SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 4

Your results are here!! for" CEHv11 Practice Test 4 "

0 of 50 questions answered correctly

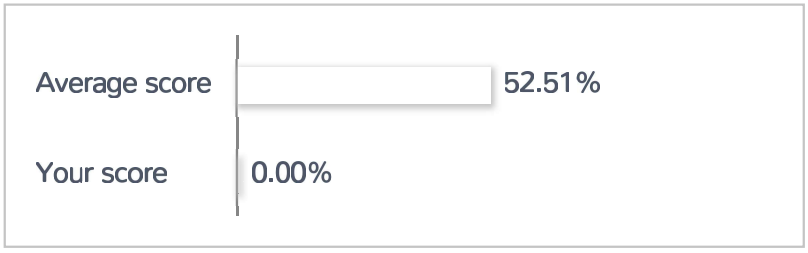
Your time: 00:00:02

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

An organization is currently accepting bids for a contract that will involve penetration testing and reporting. The organization is asking all bidders to provide proof of previous penetration testing and reporting experience. One contractor decides to print out a few reports from some previous penetration tests that they performed. What could have occurred as a result of this contractor's actions?

- **The contractor may have inadvertently exposed numerous vulnerabilities they had found at other companies on previous assessments**
- The company accepting the bids will hire the contractor because of the quality of the reports he submitted with his bid
- The contractor will have their bid accepted with a special pay bonus because of their excellent work on previous penetration tests
- The organization accepting the bids will want to use the reports as an example of the format for all bidders to use in the future

Unattempted

OBJ-1.1: Pentesters should never disclose any information from previous penetration tests to anyone outside of the assessed organization since this could expose the vulnerability found. This non-disclosure is usually outlined in the original contract and scope of work. If the contractor wishes to provide a sample report, then the report should be created specifically for the contract and only include information from a sample/test network, not a previous customer's assessment. This could also be in breach of the NDA between the pentester and the organization, as well.

2. Question

You are analyzing the logs of a web server. Consider the following log sample:

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

84.55.41.57- – [14/Apr/2016:08:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=1 AND (SELECT 6810 FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0

(Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR 3.5.30729)"
84.55.41.57- – [14/Apr/2016:08:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=(SELECT 7505 FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR 3.5.30729)"
84.55.41.57- – [14/Apr/2016:08:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=(SELECT CONCAT(0x7171787671,(SELECT (ELT(1399=1399,1))),0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR 3.5.30729)"
84.55.41.57- – [14/Apr/2016:08:22:27 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=1 UNION ALL SELECT CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL– HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR 3.5.30729)"
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Based on the logs above, which of the following type of attacks was conducted against this server?

- SQL injection
- XML injection
- Cross-site scripting
- Directory traversal

Unattempted

OBJ-5.3: SQL injection is a code injection technique that is used to attack data-driven applications. SQL injections are conducted by inserting malicious SQL statements into an entry field for execution. For example, an attacker may try to dump the contents of the database by using this technique. A common SQL injection technique is to insert an always true statement, such as 1 == 1, or in this example, 7 == 7. In this case, the SQL injection is evidenced by the SQL statements being sent to the web application hosted by WordPress. XML Injection is an attack technique used to manipulate or compromise an XML application or service's logic. The injection of unintended XML content and/or structures into an XML message can alter the application's intended logic. 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. A directory traversal attack aims to access files and directories that are stored outside the webroot folder. By manipulating variables or URLs that reference files with "dot-dot-slash (../)" sequences and its variations or using absolute file paths, it may be possible to access arbitrary files and directories stored on the file system, including application source code or configuration and critical system files.

3. Question

Which of the following secure coding best practices ensures a character like < is translated into the &lt string when writing to an HTML page?

- Session management
- **Output encoding**
- Error handling
- Input validation

Unattempted

OBJ-5.1: Output encoding involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example, translating the < character into the < string when writing to an HTML page. Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering the malfunction of various downstream components. Improper error handling can introduce various security problems where detailed internal error messages such as stack traces, database dumps, and error codes are displayed to an attacker. The session management implementation defines the exchange mechanism that will be used between the user and the web application to share and continuously exchange the session ID.

4. Question

A salesperson's laptop has become unresponsive after attempting to open a PDF in their email. A cybersecurity analyst reviews the IDS and anti-virus software for any alerts or unusual behavior but finds nothing suspicious. Which of the following threats would BEST classify this scenario?

