems to stay updated on existing patches and determining which patches are the appropriate ones.

19. Question

As part of the reconnaissance stage of a penetration test, Kumar wants to retrieve information about an organization's network infrastructure without causing an IPS alert. Which of the following is his best course of action?

- Perform a DNS zone transfer
- Use a nmap stealth scan
- **Perform a DNS brute-force attack**
- Use a nmap ping sweep

Unattempted

OBJ-2.1: The best course of action is to perform a DNS brute-force attack. The DNS brute-force attack queries a list of IPs and typically bypasses IDS/IPS systems that do not alert on DNS queries. A ping sweep or a stealth scan can be easily detected by the IPS, depending on the signatures and settings being used. A DNS zone transfer is also something that often has a signature search for it and will be alerted upon since it is a common attack technique.

20. Question

Which of the following weaknesses exist in WPS enabled wireless networks?

- Utilizes TKIP to secure the authentication handshake
- Utilizes a 24-bit initialization vector
- **Brute force occurs within 11,000 combinations**
- Utilizes a 40-bit encryption key

Unattempted

OBJ-6.1: The most prominent attack against WPS enabled wireless networks involves brute-forcing the 8-digit PIN that client uses to enroll their devices without knowing the pre-shared key. WPS checks each half of the PIN individually, reducing the number of possible combinations from a maximum of 100,000,000 to only 11,000. This only takes a few minutes to crack on most modern computers, as long as the WAP doesn't have a lockout after a certain number of failures. The lockout mechanism may also be triggered based on the client's MAC, so you can often spoof MAC to bypass this defense.

21. Question

A military defense contracting company has hired your company to conduct a penetration test against their networks. Their company has a strong vulnerability management program in place, but they are concerned that they may still be subject to remote hackers' intrusion. They have asked your company to create a red team with their most skilled hackers and conduct a long-term engagement over 6-12 months. The goal of this assessment is to emulate an attacking group that uses stealth while infiltrating the network, quietly maintaining persistence, and slowly exfiltrating data out of the network over time to determine if their cybersecurity analysts could detect this type of threat. Which of the following type of threat actors will your red team need to emulate?

- Script kiddies
- Hacktivists
- Insider threat
- **APT**

Unattempted

OBJ-3.3: An advanced persistent threat (APT) is a type of attacker that keeps a low profile while infiltrating a remote network. Once inside the network, they maintain their patience while gathering intelligence and slowly exfiltrating data out of the network. Many APTs work for a nation-state and focus on intelligence operations. Some APTs also perform corporate espionage to steal highly guarded trade secrets from competitors. APTs commonly use several attack vectors to ensure their success in gaining unauthorized access to information.

22. Question

What kind of attack is an example of IP spoofing?

- ARP poisoning
- SQL injections
- **Man-in-the-middle**
- Cross-site scripting

Unattempted

OBJ-4.1: The man-in-the-middle attack intercepts communications between two systems. For example, in an HTTP transaction, the target is the TCP connection between client and server. Using different techniques, the attacker splits the original TCP connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server. This often uses IP spoofing to trick a victim into connecting to the attack. SQL injection is a code injection technique used to attack data-driven applications. Malicious SQL statements are inserted into an entry field for execution, such as dumping the database contents to the attacker. 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 that they are directly communicating with each other. ARP Poisoning, also known as ARP Spoofing, is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN to change the pairings in its IP to MAC address table. Cross-Site Scripting (XSS) attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in a browser side script, to a different end-user.

23. Question

Which command-line tool could you use on a Windows system to enable an inactive administrator account?

- **net user**

- gpresult
- taskkill
- robocopy

Unattempted

OBJ-3.2: There are several net command utilities that you can use to view and configure shared resources on a Windows network. The net user command allows system administrators to manage user accounts on Windows PCs. You can use the command to display account information or make changes to user accounts. It can be used, among other things, to enable the inactive administrator account of a Windows system.

24. Question

Which of the following ports is used by the Service Location Protocol when organizing and locating printers, databases, and other resources in a network?

- 389
- **427**
- 443
- 445

Unattempted

OBJ-2.3: Port 427 is used by SLP. The Service Location Protocol (SLP) is a protocol or method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. This is an alternative protocol to LDAP in newer networks. While you may not have this port memorized, you should have memorized ports 389, 443, and 445 and identified that they were not associated with printers.

