SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 3

Your results are here!! for" CEHv11 Practice Test 3 "

0 of 50 questions answered correctly

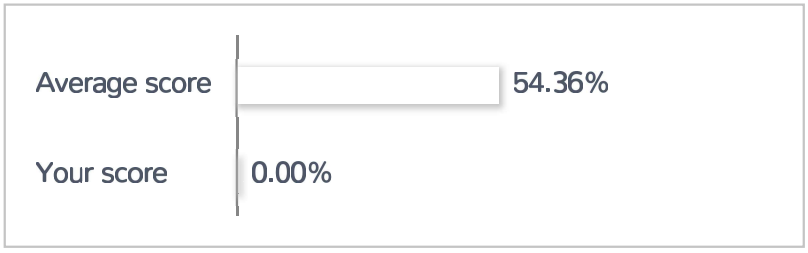
Your time: 00:00:02

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

Correct Incorrect

Review Question Summary

1. Question

You walked up behind a penetration tester in your organization and saw the following output on their Kali Linux terminal:

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

[ATTEMPT] target 192.168.1.142 – login “root” – pass “abcde” 1 of 10

[ATTEMPT] target 192.168.1.142 – login “root” – pass “efghi” 2 of 10

[ATTEMPT] target 192.168.1.142 – login “root” – pass “12345” 3 of 10

[ATTEMPT] target 192.168.1.142 – login “root” – pass “67890” 4 of 10

[ATTEMPT] target 192.168.1.142 – login “root” – pass “a1b2c” 5 of 10

[ATTEMPT] target 192.168.1.142 – login “user” – pass “abcde” 6 of 10

[ATTEMPT] target 192.168.1.142 – login “user” – pass “efghi” 7 of 10

[ATTEMPT] target 192.168.1.142 – login “user” – pass “12345” 8 of 10

[ATTEMPT] target 192.168.1.142 – login “user” – pass “67890” 9 of 10

[ATTEMPT] target 192.168.1.142 – login “user” – pass “a1b2c” 10 of 10

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

What type of test is the penetration tester currently conducting?

- Conducting a port scan of 192.168.1.142
- Conducting a Denial of Service attack on 192.168.1.142
- **Conducting a brute force login attempt of a remote service on 192.168.1.142**
- Conducting a ping sweep of 192.168.1.142/24

Unattempted

OBJ-3.2: The penetration tester is attempting to conduct a brute force login attempt of a remote service on 192.168.1.142, as shown by the multiple login attempts with common usernames and passwords. A brute force attack attempts to crack a password or username or find a hidden web page, or find the key used to encrypt a message, using a trial and error approach and hoping, eventually, to guess correctly. Port Scanning is the name for the technique used to identify open ports and services available on a network host. A denial-of-service (DoS) attack occurs when legitimate users cannot access information systems, devices, or other network resources due to a malicious cyber threat actor’s actions. A ping sweep is a basic network scanning technique used to determine which range of IP addresses map to live hosts.

2. Question

You are performing a web application security test, notice that the site is dynamic, and must be using a back-end database. You decide you want to determine if the site is susceptible to a SQL injection. What is the first character that you should attempt to use in breaking a valid SQL request?

- Single quote
- Exclamation mark
- Double quote
- Semicolon

Unattempted

OBJ-5.3: The single quote character (‘) is the character limiter in SQL. With a single quote,’ you delimit strings, and therefore you can test whether the programmer has properly escaped the strings in the targeted application. If not escaped directly, you can end any string supplied to the application and add other SQL code after it. This is a common technique for SQL injections. A semicolon is a commonly used character at the end of a line of code or command in many programming languages. An exclamation mark comments a line of code in several languages. Double quotes contain a string that is passed to a variable.

3. Question

You are conducting a static analysis of an application’s source code and see the following:

-=-

(String) page += ““;

-=-

Based on this code snippet, which of the following security flaws exists in this application?

- Insufficient logging and monitoring
- Race condition
- Improper error handling
- Improper input validation

Unattempted

OBJ-5.2: Based on this code snippet, the application is not utilizing input validation. This would allow a malicious user to conduct an XSS (cross-site scripting) attack. For example, an attacker could input the

following for a value of "ID": '>'. This could cause the victim ID to be sent to "malicious-website.com" where additional code could be run, or the session can then be hijacked. Based on the code snippet provided, we have no indications of the level of logging and monitoring being performed, nor if proper error handling is being conducted. A race condition is a software vulnerability when the resulting outcome from execution processes is directly dependent on the order and timing of certain events. Those events fail to execute in the order and timing intended by the developer.

4. Question

Sarah is working at a startup that is focused on making secure banking apps for smartphones. Her company needs to select an asymmetric encryption algorithm to encrypt the data being used by the app. Due to the need for high security of the banking data, the company needs to ensure that whatever encryption they use is considered strong, but also need to minimize the processing power required since it will be running on a mobile device with lower computing power. Which algorithm should Sarah choose to provide the same level of high encryption strength with a lower overall key length?