- Ping of death
- PII exfiltration
- **Zero-day malware**
- RAT

Unattempted

OBJ-3.3: Based on the scenario provided, it appears that the laptop has become the victim of a zero-day attack. A zero-day attack is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of. This means that there will not be a signature available in the IDS or

anti-virus definition file. Therefore, it cannot be combatted with traditional signature-based detection methods. PII (personally identifiable information) exfiltration is the unauthorized copying, transfer, or retrieval of PII data from a computer or server. A ping of death is a type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer. A remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer. Based on the scenario's information, we do not have any indications that a ping packet was sent, that PII has been exfiltrated, or that the attack now has remote control of the laptop. Since neither the IDS nor anti-virus alerted on the PDF, it is most likely a form of a zero-day attack.

5. Question

An insurance company has developed a new web application to allow its customers to choose and apply for an insurance plan. You have been asked to help perform a security review of the new web application. You have discovered that the application was developed in ASP and used MSSQL for its backend database. You have been able to locate an application's search form and introduced the following code in the search input field:

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

IMG SRC=vbscript:msgbox("Vulnerable_to_Attack");> originalAttribute="SRC"

originalPath="vbscript:msgbox("Vulnerable_to_Attack ");>"

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

When you click submit on the search form, your web browser returns a pop-up window that displays Vulnerable_to_Attack. Which of the following vulnerabilities did you discover in the web application?

- Cross-site request forgery
- SQL injection
- Command injection
- **Cross-site scripting**

Unattempted

OBJ-5.2: This is a form of Cross-Site Scripting (XSS). Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. Attackers may use a cross-site scripting vulnerability to bypass access controls such as the same-origin policy. Cross-site request forgery (CSRF or XSRF) is a malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts. There are many ways in which a malicious website can transmit commands, such as specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests can all work without the user's interaction or even knowledge. 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. Command

injection is an attack in which the goal is to execute arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user-supplied data (forms, cookies, HTTP headers, etc.) to a system shell.

6. Question

Which of the following would a virtual private cloud infrastructure be classified as?

- Infrastructure as a Service
- Platform as a Service
- Software as a Service
- Function as a Service

Unattempted

OBJ-8.1: Infrastructure as a Service (IaaS) is a computing method that uses the cloud to provide any or all infrastructure needs. In a VPC environment, an organization may provision virtual servers in a cloud-hosted network. The service consumer is still responsible for maintaining the IP address space and routing internally to the cloud. Platform as a Service (PaaS) is a computing method that uses the cloud to provide any platform-type services. Software as a Service (SaaS) is a computing method that uses the cloud to provide users with application services. Function as a Service (FaaS) is a cloud service model that supports serverless software architecture by provisioning runtime containers to execute code in a particular programming language.

7. Question

Which of the following is exploited by an SQL injection to give the attacker access to a database?

- Operating system
- Firewall
- Web application
- Database server

Unattempted

OBJ-5.3: SQL injections target the data stored in enterprise databases by exploiting flaws in client-facing applications. These vulnerabilities being exploited are most often found in web applications. The database server or operating system would normally be exploited by a remote code execution, a buffer overflow, or another type of server-side attack. The firewall would not be subject to an SQL injection.

8. Question

Syed is developing a vulnerability scanner program for a large network of sensors to monitor his company's transcontinental oil pipeline. What type of network is this?

- BAS
- CAN
- SoC
- **SCADA**

Unattempted

OBJ-7.2: SCADA (supervisory control and data acquisition) networks work off an ICS (industry control system) and maintain sensors and control systems over large geographic areas. A building automation system (BAS) for offices and data centers ("smart buildings") can include physical access control systems, but also heating, ventilation, and air conditioning (HVAC), fire control, power and lighting, and elevators and escalators. Vehicular networks are called a controller area network (CAN). A CAN uses serial communication buses to connect electronic control units and other subsystems in cars and unmanned aerial vehicles (UAV). System-on-chip (SoC) is a design where all these processors, controllers, and devices are provided on a single processor die or chip.

9. Question

Jason is conducting a penetration test against an organization's Windows network. He then enters a command into the shell and receives the following output:

-=-=-=-=-=-

C:\Users\jason\Desktop> wmic service get name,pathname,displayname,startmode | findstr /i auto | findstr /i /v "C:\Windows\\" | findstr /i /v """"

VulnerableService Some Vulnerable Service C:\Program Files\A Subfolder\B Subfolder\SomeExecutable.exe

-=-=-=-=-=-

Based on the output above, which of the following types of vulnerabilities does this Windows system contain?

- **Unquoted service path**
- Unsecure file/folder permissions
- Clear text credentials in LDAP
- Writeable services

Unattempted

OBJ-2.3: This Windows machine contains an unquoted service path vulnerability, as shown in the output. If a service is created with an executable path that contains spaces and is not enclosed within quotes, then an unquoted service path vulnerability exists. In Windows, if the service is not enclosed within quotes and is having spaces, it would handle the space as a break and pass the rest of the service path as an argument. If the service involved has SYSTEM privileges, an attacker could exploit this vulnerability and gain SYSTEM level access. This command finds the service name, executable path, the display name of the service, and auto starts in all the directories except C:\Windows\ (since by default there is no such service that has spaces and is unquoted in this folder). As shown in the output, the service called "VulnerableService" has an unquoted service path.