25. Question

Which of the following will an adversary do during the reconnaissance phase of the Lockheed Martin kill chain? (SELECT THREE)

- Select backdoor implants and appropriate command and control mechanisms
- **Harvest email addresses**
- Release of malware on USB drives

- [ ] Acquire or develop zero-day exploits
- [ ] **Identify employees on Social Media networks**
- [ ] **Discover servers facing the public internet**

Unattempted

OBJ-1.1: Passively harvesting information from a target is the main purpose of the reconnaissance phase. Harvesting email addresses from the public internet, identifying employees on social media (particularly LinkedIn profiles), discovering public-facing servers, and gathering other publicly available information can allow an attacker to develop a more thorough understanding of a targeted organization. Acquiring or developing zero-day exploits, selecting backdoor implants, and choosing command and control (C2) mechanisms will require the information gathered during reconnaissance to be effective. Still, these activities will actually occur during the weaponization phase.

26. Question

Which of the following commands can be used to resolve a DNS name to an IP address?

- ○ iplookup
- ○ query
- ○ dns
- ○ **nslookup**

Unattempted

OBJ-2.1: The nslookup command is used for DNS (Domain Name System) lookup operations. It is used to find the IP address of a particular domain name or the domain name of a particular IP address. Host and dig are also commands that can be used to lookup a domain name and convert it to an IP address within a Linux system.

27. Question

What type of wireless security measure can easily be defeated by a hacker by spoofing their network interface card's hardware address?

- ○ WPS
- ○ Disable SSID broadcast
- ○ WEP

MAC filtering

Unattempted

OBJ-4.1: Wireless access points can utilize MAC filtering to ensure only known network interface cards are allowed to connect to the network. If the hacker changes their MAC address to a trusted MAC address, they can easily bypass this security mechanism. MAC filtering is considered a good security practice as part of a larger defense-in-depth strategy, but it won't stop a skilled hacker for long. MAC addresses are permanently burned into the network interface card by the manufacturer and serve as the device's physical address. WEP is the Wired Equivalent Privacy encryption standard, which is considered obsolete in modern wireless networks. WEP can be broken using a brute force attack within just a few minutes by an attacker. Another security technique is to disable the SSID broadcast of an access point. While this prevents the SSID broadcast, a skilled attacker can still find the SSID using discovery scanning techniques. WPS is the WiFi Protected Setup. WPS is used to connect and configure wireless devices to an access point easily.

28. Question

Your company's Security Operations Center (SOC) is currently detecting an ongoing DDoS attack against your network's file server. A cybersecurity analyst has identified forty internal workstations on the network conducting the attack against your network's file server. The cybersecurity analyst believes these internal workstations are infected with malware and places them into a quarantined network area. The analyst then submits a service desk ticket to have the workstations scanned and cleaned of the infection. What type of malware was the workstation likely a victim of based on the scenario provided?

Botnet

Ransomware

Spyware

Rootkit

Unattempted

OBJ-4.3: A botnet is many internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service (DDoS) attacks, steal data, send spam, and allow the attacker to access the device and its connection. A zombie (also known as a bot) is a computer or workstation that a remote attacker has accessed and set up to forward transmissions (including spam and viruses) to other computers on the internet.

29. Question

You work for a bank interested in moving some of its operations to the cloud, but it is worried about security. You recently discovered an organization called CloudBank that was formed by 15 local banks as a way for them to build a secure cloud-based environment that can be accessed by the 15 member banks. Which cloud model BEST describes the cloud created by CloudBank?

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

Unattempted

OBJ-8.1: Community Cloud is another type of cloud computing in which the cloud setup is shared manually among different organizations that belong to the same community or area. A multi-tenant setup is developed using cloud among different organizations belonging to a particular community or group with similar computing concerns. For joint business organizations, ventures, research organizations, and tenders, a community cloud is an appropriate solution. Based on the description of 15 member banks coming together to create the CloudBank organization and its cloud computing environment, a community cloud model is most likely described.

30. Question

What technology is NOT PKI x.509 compliant and cannot be used in various secure functions?

- AES
- PKCS
- **Blowfish**
- SSL/TLS

Unattempted

OBJ-9.1: AES, PKCS, and SSL/TLS are all compatible with x.509 and can be used in a wide variety of functions and purposes. AES is used for symmetric encryption. PKCS is used as a digital signature algorithm. SSL/TLS is used for secure key exchange.

31. Question

A network technician is responsible for the basic security of the network. Management has asked if there is a way to improve the level of access users have to the company file server. Right now, any employee can upload and download files with basic system authentication (username and password). What should he configure to increase security?