- ECC
- Twofish
- Diffie-Hellman
- RSA

Unattempted

OBJ-9.1: Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits of ECC over non-ECC cryptography is an application that can achieve the same level of security provided by non-ECC cryptography while using a shorter key length. For example, an ECC algorithm using a 256-bit key length is just as strong as an RSA or Diffie-Hellman algorithm using a 3072-bit key length.

5. Question

What is the proper threat classification for a security breach that employs brute-force methods to compromise, degrade, or destroy systems?

- Attrition
- Impersonation
- Improper usage

Loss or theft of equipment

Unattempted

OBJ-3.2: Attrition attacks employ brute-force methods to compromise, degrade, or destroy systems, networks, or services. An impersonation attack occurs when the attacker gains control of an employee's account and uses it to convince other employees to perform fraudulent actions. Improper usage occurs when an employee or other authorized user utilizes the systems or networks not as intended or designed. The loss or theft of equipment usually relates to a smartphone, tablet, or laptop is lost or stolen, and then the data on it becomes compromised.

6. Question

A vulnerability scanner has reported that a vulnerability exists in the system. Upon validating the report, the analyst determines that this reported vulnerability does not exist on the system. What is the proper term for this situation?

True positive

True negative

False negative

False positive

Unattempted

OBJ-3.1: A false positive occurs when a scanner detects a vulnerability, but the vulnerability does not actually exist on the scanned system. A true positive occurs when a scanner detects a vulnerability, and the vulnerability exists on the scanned system. A true negative occurs when a scanner does not detect a vulnerability because the vulnerability does not exist on the scanned system. A false negative occurs when a scanner does not detect a vulnerability, but the vulnerability actually exists on the scanned system.

7. Question

Your network is currently under attack from multiple hosts outside of the network. Which type of attack is most likely occurring?

Spoofing

DoS

DDoS

Wardriving

Unattempted

OBJ-4.3: A Distributed Denial of Service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system or network. DoS and Spoofing attacks originate from a single host, while wardriving is focused on the surveillance and reconnaissance of wireless networks.

8. Question

Which of the following techniques listed below are not appropriate to use during a passive reconnaissance exercise against a specific target company?

WHOIS lookups

Banner grabbing

BGP looking glass usage

Registrar checks

Unattempted

OBJ-2.1: Banner grabbing requires a connection to the host to grab the banner successfully. This is an active reconnaissance activity. All other options are considered passive processes and typically use information retrieved from third-parties that do not directly connect to an organization's remote host.

9. Question

A software developer has just finished writing a new application. You have been contracted to conduct a scan to determine what vulnerabilities may exist. The developer provides you with the source code and the binary for the application. Which of the following should you perform FIRST?

Vulnerability scan

Dynamic application scan

Compliance scan

Static application scan

Unattempted

OBJ-3.1: A static application scan, or static code analysis, is the process of reviewing the source code while it is not executing. This requires the source code of the application, which in this scenario was provided.

Static analysis can help you discover how the application functions and will allow you to find mistakes caused by poor programming practices, such as the failure to conduct input validation. If you have the source code and understand how to read the language used in it, you should first conduct a static code analysis. Once completed, you can move on to a dynamic application scan.

10. Question

You are conducting a wireless penetration test against an organization. During your reconnaissance, you discover that their network is known as "BigCorpWireless" has its SSID broadcast is enabled. You configure your laptop to respond to requests for connection to "BigCorpWireless" and park at the far end of the parking lot. At the end of the workday, as people get in their cars in the parking lot, you see numerous smartphones connecting to your laptop over WiFi. Which of the following exploits did you utilize?

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

Unattempted

OBJ-6.1: A karma attack is a variant of the evil twin attack. A karma attack exploits the behavior of a wireless client trying to connect to its preferred network list. This list contains the SSIDs of access points the device has connected to in the past. When a wireless device is looking to connect to the internet, it firsts beacons to determine if any of these previously connected to networks are within range. This allows an attacker to answer the request, allowing the user to connect to them instead as an evil twin. At this point, the attacker is now the man-in-the-middle between the wireless client and the internet, which is useful for many different exploits.

11. Question

What is the BEST explanation for why consumer-based IoT devices are less secure than traditional desktops and servers?

- **IoT devices focus convenience more than security**
- IoT devices are unable to receive patches and updates
- IoT devices are only used in low security use cases
- IoT devices are not powerful enough to support encryption

Unattempted

OBJ-7.2: IoT device manufacturers are more focused on making the devices convenient to use instead of ensuring they have strong security. The other options are incorrect and not true. IoT devices can receive patches and updates through an over-the-air firmware update if a manufacturer creates the patches. IoT devices are powerful these days, and they can support encryption and other security features if manufacturers would add them to their code. IoT devices are not just used in low-security use cases, either. For example, IoT devices are often used as life-saving devices in hospitals or security systems in our homes. Unfortunately, IoT devices are notoriously lax when it comes to security. Some IoT systems may even allow a user full remote control of a device.