10. Question

You have been asked to recommend a capability to monitor all of the traffic entering and leaving the corporate network's default gateway. Additionally, the company's CIO requests to block certain content types before it leaves the network based on operational priorities. Which of the following solution should you recommend to meet these requirements?

- Install a firewall on the router's internal interface and a NIDS on the router's external interface
- Configure IP filtering on the internal and external interfaces of the router
- Installation of a NIPS on both the internal and external interfaces of the router
- **Install a NIPS on the internal interface and a firewall on the external interface of the router**

Unattempted

OBJ-4.5: Due to the requirements provided, you should install a NIPS on the gateway router's internal interface and a firewall on the external interface of the gateway router. The firewall on the external interface will allow the bulk of the malicious inbound traffic to be filtered before reaching the network. Then, the NIPS can be used to inspect the traffic entering the network and provide protection for the network using signature-based or behavior-based analysis. A NIPS is less powerful than a firewall and could easily "fail open" if it is overcome with traffic by being placed on the external interface. The NIPS installed on the internal interface would also allow various content types to be quickly blocked using custom signatures developed by the security team. We wouldn't want to place the NIPS on the external interface in the correct choice for the same reasons. We also wouldn't choose to install a NIPS on both the internal and external connections. IP filtering on both interfaces of the router will not provide the ability to monitor the traffic or to block traffic based on content type. Finally, we would not want to rely on a NIDS on the external interface alone since it can only monitor and not provide the content blocking capabilities needed.

11. Question

A disgruntled employee executes a man-in-the-middle attack on the company network. Layer 2 traffic destined for the gateway is redirected to the employee's computer. What type of attack is this an example of?

- Evil twin
- IP spoofing
- **ARP cache poisoning**
- Amplified DNS attack

Unattempted

OBJ-4.1: ARP poisoning reroutes data and allows an attacker to intercept packets of data intended for another recipient. ARP attacks can be sent from any host on the local area network, and the goal is to associate the host so that any traffic meant for something else will instead go directly to the attacker's PC.

12. Question

What must be developed to show security improvements over time?

- Testing tools
- Reports
- **Metrics**
- Taxonomy of vulnerabilities

Unattempted

OBJ-1.1: Metrics are a method of measuring something over time. If you wish to show the effect of security improvements over time, creating metrics would be a good option. For example, you may wish to look at the number of unpatched and known vulnerabilities. As this number decreases, your network would be considered to have improved security. Reports and testing tools alone cannot show progress. You must have measurable results using metrics.

13. Question

Your company is adopting a cloud-first architecture model. Management wants to decommission the on-premises SIEM your analysts use and migrate it to the cloud. Which of the following is an issue with using this approach?

- The company will have less control over the SIEM
- **Legal and regulatory issues may prevent data migration to the cloud**
- The company will be dependent on the cloud provider's backup capabilities
- A VM escape exploit could allow an attacker to gain access to the SIEM

Unattempted

OBJ-8.1: If there are legal or regulatory requirements that require the company to host their security audit data on-premises, then moving to the cloud will not be possible without violating applicable laws. For example, some companies must host their data within their national borders, even if migrating to the cloud. The other options presented are all low risk and can be overcome with proper planning and mitigations. Most cloud providers have degrees of redundancy far above what any individual on-premises provider will be able to generate, making the concern over backups a minimal risk. If the SIEM is moved to a cloud-based server, it could still be operated and controlled in the same manner as the previous on-premise solution using a virtualized cloud-based server. While a VM or hypervisor escape is possible, they are rare and can be mitigated with additional controls.

14. Question

While conducting a static analysis source code review of a program, you see the following line of code:

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

String query = “SELECT * FROM CUSTOMER WHERE CUST_ID=’” + request.getParameter(“id”) + “‘”;

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

What is the issue with the largest security issue with this line of code?

- This code is vulnerable to a buffer overflow attack
- The * operator will allow retrieval of every data field about this customer in the CUSTOMER table
- **An SQL injection could occur because input validation is not being used on the id parameter**
- The code is using parameterized queries

Unattempted

OBJ-5.3: This code takes the input of “id” directly from a user or other program without conducting any input validation. This could be exploited and used as an attack vector for an SQL injection. If a malicious user can alter the ID source, it might get replaced with something like’ or ‘1’ =’1. This will cause the SQL statement to become: “SELECT * FROM CUSTOMER WHERE CUST_ID=” or ‘1’=’1’”. Because ‘1’ always equals ‘1’, the where clause will always return ‘true,’ meaning that EVERY record in the database could now become available to the attacker. When creating SQL statements, there are reasons for and against the use of the *

operator. Its presence alone does not necessarily indicate a weakness. With only one line of code being reviewed, you cannot make any statement about whether it is vulnerable to a buffer overflow attack. You do not see the declaration values for the initialization of the id variable. This code is not using parameterized queries, but if it did, then it would eliminate this vulnerability. A parameterized query is a type of output encoding that relies on prepared statements to reduce the risk of an SQL injection.