- MDS authentication
- **Multi-factor authentication**
- Kerberos authentication
- Single sign-on authentication

Unattempted

OBJ-1.1: This security approach provides a defense layer that makes it difficult for unauthorized users to break into a system. It provides multiple factors that a user must know to obtain access. For instance, if one factor is successfully broken, there will be few others that the individual attempting to enter the system must overcome.

32. Question

A firewall administrator has configured a new DMZ to allow public systems to be segmented from the organization's internal network. The firewall now has three security zones set: Untrusted (Internet) [143.27.43.0/24]; DMZ (DMZ) [161.212.71.0/24]; Trusted (Intranet) [10.10.0.0/24]. The firewall administrator has been asked to enable remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ for the Chief Security Officer to work from his home office after hours. The CSO's home internet uses a static IP of 143.27.43.32. The remote desktop server is assigned a public-facing IP of 161.212.71.14. What rule should the administrator add to the firewall?

- **Permit 143.27.43.32 161.212.71.14 RDP 3389**
- Permit 143.27.43.0/24 161.212.71.14 RDP 3389
- Permit 143.27.43.0/24 161.212.71.0/24 RDP 3389
- Permit 143.27.43.32 161.212.71.0/24 RDP 3389

Unattempted

OBJ-4.5: Due to the requirement to allow a single remote IP to enter the firewall, the permit statement must start with a single IP in the Untrusted (Internet) zone. Based on the options provided, only 143.27.43.32 could be correct. Next, the destination is a single server in the DMZ, so only 161.212.71.14 could be correct.

The destination port should be 3389, which is the port for the Remote Desktop Protocol. Combining these three facts, only "permit 143.27.43.32 161.212.71.14 RDP 3389" could be correct.

33. Question

Fail to Pass Systems recently installed a break and inspect appliance that allows their cybersecurity analysts to observe HTTPS traffic entering and leaving their network. Consider the following output from a recorded session captured by the appliance:

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

POST /www/default.php HTTP/1.1

HOST: .123

Content-Length: 147

Cache-Control: no-cache

Origin: chrome-extension://ghwjhwrequsds

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0

Content-Type: multipart/form-data; boundary=——-

WebKitFormBoundaryaym16ehT29q60rUx

Accept:*/*

Accept-Language: zh, en-us; q=0.8, en; q=0.6

Cookie: security=low; PHPSESSID=jk3j2kdso8x73kdjhehakske

———WebKitFormBoundaryaym16ehT29q60rUx

Content-Disposition: form-data; name="q"

cat /etc/passwd

———WebKitFormBoundaryaym16ehT29q60rUx

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Which of the following statements is true?

- The /etc/passwd file was just downloaded through a webshell by an attacker
- The web browser used in the attack was Microsoft Edge
- This is a normal request from a host to your web server in the DMZ
- **A request to issue the command "cat /etc/passwd" occurred but additional analysis is required to verify if the file was downloaded**

Unattempted

OBJ-5.2: This is a post request to run the "cat /etc/passwd" command from an outside source. It is not known from the evidence provided if this command were successful or not, but it should be analyzed further as this is not what would be expected, normal traffic. While the browser's default language was configured

for Chinese (zh), this is easily changed and cannot be used to draw authoritative conclusions about the threat actor's true location or persona. The User-Agent used is listed as Mozilla, which is used by both Firefox and Google Chrome. For an in-depth analysis of the full attack this code snippet was taken from, please visit https://www.rsa.com/content/dam/en/solution-brief/asoc-threat-solution-series-webshells.pdf. This 6-page article is definitely worth your time to look over and learn how a remote access web shell is used as an exploit.

34. Question

Which of the following vulnerabilities involves leveraging access from a single virtual machine to other machines on a hypervisor?

- VM sprawl
- **VM escape**
- VM data remnant
- VM migration

Unattempted

OBJ-8.1: Virtual machine escape vulnerabilities are the most severe issue that may exist in a virtualized environment. In this attack, the attacker can access a single virtual host and then leverages that access to intrude on the resources assigned to different virtual machines. Data remnant is the residual representation of digital data that remains even after attempts have been made to remove or erase it. Virtualization sprawl is a phenomenon that occurs when the number of virtual machines on a network reaches a point where the administrator can no longer manage them effectively. Virtual machine migration is the task of moving a virtual machine from one physical hardware environment to another.