12. Question

Which of the following vulnerabilities is the greatest threat to data confidentiality?

- Web application SQL injection vulnerability
- HTTP TRACE/TRACK methods enabled
- SSL Server with SSLv3 enabled vulnerability
- phpinfo information disclosure vulnerability

Unattempted

OBJ-5.3: Each vulnerability mentioned poses a significant risk, but the greatest threat comes from the SQL injection. An SQL injection could allow an attacker to retrieve our data from the backend database directly. Using this technique, the attacker could also alter the data and put it back, and nobody would notice everything that had been changed, thereby also affecting our data integrity. The HTTP TRACE/TRACK methods are normally used to return the full HTTP request to the requesting client for proxy-debugging purposes and allow the attacker to access sensitive information in the HTTP headers. Since this only exposes information in the headers, it minimizes the risk to our system's data confidentiality. An SSL server with SSLv3 enabled is not ideal since this is an older encryption type, but it still provides some confidentiality. The phpinfo information disclosure vulnerability prints out detailed information on both the system and the PHP configuration. This information by itself doesn't disclose any information about the data stored within the system, though, so it isn't a great threat to our data's confidentiality.

13. Question

A cybersecurity analyst has received an alert that sensors continuously observe well-known call home messages at their network boundary. Still, the organization's proxy firewall is properly configured to

successfully drop the messages before leaving the network. Which of the following is MOST likely the cause of the call home messages being sent?

- An attacker is performing reconnaissance the organization's workstations
- **An infected workstation is attempting to reach a command and control server**
- A malicious insider is trying to exfiltrate information to a remote network
- Malware is running on a company workstation or server

Unattempted

OBJ-4.3: A call home message is an indicator of compromise known as beaconing. Beaconing usually occurs after a stage 1 malware program has been implanted on an organization's workstation or server, but that isn't the most correct answer to this question. Instead, beaconing indicates that a workstation or server is infected and tries to communicate with the attacker's command and control server. This beaconing will continue until the infected system (workstation or server) is found and cleared of the malware or until the botnet gives the infected host further instructions to perform (such as to attack). "Malware is running on a company workstation or server" is incorrect because we do not have positive verification of that based on this scenario. A beacon does not have to be malware. For example, it can simply be a single ping packet or DNS request being sent out every day at a certain time using the Windows task scheduler. Be careful on the exam to answer the question being asked and choose the "most" accurate answer. Since the call home signal is coming from the internal network and attempting to connect to an external server, it cannot be evidence of an attacker performing reconnaissance on your workstations. Also, nothing in the question is indicative of an insider threat trying to exfiltrate information since a call home message is generally minimal in size and not large enough to exfiltrate data.

14. Question

You have noticed some unusual network traffic outbound from a certain host. The host is communicating with a known malicious server over port 443 using an encrypted TLS tunnel. You ran a full system anti-virus scan of the host with an updated anti-virus signature file, but the anti-virus did not find any infection signs. Which of the following has MOST likely occurred?

- Directory traversal
- **Zero-day attack**
- Password spraying
- Session hijacking

Unattempted

OBJ-3.3: Since you scanned the system with the latest anti-virus signatures and did not find any signs of infection, it would most likely be evidence of a zero-day attack. A zero-day attack has a clear sign of compromise (the web tunnel being established to a known malicious server). The anti-virus doesn't have a signature yet for this particular malware variant. Password spraying occurs when an attacker tries to log in to multiple different user accounts with the same compromised password credentials. Session hijacking is exploiting a valid computer session to gain unauthorized access to information or services in a computer system. Based on the scenario, it doesn't appear to be session hijacking since the user would not normally attempt to connect to a malicious server. Directory traversal is an HTTP attack that allows attackers to access restricted directories and execute commands outside of the web server's root directory. A directory traversal is usually indicated by a dot dot slash (../) in the URL being attempted.

15. Question

Which technique would provide the largest increase in security on a network with ICS, SCADA, or IoT devices?

- **User and entity behavior analytics**
- Use of a host-based IDS or IPS
- Installation of anti-virus tools
- Implement endpoint protection platforms

Unattempted

OBJ-7.2: Since ICS, SCADA, and IoT devices often run proprietary, inaccessible, or unpatchable operating systems, the traditional tools used to detect the presence of malicious cyber activity in normal enterprise networks will not function properly. Therefore, user and entity behavior analytics (UEBA) is best suited to detect and classify known-good behavior from these systems to create a baseline. Once a known-good baseline is established, deviations can be detected and analyzed. UEBA may be heavily dependent on advanced computing techniques like artificial intelligence and machine learning and may have a higher false-positive rate. As the name suggests, the analytics software tracks user account behavior across different devices and cloud services. Entity refers to machine accounts, such as client workstations or virtualized server instances, and embedded hardware, such as the Internet of Things (IoT) devices. Traditional technologies include anti-virus tools, host-based IDS and IPS, and endpoint protection platforms.

16. Question

What method might a system administrator use to replicate the DNS information from one DNS server to another, but could also be used maliciously by an attacker?