15. Question

Which of the following policies should be created to provide employees with the guidelines and limitations they must follow when using company-provided email, computers, and network access?

- GDPR
- DLP
- PII
- **AUP**

Unattempted

OBJ-1.1: An acceptable use policy (AUP) governs employees' use of company equipment and Internet services. Enforcing an acceptable use policy is important to protect the organization from the security and legal implications of employees (or customers) misusing its equipment. Typically, the policy will forbid the use of equipment to defraud, defame, or obtain illegal material. It is also likely to prohibit unauthorized hardware or software installation and to forbid actual or attempted intrusion (snooping) explicitly. An organization's acceptable use policy may forbid the use of Internet tools outside of work-related duties or restrict such use to break times.

16. Question

Which of the following encryption types was used by WPA to better secure wireless networks than WEP?

- IV
- AES
- **TKIP**
- CCMP

Unattempted

OBJ-6.1: Wi-Fi Protected Access (WPA) fixes most of the security problems with WEP. WPA still uses the RC4 cipher but adds a mechanism called Temporal Key Integrity Protocol (TKIP) to fix the issues with key generation.

17. Question

Stephane was asked to assess the technical impact of a reconnaissance performed against his organization. He has discovered that a third party has been performing reconnaissance by querying the organization's WHOIS data. Which category of technical impact should he classify this as?

- Medium
- **Low**
- High
- Critical

Unattempted

OBJ-2.1: This would be best classified as a low technical impact. Since WHOIS data about the organization's domain name is publicly available, it is considered a low impact. This is further mitigated by the fact that your company gets to decide what information is actually published in the WHOIS data. Since only publicly available information is being queried and exposed, this can be considered a low impact.

18. Question

What type of weakness is John the Ripper used to test during a technical assessment?

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

Unattempted

OBJ-3.2: John the Ripper is a free, open-source password cracking software tool. It tests the strength of passwords during a technical assessment. John the Ripper supports both dictionary and brute force attacks.

19. Question

The management at Steven's work is concerned about rogue devices being attached to the network. Which of the following solutions would quickly provide the most accurate information that Steve could use to identify rogue devices on a wired network?

- **Router and switch-based MAC address reporting**
- A discovery scan using a port scanner
- A physical survey
- Reviewing a central administration tool like a SCCM

Unattempted

OBJ-2.1: The best option is MAC address reporting from a source device like a router or a switch. If the company uses a management system or inventory process to capture these addresses, then a report from one of these devices will show what is connected to the network even when they are not currently in the inventory. This information could then be used to track down rogue devices based on the physical port connected to a network device.

20. Question

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

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

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. An evil twin is a copy of a legitimate access point, not necessarily giving it access to a specific network or even the internet.

21. Question

Which of the following actions should be done FIRST after forensically imaging a hard drive for evidence in an investigation?

- Encrypt the image file to ensure it maintains data integrity
- Digitally sign the image file to provide non-repudiation of the collection
- Encrypt the source drive to ensure an attacker cannot modify its contents
- **Create a hash digest of the source drive and the image file to ensure they match**

Unattempted

OBJ-9.1: The first thing that must be done after acquiring a forensic disk image is to create a hash digest of the source drive and destination image file to ensure they match. A critical step in the presentation of evidence will be to prove that analysis has been performed on an identical image to the data present on the physical media and that neither data set has been tampered with. The standard means of proving this is to create a cryptographic hash or fingerprint of the disk contents and any derivative images made from it. When comparing hash values, you need to use the same algorithm used to create the reference value. While encrypting the image files is a good security practice to maintain the data's confidentiality, it does not provide data integrity like a hash digest does. Once imaged, the source drive should not be altered or encrypted. Digitally signing the image file could serve the function of non-repudiation, but it is an uncommon practice and not required to be performed.

22. Question

What command could be used to list the active services from the Windows command prompt?

- sc query type= running
- sc config
- **sc query**
- sc query \\servername

Unattempted

OBJ-3.2: Windows uses the sc query to display information about the running service. It is part of the Service Control command-line tool, known as sc. The sc config command will modify the value of a service's entries in the registry and the Service Control Manager database. The sc query command will obtain and display information about the specified service, driver, type of service, or driver type. By entering just the sc query, the command will return the information on the active services only. By using the type=running option, only the information on the running service will be displayed. If the command sc query \\servername is used, then the remote server's active services (\\servername) will be displayed.