35. Question

You are trying to select the best device to install to detect an outside attacker trying to reach into your internal network. The device should log the event, but it should not take any action to stop it. Which of the following devices would be the BEST for you to select?

- **IDS**
- Proxy server
- IPS
- Authentication server

Unattempted

OBJ-4.5: An intrusion detection system is a device or software application that monitors a network or system for malicious activity or policy violations. Any malicious activity or violation is typically reported to an administrator or collected centrally using a security information and event management system. Unlike an IPS, which can stop malicious activity or policy violations, an IDS can only log these issues and not stop them.

36. Question

Which of the following techniques would be the most appropriate solution to implementing a multi-factor authentication system?

- Smartcard and PIN
- Username and password
- Fingerprint and retinal scan
- Password and security question

Unattempted

OBJ-1.1: Multi-factor authentication (MFA) creates multiple security layers to help increase the confidence that the user requesting access is who they claim to be by requiring two distinct factors for authentication. These factors can be something you know (knowledge factor), something you have (possession factor), something you are (inheritance factor), something you do (action factor), or somewhere you are (location factor). By selecting a smartcard (something you have) and a PIN (something you know), you have implemented multi-factor authentication. Choosing a fingerprint and retinal scan would instead use only one factor (inheritance). Choosing a username, password, and security question would also be only using one factor (knowledge). For something to be considered multi-factor, you need items from at least two different authentication factor categories: knowledge, possession, inheritance, location, or action.

37. Question

Your company recently suffered a small data breach caused by an employee emailing themselves a copy of the current customer's names, account numbers, and credit card limits. You are determined that something like this shall never happen again. Which of the following logical security concepts should you implement to prevent a trusted insider from stealing your corporate data?

- Strong passwords
- MDM

- DLP
- Firewall

Unattempted

OBJ-7.1: Data loss prevention software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in use (endpoint actions), in-motion (network traffic), and at rest (data storage). Since the user was an authorized user (employee), changing your password policy, reconfiguring the firewall, or setting up an MDM solution would not solve this problem. Instead, a DLP solution must be implemented.

38. Question

A vulnerability scan has returned the following results:

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Detailed Results

10.56.17.21 (APACHE-2.4)

Windows Shares

Category: Windows

CVE ID: –

Vendor Ref: –

Bugtraq ID: –

Service Modified – 8.30.2017

Enumeration Results:

print$ c:\windows\system32\spool\drivers

files c:\FileShare\Accounting

Temp c:\temp

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

What best describes the meaning of this output?

- There is an unknown bug in an Apache server with no Bugtraq ID
- There is no CVE present, so this is a false positive caused by Apache running on a Windows server
- **Connecting to the host using a null session allows enumeration of the share names on the host**
- Windows Defender has a known exploit that must be resolved or patched

Unattempted

OBJ-3.1: These results from the vulnerability scan conducted shows an enumeration of open Windows shares on an Apache server. The enumeration results show three share names (print$, files, Temp) were

found using a null session connection. There is no associated CVE with this vulnerability, but it is not a false positive. Not all vulnerabilities have a CVE associated with them. Nothing in this output indicates anything concerning Windows Defender, so this is not the correct answer. Bugtraq IDs are a different type of identification number issued for vulnerabilities by SecurityFocus. Generally, if there is a CVE, there will also be a Bugtraq ID. Both the CVE and Bugtraq ID being blank is not suspicious since we are dealing with a null enumeration result.

39. Question

You just received an email from Bob, your investment banker, stating that he completed the wire transfer of $10,000 to your bank account in Vietnam. The problem is, you do not have a bank account in Vietnam, so you immediately call Bob to ask what happened. Bob explains that he received an email from you requesting the transfer. You insist you never sent that email to Bob initiating this wire transfer. What aspect of PKI could be used to BEST ensure that a sender actually sent a particular email message and avoid this type of situation?

- Recovery agents
- CRL
- **Non-repudiation**
- Trust models

Unattempted

OBJ-9.1: Non-repudiation occurs when a sender cannot claim they didn't send an email when they did. A digital signature should be attached to each email sent to achieve non-repudiation. This digital signature is comprised of a digital hash of the email's contents, and then encrypting that digital hash using the sender's private key. The receiver can then unencrypt the digital hash using the sender's public key to verify the message's integrity.

40. Question

Tim, a help desk technician, receives a call from a frantic executive who states that their company-issued smartphone was stolen during their lunch meeting with a rival company's executive. Tim quickly checks the MDM administration tool and identifies that the user's smartphone is still communicating with the MDM, and displays its location on a map. What should Tim do next to ensure the stolen device's data remains confidential and inaccessible to the thief?