- Zone transfers
- DNSSEC
- CNAME
- DNS registration

Unattempted

OBJ-2.3: Zone transfers provide an easy way to send all the DNS information from one DNS server to another, but an attacker could also use it for reconnaissance against your organization. For this reason, most administrators disable zone transfers from untrusted servers. DNSSEC strengthens authentication in DNS using digital signatures based on public-key cryptography. CNAME is a Canonical Name Record or Alias Record. A type of resource record in the Domain Name System (DNS) specifies that one domain name is an alias of another canonical domain name. DNS registration is a service, which allows the owner of a domain name to use their name servers, which can match the domain name in question.

17. Question

You are conducting a wireless penetration test against an organization. You have been monitoring the WPA2 encrypted network for almost an hour but have been unable to successfully capture a handshake. Which of the following exploits should you use to increase your chances of capturing a handshake?

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

Unattempted

OBJ-6.1: Deauthentication attacks are used in the service of an evil twin, replay, cracking, denial of service, and other attacks. All 802.11 Wi-Fi protocols include a management frame that a client can use to announce that it wishes to terminate a connection with an access point. The victim's device will be kicked off the access point by spoofing the victim's MAC address and sending the deauthentication frame to the access point. If the user is still using the network, the wireless adapter will automatically reconnect by sending a handshake to the access point. This allows the attacker to capture the handshake during the reconnection.

18. Question

A project lead reviews the statement of work for an upcoming project that is focused on identifying potential weaknesses in the organization's internal and external network infrastructure. As part of the project, a team of external contractors will attempt to employ various attacks against the organization. The work statement specifically addresses the utilization of an automated tool to probe network resources in an attempt to develop logical diagrams indicating weaknesses in the infrastructure. Based on this scope of work, what type of activity is to be performed?

- Session hijacking
- Vulnerability scanning
- Social engineering
- **Penetration testing**

Unattempted

OBJ-1.1: Penetration testing is the act of using a computer system, an individual network, or another application to find vulnerabilities that an attacker could use to compromise your systems. Penetration testing can also find endpoints with vulnerabilities, which makes the attack surface greater.

19. Question

You have been tasked to create some baseline system images to remediate vulnerabilities found in different operating systems. Before any of the images can be deployed, they must be scanned for malware and vulnerabilities. You must ensure the configurations meet industry-standard benchmarks and that the baselining creation process can be repeated frequently. What vulnerability option would BEST create the process requirements to meet the industry-standard benchmarks?

- **Utilizing an operating system SCAP plugin**
- Utilizing an authorized credential scan
- Utilizing a known malware plugin
- Utilizing a non-credential scan

Unattempted

OBJ-3.1: Security Content Automation Protocol (SCAP) is a multi-purpose framework of specifications supporting automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement. It is an industry-standard and support testing for compliance. The other options will not allow for a truly repeatable process since individual scans would occur each time instead of comparing against a known good baseline.

20. Question

Which of the following cryptographic algorithms is classified as asymmetric?

- RSA
- RC4
- AES
- DES

Unattempted

OBJ-9.1: RSA (Rivest–Shamir–Adleman) was one of the first public-key cryptosystems and is widely used for secure data transmission. As a public-key cryptosystem, it relies on an asymmetric algorithm. AES, RC4, and DES are all symmetric algorithms.

21. Question

A pentester is trying to map the organization's internal network. The analyst enters the following command (nmap -n -sS -T4 -p 80 10.0.3.0/24). What type of scan is this?

- Stealth Scan
- Quick Scan
- Intense Scan
- Comprehensive Scan

Unattempted

OBJ-2.2: In nmap, the -sS flag signifies a stealth scan. This is also known as an SYN scan and is the most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network, and is not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections.

22. Question

During your reconnaissance, you have determined that your client has devices used to send remote control signals to industrial assets used by their critical infrastructure utilities connected to their corporate network. Which of the following methods would MOST likely be the best method for exploiting these systems?

- **Use Metasploit modules designed to target the SCADA systems**
- Use social engineering to trick a user into opening a malicious APK
- Use a spearphishing campaign to trick a user into installing a RAT
- Identify a jailbroken device for easy exploitation

Unattempted

OBJ-7.2: A penetration tester can exploit supervisory control and data acquisition (SCADA) systems if they are within the engagement's scope. While Metasploit was initially designed for engagements against workstations and servers, Metasploit has several modules in the exploit/ windows/scada category that target vendor-specific SCADA components running Windows. Many of these trigger a buffer overflow, though, so be careful when using them and ensure you have permission to exploit these devices in your written authorization.

23. Question

You conducted a security scan and found that port 389 is being used when connecting to LDAP for user authentication instead of port 636. The security scanning software recommends that you remediate this by changing user authentication to port to 636 wherever possible. What should you do?