23. Question

Your company has been contracted to develop an Android mobile application for a major bank. You have been asked to verify the security of the Java function's source code below:

```
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
int verifyAdmin(String password)
{
    if (password.equals("mR7HCS14@31&#")) {
     return 0;
   }
   return 1;
}
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

Which of the following vulnerabilities exist in this application's authentication function based solely on the source code provided?

- The function is using hard-coded credentials to verify the password entered by the user
- The function is vulnerable to an SQL injection attack
- The function is using parameterized queries
- The function is vulnerable to a buffer overflow attack

Unattempted

OBJ-7.1: The function uses hard-coded credentials in the function, which is an insecure practice that can lead to compromise. The password for the application is shown in the source code as mR7HCS14@31&#. Even if this was obfuscated using encoding or encryption, it is a terrible security practice to include hard-coded credentials in the application since an attacker can reverse-engineer them. In this case, it could be used to rob the bank or its customers! There is no evidence of a SQL injection or buffer overflow attack vulnerability based on the code being shown. In fact, this code doesn't even show any SQL or ability to connect to an SQL database. We cannot see the variable initiation in this code, either, so we cannot determine if it is vulnerable to a buffer overflow attack. Finally, a parameterized query is a security feature, not a vulnerability, and this source code does not show any evidence of parameterized queries being used.

24. Question

Due to new regulations, your organization's CIO has the information security team institute a vulnerability management program. What framework would BEST support this program's establishment?

- SDLC

- NIST
- OWASP
- SANS

Unattempted

OBJ-3.1: NIST (National Institute of Standards and Technology) produced a useful patch and vulnerability management program framework in its Special Publication (NIST SP 800-40). It would be useful during the program's establishment and provide a series of guidelines and best practices. SANS is a company specializing in cybersecurity and secure web application development training and sponsors the Global Information Assurance Certification (GIAC). The SDLC is the software development lifecycle. It is a method for dividing programming projects into separate phases. The Open Web Application Security Project (OWASP) is a community effort that provides free access to many secure programming resources. The resources provided include documentation on web app vulnerabilities and mitigation tactics, software tools used to identify and handle threats that target web applications, frameworks for secure development life cycle implementation, frameworks for penetration testing web apps, general secure coding best practices, guidelines for specific web-based languages, and more.

25. Question

Which cloud computing concept is BEST described as focusing on the replacement of physical hardware at a customer's location with cloud-based resources?

- IaaS
- PaaS
- SECaaS
- SaaS

Unattempted

OBJ-8.1: Infrastructure as a Service (Iaas) is focused on moving your servers and computers into the cloud. If you purchase a server in the cloud and then install and manage the operating system and software, this is Iaas.

26. Question

An attacker sends an email out to 100,000 random email addresses. In the email the attacker sent, it claims that "Your Bank of America account is locked out. Please click here to reset your password." Which of the following attack types is being used?

- **Phishing**
- Whaling
- Vishing
- Spear phishing

Unattempted

OBJ-4.2: Phishing relies on sending out a large volume of email to a broad set of recipients in the hopes of collecting the desired action or information. Spearphishing involves targeting specific individuals using well-crafted emails to gather information from a victim.

27. Question

You are planning to exploit a network-based vulnerability against an organization as part of a penetration test. You attempted to connect your laptop to the network jack in their conference room. You found yourself in the highly restricted VLAN that the organization allows its visitors to connect to when conducting presentations. This VLAN only allows you to access the internet, not the internal network. You decide you need to conduct VLAN hopping. Which of the following methods would be MOST likely to succeed?

- Harvest the user credentials of an employee and use those to connect
- Spoof the MAC address of the room's VOIP phone to your laptop
- **Poison or overflow the MAC table of the switch**
- Connect a wireless access point to the conference room's network jack

Unattempted

OBJ-4.1: VLAN hopping is the act of illegally moving from one VLAN to another. A VLAN (virtual LAN) is a logical grouping of switch ports extending across any number of switches on an Ethernet network. One of the most common VLAN hopping methods is to overflow the MAC table on a vulnerable switch. When this occurs, the switch defaults to operating as a hub and repeats all frames being received through all of its ports. This “fail open” method ensures the network can continue to operate, but it is a security risk that can be exploited by the penetration tester.

28. Question

Your organization has recently been the target of a spearphishing campaign. You have identified the website associated with the link in the spearphishing emails and want to block it. Which of the following techniques would be the MOST effective in this situation?

- URL filter
- Quarantine
- Application blacklist
- Containment

Unattempted