- Reset the device's password
- Remotely encrypt the device

- Perform a remote wipe of the device
- Identify the IP address of the smartphone

Unattempted

OBJ-7.1: To ensure the data remains confidential and is not accessed by the thief, Tim should perform a remote wipe of the device from the MDM. This will ensure any corporate data is erased before anyone accessing it. Additionally, Tim could reset the device's password, but if the thief can guess or crack the password, they would have access to the data. Identifying the smartphone's IP address is not a useful step in protecting the data on the device. Additionally, devices should be encrypted BEFORE they are lost or stolen, not after. Therefore, the option to remotely encrypt the device is provided as a wrong answer and a distractor.

41. Question

You are currently working as a firewall technician. You have received a request to open up a few ports on the firewall to allow a newly VoIP system to operate properly. The installer has requested that the ports associated with SIP, RDP, H.323, and RTP be opened to allow the new system to operate properly. Which of these ports are NOT used by a typical VoIP system?

- SIP
- H.323
- RDP
- RTP

Unattempted

OBJ-4.1: RDP is the protocol for the Remote Desktop Protocol and operates over port 3389. This is not used in a typical VoIP system. SIP (Session Initiation Protocol), H.323 (voice/video conferencing) protocol, and the RTP (Real-time Transport Protocol) are all used heavily in VoIP and video conferencing solutions.

42. Question

A cybersecurity analyst just finished conducting an initial vulnerability scan and is reviewing their results. To avoid wasting time on results that are not really a vulnerability, the analyst wants to remove any false positives before remediating the findings. Which of the following is an indicator that something in their results would be a false positive?

- A scan result showing a version that is different from the automated asset inventory

- A finding that shows the scanner compliance plug-ins are not up-to-date
- A 'HTTPS entry that indicates the web page is securely encrypted
- **Items classified by the system as Low or as For Informational Purposes Only**

Unattempted

OBJ-3.1: When conducting a vulnerability scan, it is common for the report to include some findings that are classified as "low" priority or "for informational purposes only." These are most likely false positives and can be ignored by the analyst when starting their remediation efforts. "An HTTPS entry that indicates the web page is securely encrypted" is not a false positive but a true negative (a non-issue). A scan result showing a different version from the automated asset inventory should be investigated and is likely a true positive. A finding that shows the scanner compliance plug-ins are not up-to-date would likely also be a true positive that should be investigated.

43. Question

Which of the following nmap commands should be utilized by a penetration tester that wants to scan every TCP registered port with fingerprinting, service, and operating system detection on a Class B network that is blocking ICMP?

- nmap -Pn -O -sS -p 1-65535 172.16.1.0/8
- nmap -Pn -A -sT –p 0-65535 172.16.1.0/24
- nmap -Pn -A --sS –p 1-1024 -sS 172.16.1.0/16
- **nmap -Pn -A -O –p 1-1024 -sS 172.16.1.0/16**

Unattempted

OBJ-2.2: There are several ways to answer this question, even if you don't remember ever piece of the NMAP syntax. First, the question asks you to scan a Class B network, and if we want to scan the entire Class B, we would have to scan a /16. This removed two of our four choices. Now, considering the last two choices, we have a major differences: only one of these options would provide operating system detection (-O).

44. Question

What nmap switch would you use to perform operating system detection?

- -sP

- -s0
- **–O**
- -OS

Unattempted

OBJ-2.2: The –O switch is used to tell nmap to conduct fingerprinting of the operating system based on the responses received during scanning. Nmap will then report on the suspected operating system of the scanned host. If you use –O –v, you will get additional details, as this runs the operating system scan in verbose mode. The -OS flag is made up and not supported by nmap. The -s0 flag conducts an IP protocol scan of the target. The -sP flag conducts a simple ping scan against the target.

45. Question

Windows file servers commonly hold sensitive files, databases, passwords, and more. What common vulnerability is usually used against a Windows file server to expose sensitive files, databases, and passwords?

- CRLF injection
- SQL injection
- **Missing patches**
- Cross-site scripting

Unattempted

OBJ-3.2: Missing patches are the most common vulnerability found on both Windows and Linux systems. When a security patch is released, attackers begin to reverse engineer the security patch to exploit the vulnerability. If your servers are not patched against the vulnerability, they can become victims of the exploit, and the server's data can become compromised. Cross-Site Scripting (XSS) attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. Cross-site scripting focuses on exploiting a user's workstation, not a server. CRLF injection is a software application coding vulnerability that occurs when an attacker injects a CRLF character sequence where it is not expected. SQL injection is the placement of malicious code in SQL statements via web page input. SQL is commonly used against databases, but they are not useful when attacking file servers.