- Conduct remediation actions to update encryption keys on each server to match port 636
- Mark this as a false positive in your audit report since the services that typically run on ports 389 and 636 are identical
- Change all devices and servers that support it to port 636 since port 389 is a reserved port that requires root access and can expose the server to privilege escalation attacks
- **Change all devices and servers that support it to port 636 since encrypted services run by default on port 636**

Unattempted

OBJ-2.3: LDAP can be run on either port 389 or port 636. Port 389 is the standard port for LDAP but typically runs unencrypted LDAP services over this port. Instead, you should change all devices and servers that can technically support the change to port 636 since LDAP services over port 636 are encrypted by default.

24. Question

Which of the following tools can NOT be used to conduct a banner grab from a web server on a remote host?

- wget
- **ftp**
- netcat
- telnet

Unattempted

OBJ-2.1: FTP cannot be used to conduct a banner grab. A cybersecurity analyst or penetration tester uses a banner grab to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network. This is commonly done using telnet, wget, or netcat.

25. Question

You are conducting a wireless penetration test against an organization. You have identified that they are using WEP encryption on their wireless access points. You are impatient and do not want to wait to collect enough packets to find a repeated initialization vector. You decide to extract part of the key material from one of the packets and use it to send an ARP request to the AP. Which of the following exploits did you utilize in this attack?

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

Unattempted

OBJ-6.1: A fragmentation attack obtains the pseudorandom generation algorithm (PRGA) of network packets used in WEP. The PRGA can be used to craft encrypted packets that you can inject into the access point. These injected packets can speed up cracking the WEP password; otherwise, it might take a while to receive enough packets to get the repeated IV. In a fragmentation attack, you extract part of the key material from at least one packet and use this to send an ARP request to the AP. If successful, the AP responds with more of the key material in the packet echoed back to you. You repeat this process many times until around 1500 bytes of the PRGA is captured, at which point you can then use a packet crafting tool to begin the injection process.

26. Question

You have been given access to a Windows system located on an Active Directory domain as part of a white box penetration test. Which of the following commands would provide information about other systems on this network?

- net user
- net group
- **net use**
- net config

Unattempted

OBJ-2.3: The net use command will list network shares that the workstation is using. This will help to identify file servers and print servers on the network. The net group command can only be used on domain controllers. The net config command will allow servers and workstations services to be controlled once they have already been identified. The net user command would show any user accounts on the local Windows workstation you are using.

27. Question

A cybersecurity analyst from BigCorp contacts your company to notify them that several of your computers were seen attempting to create a denial of service condition against their servers. They believe your company has become infected with malware, and those machines were part of a larger botnet. Which of the following BEST describes your company's infected computers?

- Monsters
- Bugs
- Zero-day
- **Zombie**

Unattempted

OBJ-4.3: A zombie is a computer connected to the internet that has been compromised by a hacker, computer virus, or trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread email spam and launch denial-of-service attacks (DoS attacks).

28. Question

A recent threat has been announced in the cybersecurity world, stating a critical vulnerability in a particular operating system's kernel. Unfortunately, your company has not maintained a current asset inventory, so you are unsure of how many your servers may be affected. What should you do to find all of the affected servers within your network?

- Manually review the syslog server's logs
- **Conduct an OS fingerprinting scan across the network**
- Conduct a service discovery scan on the network
- Conduct a packet capture of data traversing the server network

Unattempted

OBJ-2.2: By utilizing operating system fingerprinting using a tool like nmap, you can identify the servers running each version of an operating system. This will give you an accurate list of the possibly affected servers. Once you have this list, you can focus your attention on just those servers that need further inspection and scanning. Manually review the Syslog server's log would take too long, and would not find servers that don't send their logs to the Syslog server. Conducting a packet capture would only allow you to find the server actively transmitting data during the period of time you are capturing. Conducting a service discovery scan would not identify which servers are running which operating systems effectively. For example, if you see that the Apache web service is running on port 80, it doesn't indicate running Linux or Windows as the underlying server.

29. Question

What nmap switch would you use to determine which UDP ports are open on a targeted network?

- -sP
- -sS
- **-sU**
- -sN

Unattempted

OBJ-2.2: In nmap, the -sU flag is used to scan UDP ports. The -sS flag will only scan TCP ports using an SYN scan. The -sP flag is a legacy (and depreciated) command for a ping scan. The -sN flag is used to conduct a TCP NULL scan.

30. Question

Which of the following is a DNS record type?

- DHCP
- **PTR**
- TTL
- LDAP

Unattempted

OBJ-2.1: There are several types of DNS records, including A, AAAA, CNAME, PTR, SVR, and TXT. PTR records are used for the Reverse DNS (Domain Name System) lookup. Using the IP address, you can get the associated domain/hostname. An A record should exist for every PTR record.

31. Question

Your company, HackMe Incorporated, is a US-based company specializing in conducting penetration tests for large corporations. Big Corp has recently asked you to perform a penetration test of its offices in Saudi Arabia and Iran. The penetration test would include both remote attacks and on on-site USB key drop attack. Which of the following MUST you investigate BEFORE you begin to negotiate the contract for this engagement?