OBJ-4.2: A URL filter can be used to block a website based on its website address or universal resource locator (URL). This is not a containment technique but a blocking and filtering technique. Quarantine would be used against an infected machine, and it would not be effective against trying to block access to a given website across the entire organization. An application blacklist is used to prevent an application from running, so this cannot be used to block a single malicious or suspicious website or URL.

29. Question

Which of the following technologies combines the functionality of a firewall, malware scanner, and other security appliances into one device?

- IDS
- Syslog
- IPS
- UTM

Unattempted

OBJ-4.5: A Unified Threat Management (UTM) appliance is one that enforces a variety of security-related measures, combining the work of a firewall, malware scanner, and intrusion detection/prevention. A UTM centralizes the threat management service, providing simpler configuration and reporting than isolated applications spread across several servers or devices.

30. Question

Your company is setting up a system to accept credit cards in their retail and online locations. Which of the following compliance types should you be MOST concerned with dealing with credit cards?

- PCI-DSS
- PII

- GDPR
- PHI

Unattempted

OBJ-1.1: The Payment Card Industry Data Security Standard (PCI DSS) applies to companies of any size that accept credit card payments. If your company intends to accept card payment and store, process, and transmit cardholder data, you need to securely host your data and follow PCI compliance requirements.

31. Question

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

- Third-party hosted
- Off-site
- External
- **Internal**

Unattempted

OBJ-4.2: An internal target type means that assets can be accessed from within the organization. This can either be physically or logically from within the network, and it best simulates an insider threat. This target type can also be used to simulate an external hacker who has gained credentials on the network, such as through the use of a spearphishing attack.

32. Question

A cybersecurity analyst is preparing to run a vulnerability scan on a dedicated Apache server that will be moved into a DMZ. Which of the following vulnerability scans is most likely to provide valuable information to the analyst?

- **Web application vulnerability scan**
- Port scan
- Database vulnerability scan
- Network vulnerability scan

Unattempted

OBJ-5.1: Since Apache is being run on the scanned server, this indicates a web server. Therefore, a web application vulnerability scan would be the most likely to provide valuable information. A network vulnerability scan or port scan can provide valuable information against any network-enabled server. Since an Apache server doesn't contain a database by default, running a database vulnerability scan is not likely to provide any valuable information to the analyst.

33. Question

Which of the following is a best practice that should be followed when scheduling vulnerability scans of an organization's data center?

- Schedule scans to be conducted evenly throughout the day
- Schedule scans to begin at the same time every day
- **Schedule scans to run during periods of low activity**
- Schedule scans to run during peak times to simulate performance under load

Unattempted

OBJ-3.1: For the best results, the scans should be scheduled during periods of low activity. This will help to reduce the negative impact of scanning on business operations. The other three options all carry a higher risk of causing disruptions to the network or its business operations.

34. Question

Sarah has reason to believe that systems on her network have been compromised by an APT. She has noticed many file transfers outbound to a remote site via TLS-protected HTTPS sessions from unknown systems. Which of the following techniques would most likely detect the APT?

- **Endpoint forensics**
- Network forensics
- Network traffic analysis
- Endpoint behavior analysis

Unattempted

OBJ-3.3: An advanced persistent threat (APT) is a stealthy computer network threat actor, typically a nation-state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. APTs usually send encrypted traffic so that they are harder to detect

through network traffic analysis or network forensics. This means that you need to focus on the endpoints to detect an APT. Unfortunately, APTs are very sophisticated, so endpoint behavioral analysis is unlikely to detect them easily, so Sarah will need to conduct endpoint forensics as her most likely method to detect an APT and their associated infections on her systems.

35. Question

Your organization's networks contain 4 subnets: 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0. Using nmap, how can you scan all 4 subnets using a single command?

- nmap -Pn 10.0.0.0,1.0,2.0,3.0
- **nmap -Pn 10.0.0-3.0**
- nmap -Pn 10.0.0.0/23
- nmap -Pn 10.0.0.0/25

Unattempted

OBJ-2.2: The simplest way to scan multiple subnets adjacent to each other is to use the -Pn tells the command to conduct a host-only scan of every IP in this target space without using ping. Using the dash (-) in the IP address means to scan "this network through this network." So, 10.0.0-3.0 will scan every IP from 10.0.0.0 through 10.0.3.255.

36. Question

On your lunch break, you walked down to the coffee shop on the corner. You open your laptop and connect to their wireless network. After a few minutes of surfing the Internet, a pop-up is displayed on your screen. You close the pop-up, finish your lunch break, shut down the laptop, and put it back into your backpack. When you get back to the office, you take out the laptop and turn it on, but instead of your normal desktop background, you are greeted by a full-screen image with a padlock and a message stating you have to pay 1 BTC to regain access to your personal files. What type of malware has infected your laptop?

- Spyware
- **Ransomware**
- Rootkit
- Trojan

Unattempted