46. Question

David noticed that port 3389 was open on one of the POS terminals in a store during a scheduled PCI compliance scan. Based on the scan results, what service should he expect to find enabled on this terminal?

- RDP
- LDAP
- IMAP
- MySQL

Unattempted

OBJ-2.2: Port 3389 is an RDP port used for the Remote Desktop Protocol. If this port isn't supposed to be opened, then an incident response plan should be the next step since this can be used for remote access by an attacker. MySQL runs on port 3306. LDAP runs on port 389. IMAP over SSL runs on port 993.

47. Question

What SCAP component provides a list of entries that contains an identification number, a description, and a public reference for each publicly known weakness in a piece of software?

- CVE
- XCCDF
- CPE
- CCE

Unattempted

OBJ-3.1: The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures. XCCDF (extensible configuration checklist description format) is a language that is used in creating checklists for reporting results. The Common Configuration Enumeration (CCE) provides unique identifiers to system configuration issues to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets.

48. Question

You want to provide controlled remote access to the remote administration interfaces of multiple servers hosted on a private cloud. What type of segmentation security solution is the best choice for this scenario?

- Physical

- Bastion hosts
- Airgap
- **Jumpbox**

Unattempted

OBJ-8.1: Installing a jumpbox as a single point of entry for the administration of servers within the cloud is the best choice for this requirement. The jumpbox only runs the necessary administrative port and protocol (typically SSH). Administrators connect to the jumpbox then use the jumpbox to connect to the admin interface on the application server. The application server's admin interface has a single entry in its ACL (the jumpbox) and denies any other hosts' connection attempts. A bastion host is a special-purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application. For example, a proxy server and all other services are removed or limited to reduce the threat to the computer. An airgap system is a network or single host computer with unique security requirements that may physically be separated from any other network. Physical separation would prevent a system from accessing the remote administration interface directly and require an airgap system to reach the private cloud.

49. Question

Your organization's primary operating system vendor just released a critical patch for your servers. Your system administrators have recently deployed this patch and verified the installation was successful. This critical patch was designed to remediate a vulnerability that can allow a malicious actor to execute code on the server over the Internet remotely. You ran a vulnerability scan of the network and determined that all servers are still being reported as having the vulnerability. You verified all your scan configurations are correct. Which of the following might be the reason that the scan report still showing the servers as vulnerable? (SELECT ALL THAT APPLY)

- The wrong IP address range was scanned during your vulnerability assessment
- You conducted the vulnerability scan without waiting long enough after the patch was installed
- **This critical patch did not remediate the vulnerability**
- **The vulnerability assessment scan is returning a false positive**

Unattempted

OBJ-3.1: There are two reasonable choices presented: (1) the vulnerability assessment scan is returning a false positive, or (2) this critical patch did not remediate the vulnerability. It is impossible to know which is based on the description in the question. If the patch was installed successfully, as the question states, then

it is possible that the critical patch was coded incorrectly and did not actually remediate the vulnerability. While most operating system vendors test their patches before release to prevent this, they are sometimes rushed into production with extremely critical patches. The patch does not actually remediate the vulnerability on all systems. When this occurs, the vendor will issue a subsequent patch to fix it and supersede the original patch. The other option is that the vulnerability assessment tool is incorrectly configured and is returning a false positive. This can occur when the signature used to detect the vulnerability is too specific or too generic to actually detect whether the system was patched for the vulnerability or not. The other options are incorrect, as you do not have to wait a certain period of time after installation before scanning. It is assumed that you are scanning the same IP range both times as you have verified your scan configuration.

50. Question

Which of the following is a special type of embedded operating system that uses a predictable and consistent scheduler?

- IoT
- Mobile
- **RTOS**
- PoS

Unattempted

OBJ-7.2: A real-time operating system (RTOS) is a special type of embedded OS. An RTOS ideal for embedded systems because they tend to have strict requirements for when a task should be completed and do not have particularly taxing workloads. An RTOS uses a predictable and consistent scheduler, unlike a general-purpose OS like Windows or macOS.

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
TERMS & CONDITIONS
PRIVACY POLICY

Privacy Policy