- Budget allocate to the penetration test
- Support resources available to your team
- Type of threat actor your team will emulate
- **Export restrictions that may apply to your tools**

Unattempted

OBJ-9.1: The United States has export restrictions that govern the shipment or transfer of software, technology, services, and other controlled items outside of the United States borders. The Export Administration Regulations (EAR) is regulated by the Bureau of Industry and Security (BIS) within the U.S. Department of Commerce. The EAR may control the export, re-export, or transfer of items such as software, hardware, algorithms, and other technical items you may require for your on-site penetration test. Exports can include the transfer of a physical product from inside the US to an external location and other actions. The simple act of releasing technology to someone other than a US citizen or lawful permanent resident within the United States is deemed an export. This includes making available software for electronic transmission that can be received by individuals outside the US.

32. Question

Which of the following tools would you use to audit a multi-cloud environment?

- Prowler
- **ScoutSuite**
- Pacu
- OpenVAS

Unattempted

OBJ-8.1: ScoutSuite is used to audit instances and policies created on multi-cloud platforms. Prowler is a cloud auditing tool, but it can only be used on AWS. Pacu is an exploitation framework that is used to test the security configurations of an AWS account. OpenVAS is a general-purpose vulnerability scanner but does not deal with cloud-specific issues.

33. Question

During your reconnaissance, you have determined that your client's employees all use Android smartphones that connect back to the corporate network over a secure VPN connection. Which of the following methods would MOST likely be the best method for exploiting these?

- **Use social engineering to trick a user into opening a malicious APK**
- Use web-based exploits against the devices web interfaces
- Identify a jailbroken device for easy exploitation
- Use a tool like ICSSPLOIT to target specific vulnerabilities

Unattempted

OBJ-7.1: When targeting mobile devices, you must first determine if the company uses iPhones or Android-based devices. If they are using Android-based devices, you can use social engineering to trick a user into installing a malicious APK. As a penetration tester, you can create a malicious APK using msfvenom in the Metasploit framework. The user can install it directly from your website instead of the Google Play store.

34. Question

A technician just completed the second phase of their scans using Firewalk and the following output was displayed on their terminal:

-=-=-=-=-

TCP port 21 – no response

TCP port 22 – no response

TCP port 23 – Time-to-live exceeded

-=-=-=-=-

Based on these scan results, which of the following statements are true?

- Firewall is blocking ports 21 through 23 and a service on the target is listening on port 23
- A TTL response error indicates port 23 was able to make a connection to the target
- No response from port 21 and 22 indicates services are not running on the target
- **Port 23 was not blocked at the firewall because the scan on port 23 passed through the filtering device**

Unattempted

OBJ-2.2: Firewalk is a scanning tool that sends TCP or UDP packets with a TTL one greater than the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. If the gateway host does not allow the traffic, it will likely drop the packets and no response will be sent. Therefore, if a TTL exceeded message is received, this indicates that the associated port is being filtered by a firewall and not the gateway itself.

35. Question

During a security audit, you discovered that customer service employees have been sending unencrypted confidential information to their personal email accounts via email. What technology could you employ to detect these occurrences in the future and send an automated alert to the security team?

- UTM
- MDM
- **DLP**
- SSL

Unattempted

OBJ-7.1: Data loss prevention (DLP) software detects potential data breaches/data exfiltration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in-use, in-motion, and at-rest. This can be configured to detect and alert on future occurrences of this issue. Secure Socket Layer (SSL) is a distraction in this question since the questions asked about information being sent unencrypted. The connection between the client and the email server could be encrypted using SSL. However, the information is still be sent to an employee's personal email account, which equates to a loss of control over the

company's confidential data. Mobile Device Management (MDM) software is used for the configuration and securing of mobile devices like smartphones and tablets. Unified Threat Management (UTM) is a device that combines the functions of a firewall, anti-malware solution, and IDS into a single piece of hardware. Some UTM's may provide a DLP functionality, but the answer of a DLP is a better answer to this question.

36. Question

Which of the following is true concerning LM hashes?

- **LM hashes are not generated when the password length exceeds 15 characters**
- LM hashes consist of 48 hexadecimal characters
- Uppercase characters in the password are converted to lowercase
- LM hashes are based on AES128 cryptographic standard

Unattempted

OBJ-3.2: LM hash, also known as LanMan hash or LAN Manager hash, is a compromised password hashing function. This was the primary hash that Microsoft LAN Manager and Microsoft Windows versions before Windows NT used to store user passwords. Support for the legacy LAN Manager protocol continued in later versions of Windows for backward compatibility. Still, it was recommended by Microsoft to be turned off by administrators due to the LM hash's weak strength. LM hashes are not generated when the password length exceeds 15 characters since it is stored as a 16-byte value.

37. Question

The network administrator noticed that the border router has high network capacity loading during non-working hours. This load is causing web services outages. Which of the following is the MOST likely cause of the issue?

- Session hijacking
- Evil twin
- ARP cache poisoning
- **Distributed DoS**

Unattempted

OBJ-4.3: Distributed Denial of Service (DDoS) is when a computer or multiple computers are compromised due to a network breach or virus attack. This kind of attack can impact the network and cause outages or

slowness if your workstation is affected and acting as part of a botnet.

38. Question

Which of the following provides origin authenticity through source authentication, data integrity through hash functions, and confidentiality through encryption protection for IP packets?

- DES
- SHA
- **IPSEC**
- CRC

Unattempted

OBJ-9.1: Internet Protocol Security (IPSec) is a network protocol that encrypts and authenticates data sent over a network. All other choices offer encryption or authentication.

39. Question

Which of the following is the most difficult to confirm with an external vulnerability scan?

- Unpatched web server
- Cross-site scripting (XSS)
- Cross-site request forgery (XSRF/CSRF)
- **Blind SQL injection**

Unattempted

OBJ-3.1: Vulnerability scanners typically cannot confirm that a blind SQL injection with the execution of code has previously occurred. XSS and CSRF/XSRF are typically easier to detect because the scanner can pick up information that proves a successful attack. The banner information can usually identify unpatched servers.

40. Question

A system administrator wants to verify that external IP addresses cannot collect software versioning from servers on the network. Which of the following should the system administrator do to confirm the network is protected?

- Use nmap to query known ports
- **Analyze packet captures**
- Utilize netstat to locate active connections
- Review the ID3 logs on the network

Unattempted

OBJ-2.3: Captured packets show you the information that was traveling through certain files, etc. Packet sniffers detail the information they've received, so working through those shows if the external network shows or details software versions.

41. Question

Your company has just announced a change to an "API first" model of software development. As a cybersecurity analyst, you are immediately concerned about the possibility of an insecure deserialization vulnerability in this model. Which of the following is the primary basis for an attack against this vulnerability?

- **Accepting serialized objects from untrusted sources or the use of serialized non-primitive data may lead to remote code execution**
- Insufficient logging and monitoring makes it impossible to detect when insecure deserialization vulnerabilities are exploited
- Lack of input validation could allow for a SQL attack
- Lack of input validation could lead to a cross-site scripting attack

Unattempted

OBJ-5.2: When implementing an API, objects in memory from one computer can be serialized and passed to another for deserialization. If the API user is malicious, they may create a fictitious object, appropriately serialize it, and then send it through the API for execution. The only model for defeating this approach is to allow the API to be exposed to trusted sources or to not serialize anything with potentially executable source code (i.e., non-primitive data types). Cross-site scripting and SQL attacks are not a concern for an API first model. While stuffiest logging and monitoring would prevent an analyst from detecting if a deserialization vulnerability was exploited, these alone would not be the basis for an attack against deserialization.

42. Question

Which of the following hashing algorithms results in a 160-bit fixed output?

- NTLM
- MD-5
- SHA-2
- **SHA-1**

Unattempted

OBJ-9.1: SHA-1 creates a 160-bit fixed output. SHA-2 creates a 256-bit fixed output. NTLM creates a 128-bit fixed output. MD-5 creates a 128-bit fixed output.

43. Question

Which of the following attacks would most likely be used to create an inadvertent disclosure of information from an organization's database?

- **SQL injection**
- Buffer overflow
- Cross-site scripting
- Denial of service

Unattempted

OBJ-5.3: A SQL injection poses the most direct and more impactful threat to an organization's database. A SQL injection could allow the attacker to execute remote commands on the database server and lead to sensitive information disclosure. A buffer overflow attack attempts to overwrite the memory buffer to send additional data into adjacent memory locations. A buffer overflow attack might target a database server, but it isn't intended to disclose information directly. Instead, a buffer overflow attack may be used to gain initial access to a server and allow for other malicious code running. A denial of service targets the availability of the information by attempting to take the server offline. A cross-site scripting attack typically is focused on the user, not the server or database.

44. Question

Which of the following types of attacks involves changing the system's MAC address before it connects to a wireless network?

- Zombie

- Botnet
- **Spoofing**
- DDoS

Unattempted

OBJ-4.1: Spoofing is an attack where the attacker disguises their identity. Examples of spoofing include changing their MAC address (MAC spoofing), their IP address (IP spoofing), or their email address (most commonly used during a phishing campaign).

45. Question

Which type of threat actor can accidentally or inadvertently cause a security incident in your organization?

- **Insider threat**
- APT
- Organized Crime
- Hacktivist

Unattempted

OBJ-4.2: An insider threat is a type of threat actor assigned privileges on the system that cause an intentional or unintentional incident. Insider threats can be used as unwitting pawns of external organizations or make crucial mistakes that can open up exploitable security vulnerabilities. Hacktivists, Organized Crimes, and advanced persistent threats (APT) entities do not accidentally or unwittingly target organizations. Instead, their actions are deliberate in nature. A hacktivist is an attacker that is motivated by a social issue or political cause. Organized crime is a type of threat actor that uses hacking and computer fraud for commercial gain. An advanced persistent threat (APT) is a type of threat actor who can obtain, maintain, and diversify access to network systems using exploits and malware.

46. Question

You are conducting a static code analysis of a Java program. Consider the following code snippet:

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

String custname = request.getParameter("customerName");

String query = "SELECT account_balance FROM user_data WHERE user_name = ? ";

PreparedStatement pstmt = connection.prepareStatement(query);

pstmt.setString(1, custname);

ResultSet results = pstmt.executeQuery( );

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

Based on the code above, what type of secure coding practice is being used?

- Input validation
- **Parameterized queries**
- Session management
- Authentication

Unattempted

OBJ-5.3: A parameterized query (also known as a prepared statement) is a means of pre-compiling a SQL statement so that all you need to supply are the "parameters" (think "variables") that need to be inserted into the statement for it to be executed. It's commonly used as a means of preventing SQL injection attacks. This code snippet is an example of a Java implementation of a parameterized query. Input validation would involve the proper testing of any input supplied by a user to an application. Since the first line takes the custname input without any validation, this is not an example of the input validation secure coding practice. Session management refers to the process of securely handling multiple requests to a web-based application or service from a single user or entity. Authentication is the act of proving an assertion, such as the identity of a computer system user. This code snippet is neither a form of session management nor authentication. You should not fully understand what this code is doing for the exam, but you should understand what it is not doing. There is nothing in the code that indicates session management or receiving usernames and passwords. Therefore, we can rule out session management and authentication. This leaves us with input validation and parameterized queries as our best options. Based on the code, we see the word query multiple times, which should be a hint that the answer is a parameterized query even if you can't read this Java code fully.

47. Question

Review the following packet captured at your NIDS:

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

23:12:23.154234 IP 86.18.10.3:54326 > 71.168.10.45:3389 Flags [P.], Seq 1834:1245, ack1, win 511, options [nop,nop, TS val 263451334 erc 482862734, length 125

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

After reviewing the packet above, you discovered there is an unauthorized service running on the host. Which of the following ACL entries should be implemented to prevent further access to the unauthorized service while maintaining full access to the approved services running on this host?

- **DENY TCP ANY HOST 71.168.10.45 EQ 3389**

- DENY IP HOST 86.18.10.3 EQ 3389
- DENY TCP ANY HOST 86.18.10.3 EQ 25
- DENY IP HOST 71.168.10.45 ANY EQ 25

Unattempted

OBJ-4.5: Since the question asks you to prevent unauthorized service access, we need to block port 3389 from accepting connections on 71.168.10.45 (the host). This option will deny ANY workstation from connecting to this machine (host) over the Remote Desktop Protocol service that is unauthorized (port 3389).

48. Question

A network administrator receives a call asking for assistance with connecting to the network. The person on the phone asks for the IP address, subnet mask, and VLAN required to access the network. What type of attack might this be?

- Zero-day attack
- VLAN hopping
- Spoofing
- **Social engineering**

Unattempted

OBJ-4.2: Social engineering is a type of attack on a network in which an attacker uses their confidence and their victims' gullibility to gain access. It is the only type of attack on a network that is directed towards the human element. The human interaction with the network administrator makes the other three answers incorrect.

49. Question

You are reverse engineering a piece of malware recovered from a retailer's network for analysis. They found that the malicious code was extracting track data from their customer's credit cards during processing. Which of the following types of threats would you classify this malware as?

- Ransomware
- Rootkit
- **POS malware**

Keylogger

Unattempted

OBJ-3.3: Point-of-sale malware (POS malware) is usually a type of malicious software (malware) that is used by cybercriminals to target point of sale (POS) and payment terminals with the intent to obtain credit card and debit card information, a card's track 1 or track 2 data and even the CVV code, by various man-in-the-middle attacks, that is the interception of the processing at the retail checkout point of sale system. Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. Keyloggers are a type of monitoring software designed to record keystrokes made by a user. These keyloggers can record the information you type into a website or application and send to back to an attacker. A rootkit is a malware class that modifies system files, often at the kernel level, to conceal its presence.

50. Question

Cybersecurity analysts are experiencing some issues with their vulnerability scans aborting because the previous day's scans are still running when the scanner attempts to start the current day's scans. Which of the following recommendations is LEAST likely to resolve this issue?

Reduce the scope of scans

Reduce the frequency of scans

Add another vulnerability scanner

Reduce the sensitivity of scans

Unattempted

OBJ-3.1: If the cybersecurity analyst were to reduce the scans' sensitivity, it still would not decrease the time spent scanning the network and could alter the effectiveness of the results received. In this scenario, the scans, as currently scoped, are taking more than 24 hours to complete with the current resources. The analyst could reduce the scans' scope, thereby scanning fewer systems or vulnerabilities signatures and taking less time to complete. Alternatively, the analyst could reduce the scans' frequency by moving to a less frequent schedule, such as one scan every 48 hours or one scan per week. The final option would be to add additional vulnerability scanners to the process. This would allow the two scanners to work together to divide the workload and complete the task within the 24-hour scan frequency currently provided.

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 →

Privacy Policy