OBJ-3.3: This scenario is describing a ransomware attack. Your personal files are being held hostage and will not be released unless you pay a ransom (in this case, 1 BTC). You should restore your machine from a known good backup and restore your personal files from the backup, as well. You should not pay the ransom since the attackers usually still will not unlock your files.

37. Question

An internet marketing company decided that they didn't want to follow the rules for GDPR because it would create too much work for them. They wanted to buy insurance, but no insurance company would write them a policy to cover any fines received. They considered how much the fines might be and decided to ignore the regulation and its requirements. Which of the following risk strategies did the company choose?

- Avoidance
- Mitigation
- **Acceptance**
- Transference

Unattempted

OBJ-1.1: The internet marketing company initially tried to transfer the risk (buy insurance) but then decided to accept the risk. To avoid the risk, the company would have changed how it did business or would prevent European customers from signing up on their mailing list using geolocation blocks.

38. Question

A security analyst is conducting a log review of the company's web server and found two suspicious entries:

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

[12Nov2020 10:07:23] "GET /logon.php?user=test'+oR+7>1%20—HTTP/1.1" 200 5825 [12Nov2020 10:10:03] "GET /logon.php?user=admin';%20—HTT{/1.1" 200 5845

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

The analyst contacts the web developer and asks for a copy of the source code to the logon.php script. The script is as follows:

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

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

Based on source code analysis, which type of vulnerability is this web server vulnerable to?

- LDAP injection

- SQL injection
- Directory traversal
- Command injection

Unattempted

OBJ-5.3: Based on the log entries, it appears the attack was successful in conducting a SQL injection. Notice the escape character (') used in the log. A connection to the MySQL database is being used in the script, which could be exploited since no input validation is being performed. Command injection is an attack in which the goal is to execute arbitrary commands on the host operating system via a vulnerable application. SQL injection is a specific type of command injection. LDAP injection is a code injection technique used to exploit web applications that could reveal sensitive user information or modify information represented in the LDAP (Lightweight Directory Access Protocol) data stores. Directory traversal or Path Traversal is an HTTP attack that allows attackers to access restricted directories and execute commands outside of the web server's root directory.

39. Question

Your organization has just migrated to provisioning its corporate desktops as virtual machines and accessing them using thin clients. The organization believes this will enhance security since the desktop can be rewritten with a new baseline image every time the user logs into it. Based on this scenario, which of the following technologies has the organization adopted?

- VPC
- VPN
- VDI
- UEBA

Unattempted

OBJ-8.1: Virtual desktop infrastructure (VDI) is a virtualization implementation that separates the personal computing environment from a user's physical computer. Virtual private cloud (VPC) is a private network segment made available to a single cloud consumer on a public cloud. A virtual private network (VPN) is a secure tunnel created between two endpoints connected via an insecure network, typically the internet. User and entity behavior analytics (UEBA) is a system that can provide an automated identification of suspicious activity by user accounts and computer hosts.

40. Question

A penetration tester is conducting an assessment of a wireless network that is secure using WPA2 Enterprise encryption. Which of the following are major differences between conducting reconnaissance of a wireless network versus a wired network? (SELECT TWO)

- [ ] Authentication
- [ ] MAC filtering
- [ ] Network access control
- [ ] Port security
- [ ] **Physical accessibility**
- [ ] **Encryption**

Unattempted

OBJ-6.1: Most wireless networks utilize end-to-end encryption, whereas wired networks do not. Physical accessibility is another major difference between wireless and wired networks since wireless networks can be accessed from a distance using powerful antennas. Authentication, MAC filtering, and network access control (NAC) can be implemented equally on wired and wireless networks. Port security is only applicable to wired networks.

41. Question

What is a reverse proxy commonly used for?

- ( ) **Directing traffic to internal services if the contents of the traffic comply with the policy**
- ( ) Allowing access to a virtual private cloud
- ( ) To prevent the unauthorized use of cloud services from the local network
- ( ) To obfuscate the origin of a user within a network

Unattempted

OBJ-8.1: A reverse proxy is positioned at the cloud network edge and directs traffic to cloud services if the contents of that traffic comply with the policy. This does not require the configuration of the users' devices. This approach is only possible if the cloud application has proxy support. You can deploy a reverse proxy and configure it to listen for client requests from a public network, like the internet. The proxy then creates the appropriate request to the internal server on the corporate network and passes the server's response back to the external client. They are not generally intended to obfuscate the source of communication, nor are they

necessarily specific to the cloud. A cloud access security broker (CASB) can be used to prevent unauthorized use of cloud services from the local network.

42. Question

During your reconnaissance, you have determined that your client's employees all use iPhones 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 an iPhone, it becomes much more difficult to attack since iPhone users can only install trusted apps from the App Store. If the user has jailbroken their phone, they can sideload apps and other malware. After identifying a jailbroken device, you can use social engineering to trick the user into installing your malicious code and then take control of their device.

43. Question

You are conducting a code review of a program and observe the following calculation of 0xffffffff + 1 was attempted, but the result was returned as 0x0000000. Based on this, what type of exploit could be created against this program?

- SQL injection
- **Integer overflow attack**
- Password spraying
- Impersonation

Unattempted

OBJ-5.2: Integer overflows and other integer manipulation vulnerabilities frequently result in buffer overflows. An integer overflow occurs when an arithmetic operation results in a large number to be stored in the space allocated for it. Integers are stored in 32 bits on the x86 architecture; therefore, if an integer

operation results in a number greater than 0xffffffff, an integer overflow occurs, as was the case in this example. SQL injection is an attack that injects a database query into the input data directed at a server by accessing the application's client-side. Password spraying is a type of brute force attack in which multiple user accounts are tested with a dictionary of common passwords. Impersonation is the act of pretending to be another person or system for fraud.

44. Question

You have been asked to create an allow statement on the firewall's ACL to allow NTP traffic to pass into the network. Which port should be included?

- **123**
- 69
- 636
- 143

Unattempted

OBJ-2.3: The correct port for NTP is 123. Port 69 is used for TFTP. Port 143 is used for IMAP. Port 636 is used for LDAPS.

45. Question

You are scanning a taregt as part of a penetration test. You discovered that the network uses Snort configured as a network-based IDS. Which of the following occurs when an alert rule has been matched in Snort during your scan?

- The IDS will send an alert, stop checking the rest of the rules, and allow the packet to continue its journey
- The source IP address will be blocked and its connection with the network terminated
- The packet matching the rule will be dropped and the IDS will continue scanning new packets
- **The entire packet will be evaluated until all of the IDS alert rules have been checked and the packet is allowed to continue its journey**

Unattempted

OBJ-2.3: If Snort is operating as an IDS, it will not block the connection or drop the packet. Instead, Snort will evaluate the entire packet and check all the alert rules, logging any matches it finds, and then allow it to

continue onward to its destination.

46. Question

Which of the following focuses on using digitized data as an internal means to reach a physical goal?

- OT systems
- IT systems
- Services
- Digital products

Unattempted

OBJ-7.2: Operational technology (OT) is the application of digital technology for detecting or causing changes in physical devices through monitoring and/or control. OT differs from IT in that it uses digitized data as an internal means to a physical goal, rather than to make information available to users. OT refers to physical devices (for instance, valves and pumps in machinery) that use digitized data to take physical action. OT devices can be as small as the engine control module (ECM) of a car or as large as the distributed control network of a national electricity grid. The collective term 'industrial control systems' (ICSs) refers to OT systems such as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), remote terminal units (RTUs), and programmable logic controllers (PLCs), along with dedicated networks and organization units. The Internet of Things (IoT) supports OT devices, allowing them to connect both to each other and to information systems.

47. Question

A malicious user is blocking mobile devices from connecting to the Internet when other people are in the coffee shop. What is the malicious user performing?

- Blacklisting IP addresses in the ACL
- Frequency jamming
- Spoofing
- Man-in-the-middle attack

Unattempted

OBJ-6.1: Frequency jamming is one of the many exploits used to compromise a wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming

frequencies of illegitimate traffic. There is no indication that the malicious user is creating a rogue AP (which is a form of spoofing) or performing a MITM attack by having users connect through their laptop or device. Also, there is no mention of certain websites or devices being blocked logically. Therefore there is no blacklisting of IP addresses performed.

48. Question

Which of the following hashing algorithms results in a 256-bit fixed output?

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

Unattempted

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

49. Question

You want to conduct OSINT against an organization in preparation for an upcoming engagement. Which of the following tools should you utilize?

- **Shodan**
- OpenVAS
- Aircrack-NG
- Social Engineer Toolkit (SET)

Unattempted

OBJ-2.1: Shodan (shodan.io) is a search engine that identifies Internet-connected devices of all types. The engine uses banner grabbing to identify the type of device, firmware/OS/app type, and version, plus vendor and ID information. This involves no direct interaction with the company's public-facing internet assets since this might give rise to detection. This is also the first place an adversary might use to conduct reconnaissance on your company's network. OpenVas, SET, and Aircrak-NG are not considered OSINT tools. OpenVas is a vulnerability scanner. SET is a social engineering tool. Aircrack-NG is a wireless hacking tool.

50. Question

How is sniffing broadly categorized?

- Unmanaged and managed
- **Active and passive**
- Broadcast and unicast
- Filtered and unfiltered

Unattempted

There are two types of sniffing: Passive Sniffing and Active Sniffing.

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 →

Quick Links

ABOUT US

FAQ

BROWSE ALL PRACTICE TESTS

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy