SKILLCERTPRO
IT CERTIFICATION TRAININGS

0

Information Security / By SkillCertPro

Practice Set 11

Your results are here!! for" CEHv11 Practice Test 11 "

0 of 49 questions answered correctly

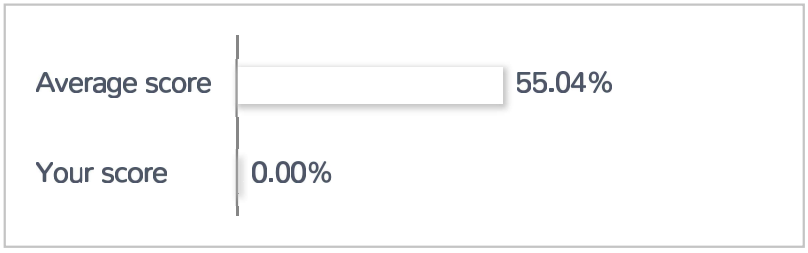
Your time: 00:00:03

Your Final Score is : 0

You have attempted : 0

Number of Correct Questions : 0 and scored 0

Number of Incorrect Questions : 0 and Negative marks 0



You can review your answers by clicking view questions.

Important Note : Open Reference Documentation Links in New Tab (Right Click and Open in New Tab).

Restart Test | View Answers

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34

35 36 37 38 39 40 41 42 43 44 45 46 47 48 49

Correct Incorrect

Review Question Summary

1. Question

Consider the following snippet from a log file collected on the host with the IP address of 10.10.3.6.

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

Time: Jun 12, 2020 09:24:12 Port:20 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP

Time: Jun 12, 2020 09:24:14 Port:21 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP

Time: Jun 12, 2020 09:24:16 Port:22 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP

Time: Jun 12, 2020 09:24:18 Port:23 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP

Time: Jun 12, 2020 09:24:20 Port:25 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP

Time: Jun 12, 2020 09:24:22 Port:80 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP

Time: Jun 12, 2020 09:24:24 Port:135 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP

Time: Jun 12, 2020 09:24:26 Port:443 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP

Time: Jun 12, 2020 09:24:26 Port:445 Source: 10.10.3.2 Destination:10.10.3.6 Protocol:TCP

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

What type of activity occurred based on the output above?

- Denial of service attack targeting 10.10.3.6
- Fragmentation attack targeting 10.10.3.6
- Port scan targeting 10.10.3.2
- **Port scan targeting 10.10.3.6**

Unattempted

OBJ-2.2: Port Scanning is the name for the technique used to identify open ports and services available on a network host. Based on the logs, you can see a sequential scan of some commonly used ports (20, 21, 22, 23, 25, 80, 135, 443, 445) with a two-second pause between each attempt. The scan source is 10.10.3.2, and the destination of the scan is 10.10.3.6, making "Port scan targeting 10.10.3.6" the correct choice. IP fragmentation attacks are a common form of denial of service attack, in which the perpetrator overbears a network by exploiting datagram fragmentation mechanisms. 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.

2. Question

You are assisting a member of your organization's security team during an incident response. The team member asks you to determine if any strange TCP connections are occurring on a given workstation. You open the command prompt on the workstation. Which of the following tools would provide you with information on any TCP connections currently on the workstation?

- tracert
- arp
- **netstat**
- route

Unattempted

OBJ-2.3: Netstat (network statistics) is a command-line network utility tool that displays network connections for the Transmission Control Protocol (incoming and outgoing), routing tables, and several network interface and network protocol statistics. It is useful when determining if a workstation is attempting outbound connections due to malware (beaconing activity) or has ports open and listening for inbound connections.

3. Question

You suspect that your server has been the victim of a web-based attack. Which of the following ports would most likely be seen in the logs to indicate the attack's target?

- 21
- 3389
- 389
- **443**

Unattempted

OBJ-2.2: Web-based attacks would likely appear on port 80 (HTTP) or port 443 (HTTPS). An attack against Active Directory is likely to be observed on port 389 LDAP. An attack on an FTP server is likely to be observed on port 21 (FTP). An attack using the remote desktop protocol would be observed on port 3389 (RDP).

4. Question

A network technician needs to monitor the network to find a user who is browsing websites against the company policy. What should the technician use to view the website and find the user browsing it?

- Top listener tool
- Intrusion detection system
- **Packet sniffer**
- SNMP GET

Unattempted

OBJ-4.1: Packet Sniffers can capture and analyze network user traffic. This information can be queried to view website addresses, contents, and sometimes even the password information. This differs from an intrusion detection system in that IDS' wait to receive implicitly-malicious data in a network before logging the event.

5. Question

A cybersecurity analyst working at a major university is reviewing the SQL server log of completed transactions and notices the following entry:

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

"select ID, GRADE from GRADES where ID=1235235; UPDATE GRADES set GRADE='A' where ID=1235235;"

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

Based on this transaction log, which of the following most likely occurred?

- The application and the SQL database are functioning properly
- The SQL server has insufficient logging and monitoring
- **Someone used an SQL injection to assign straight A's to the student with ID #1235235**
- A student with ID #1235235 used an SQL injection to give themselves straight A's

Unattempted

OBJ-5.3: Based on this transaction log entry, it appears that the ID# field was not properly validated before being passed to the SQL server. This would allow someone to conduct an SQL injection and retrieve the student's grades and set all of this student's grades to an 'A' at the same time. It is common to look for a '1==1' type condition to identify an SQL injection. There are other methods to conduct an SQL injection attack that could be utilized by an attacker. If input validation is not being performed on user-entered data, an attacker can exploit any SQL language aspect and inject SQL-specific commands. This entry is suspicious and

indicates that either the application or the SQL database is not functioning properly. Still, there appears to be adequate logging and monitoring based on what we can see and whether the question never indicates logging was an issue. An SQL database would not be designed to set ALL of a particular student's grades to A's, thus making this single entry suspicious. Most SQL statements in an SQL log will be fairly uniform and repetitive by nature when you review them. This leaves us with the question as to who person this SQL injection. Per the question choices, it could be the student with ID# 1235235 or "someone." While it seems as if student #1235235 had the most to gain from this, without further investigation, we cannot prove that it actually was student #1235235 that performed the SQL injection. Undoubtedly, student #125235 should be a person of interest in any ensuing investigations, but additional information (i.e., whose credentials were being used, etc.) should be used before making any accusations. Therefore, the answer is that "someone" performed this SQL injection.

6. Question

Which of the following cryptographic algorithms is classified as symmetric?

- RSA
- **AES**
- Diffie-Hellman
- ECC

Unattempted

OBJ-9.1: The Advanced Encryption Standard (AES) is a symmetric-key algorithm for encrypting digital data. It was established as an electronic data encryption standard by NIST in 2001. AES can use a 128-bit, 192-bit, or 256-bit key, and uses a 128-bit block size.

7. Question

What technique is most effective in determining whether or not increasing end-user security training would benefit the organization during your technical assessment of their network?

- Network sniffing
- Vulnerability scanning
- Application security testing
- **Social engineering**

Unattempted

OBJ-4.2: Social engineering refers to the psychological manipulation of people into performing actions or divulging confidential information. During your technical assessment, utilizing social engineering techniques such as phishing or pharming can help you determine if additional end-user security training should be included in the organization. The other three options focus solely on technical controls. Therefore adding end-user training would not affect these technology options.

8. Question

The Pass Certs Fast corporation has recently been embarrassed by several high profile data breaches. The CIO proposes improving the company's cybersecurity posture by migrating images of all the current servers and infrastructure into a cloud-based environment. What, if any, is the flaw in moving forward with this approach?

- This is a reasonable approach that will increase the security of the servers and infrastructure
- The company has already paid for the physical servers and will not fully realize their ROI on them due to the migration
- **This approach only changes the location of the network and not the attack surface of it**
- This approach assumes that the cloud will provide better security than is currently done on-site

Unattempted

OBJ-8.1: A poorly implemented security model at a physical location will still be a poorly implemented security model in a virtual location. Unless the fundamental causes of the security issues that caused the previous data breaches have been understood, mitigated, and remediated, then migrating the current images into the cloud will change where the processing occurs without improving the network's security. While the statement concerning unrealized ROI may be accurate, it simply demonstrates the sunk cost argument's fallacy. These servers were already purchased, and the money was spent. Regardless of whether we maintain the physical servers or migrate to the cloud, that money is gone. Those servers could also be repurposed, reused, or possibly resold to recoup some of the capital invested. While the company's physical security will potentially improve in some regards, the physical security of the endpoints on-premises is still a concern that cannot be solved by this cloud migration. Additionally, the scenario never stated that physical security was an issue that required being addressed, so it is more likely that the data breach occurred due to a data exfiltration over the network. As a cybersecurity analyst, you must consider the business case and the technical accuracy of a proposed approach or plan to add the most value to your organization.

9. Question

Which of the following would trigger the penetration test to stop and contact the system owners during an engagement?

- A production server is successfully exploited
- A production server is unresponsive to ping requests
- **Discovery of a production server with its log files deleted**
- Discovery of encrytped credit card data being stored in their database

Unattempted

OBJ-1.1: The penetration testing team should have a direct communication path with the system owners or their trusted agents during an engagement. Suppose the team discovers any security breaches, current hacking activity, extremely critical findings on a production server, or a production server becomes unresponsive during exploitation. In that case, the team should stop what they are doing and contract their trusted point of contact within the organization to get further guidance. Deleted log files should be considered an indicator of compromise and should be investigated by the company's security team before you continue with your engagement.

10. Question

A new alert has been distributed throughout the information security community regarding a critical Apache vulnerability. What action could you take to ONLY identify the known vulnerability?

- Perform a web vulnerability scan on all servers in the environment
- Perform an authenticated scan on all web servers in the environment
- **Perform a scan for the specific vulnerability on all web servers**
- Perform an unauthenticated vulnerability scan on all servers in the environment

Unattempted

OBJ-5.1: Since you wish to check for only the known vulnerability, you should scan for that specific vulnerability on all web servers. All web servers are chosen because Apache is a web server application. While performing an authenticated scan of all web servers or performing a web vulnerability scan of all servers would also find these vulnerabilities, it is a much larger scope. It would waste time and processing power by conducting these scans instead of properly scoping the scans based on your needs. Performing unauthenticated vulnerability scans on all servers is also too large in scope (all servers) while also being less effective (unauthenticated scan).

11. Question

You have just received an email that claims to be from the Federal Bureau of Investigation (FBI). The email claims that your computer was identified as part of a botnet being used to distribute pirated copies of a new movie. The email states that you must click the link below and pay a fine of $1000 within 24 hours, or federal agents will be sent to your home to arrest you for copyright infringement. What social engineering principle is this email relying on using?

- **Intimidation**
- Consensus
- Trust
- Familiarity

Unattempted

OBJ-4.2: Intimidation is a commonly used technique during a social engineering campaign. It relies on trying to scare or frighten a person into clicking a link. Often, these emails will claim to be from the FBI, IRS, or other government agencies.

12. Question

You are conducting a quick nmap scan of a target network. You want to conduct an SYN scan, but you don't have raw socket privileges on your workstation. Which of the following commands should you use to conduct the SYN scan from your workstation?

- nmap -sS
- nmap -sX
- **nmap -sT**
- nmap -O

Unattempted

OBJ-2.2: The nmap TCP connect scan (-sT) is used when the SYN scan (-sS) is not an option. You should use the -sT flag when you d not have raw packet privileges on your workstation or if you are scanning an IPv6 network. This flag tells nmap to establish a connection with the target machine by issuing the connect system call instead of directly using an SYN scan. Normally, a fast scan using the -sS (SYN scan) flag is more often conducted, but it requires raw socket access on the scanning workstation. The -sX flag would conduct a Xmas scan where the FIN, PSH, and URG flags are used in the scan. The -O flag would conduct an operating system detection scan of the target system.

13. Question

What tool can be used to scan a network to perform vulnerability checks and compliance auditing?

- **Nessus**
- Metasploit
- Nmap
- BeEF

Unattempted

OBJ-3.1: Nessus is a popular vulnerability scanner. It can be used to check how vulnerable your network is by using various plugins to test for vulnerabilities. Also, Nessus can perform compliance auditing, like internal and external PCI DSS audit scans. The nmap tool is a port scanner. The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

14. Question

A recently hired security employee at a bank was asked to perform daily scans of the bank's intranet to look for unauthorized devices. The new employee decides to create a script that scans the network for unauthorized devices every morning at 2:00 am. Which programming language would work best to create this script?

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

Unattempted

OBJ-5.1: Python is a commonly used scripting language used in cybersecurity. PHP is used as a scripting language for web applications. C# and ASP.NET are both compiled languages, not scripting languages.

15. Question

You are attending a cybersecurity conference and just watched a security researcher demonstrating the exploitation of a web interface on a SCADA/ICS component. This caused the device to malfunction and be

destroyed. You recognize that the same component is used throughout your company's manufacturing plants. Which of the following mitigation strategies would provide you with the most immediate protection against this emergent threat?

- Demand that the manufacturer of the component release a patch immediately and deploy the patch as soon as possible
- **Evaluate if the web interface must remain open for the system to function; if it isn't needed, block the web interface**
- Replace the affected SCADA/ICS components with more secure models from a different manufacturer
- Logically or physically isolate the SCADA/ICS component from the enterprise network

Unattempted

OBJ-7.2: The most immediate protection against this emergent threat would be to block the web interface from being accessible over the network. Before doing this, you must evaluate whether the interface needs to remain open for the system to function properly. If it is not needed, you should block it to minimize the SCADA/ICS component's attack surface. Ideally, your SCADA/ICS components should already be logically or physically isolated from the enterprise network. Since the question doesn't mention the networks as an area of concern, we can assume they are already following the industry best practice of logical or physical segmentation between the SCADA/ICS network and the enterprise network. On the exam, make sure you focus on the question being asked. In this case, the question focuses on the web interface. Developing a patch can be a time-consuming process, therefore waiting for the manufacturer to provide a patch will not provide immediate protection to your components. The same is true for replacing the affected components. Even if you could get the company to authorize the funding for such a purchase, it would take time to order, ship, receive, and install the new components. Additionally, you would cause unwanted downtime in the factory during the installation of the components, making it an ineffective option when simply blocking the web interface is free, quick, and effective.

16. Question

Edward's bank recently suffered an attack where an employee made an unauthorized modification to a customer's bank balance. Which tenant of cybersecurity was violated by this employee's actions?

- Confidentiality
- Authentication
- **Integrity**
- Availability

Unattempted

OBJ-1.1: The CIA Triad is a security model that helps people think about various parts of IT security. Integrity ensures that no unauthorized modifications are made to the information. The attack described here violates the integrity of the customer's bank account balance. Confidentiality is concerned with unauthorized people seeing the contents of the data. In this scenario, the employee is authorized to see the bank balance but not change its value. Availability is concerned with the data being accessible when and where it is needed. Again, this wasn't affected by the employee's actions. Authentication is concerned with only authorized people accessing the data. Again, this employee was authorized to see the balance.

17. Question

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

- Command injection allowed
- Directory listing enabled
- Reflected XSS
- Insecure HTTP methods allowed

Unattempted

OBJ-5.1: A command injection is unlikely since this is a static webpage and does not accept any user input. A command injection allows the user to supply malicious input to the web server and then passes that data to a system shell for execution. In this sense, command injection does create new instances of execution and can, therefore, leverage languages that the web app does not directly support.

18. Question

You are trying to select the best device to install to proactively stop outside attackers from reaching your internal network. Which of the following devices would be the BEST for you to select?

- IPS
- IDS
- Syslog server
- Proxy server

Unattempted

OBJ-4.5: An intrusion prevention system (IPS) is a form of network security that detects and prevents identified threats. Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents, and capturing information about them. An IPS can block malicious network traffic, unlike an IDS, which can only log them.

19. Question

Which of the following is usually not considered when evaluating the attack surface of an organization?

- Software applications
- External and internal users
- **Software development lifecycle model**
- Websites and cloud entities

Unattempted

OBJ-2.1: The software development lifecycle model used by a company is purely an internal function relevant only to the development of custom software within the organization. Regardless of whether a waterfall or agile methodology is chosen, it does not directly affect the organization's attack surface. The attack surface represents the set of things that could be attacked by an adversary. External and internal users, websites, cloud entities, and software applications used by an organization are all possible entry points that an adversary could attempt an attack upon.

20. Question

Which cloud computing concept is BEST described as focusing on the replacement of applications and programs on a customer's workstation with cloud-based resources?

- PaaS
- **SaaS**
- DBaaS
- IaaS

Unattempted

OBJ-8.1: Software as a Service (SaaS) is used to provide web applications to end-users. This can be a calendar, scheduling, invoicing, word processor, database, or other programs. For example, Google Docs and

Officer 365 are both word processing SaaS solutions.

21. Question

As a newly hired cybersecurity analyst, you are attempting to determine your organization's current public-facing attack surface. Which of the following methodologies or tools generates a current and historical view of the company's public-facing IP space?

- Google hacking
- nmap
- Review network diagrams
- **shodan.io**

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. The nmap scanning tool can provide an analysis of the current state of public exposure but has no mechanism to determine the history, nor will it give the same depth of information that shodan.io provides. Google Hacking can determine if a public exposure occurred over public-facing protocols, but it cannot conclusively reveal all the exposures present. Google hacking relies on using advanced Google searches with advanced syntax to search for information across the internet. Network diagrams can show how a network was initially configured. Unless the diagrams are up-to-date, which they usually aren't, they cannot show the current "as is" configuration. If you can only select one tool to find your attack surface's current and historical view, shodan is your best choice.

22. Question

A cybersecurity analyst notices that an attacker is trying to crack the WPS pin associated with a wireless printer. The device logs show that the attacker tried 00000000, 00000001, 00000002 and continued to increment by 1 number each time until they found the correct PIN of 13252342. Which of the following type of password cracking was being performed by the attacker?

- Rainbow table
- Hybrid
- **Brute-force**

Dictionary

Unattempted

OBJ-6.1: Brute-force attack when an attacker uses a set of predefined values to attack a target and analyze the response until he succeeds. Success depends on the set of predefined values. It will take more time if it is larger, but there is a better probability of success. In a traditional brute-force attack, the passcode or password is incrementally increased by one letter/number each time until the right passcode/password is found.

23. Question

Which type of method is used to collect information during the passive reconnaissance?

Social engineering

Network traffic sniffing

Publicly accessible sources

Man in the middle attacks

Unattempted

OBJ-2.1: Passive reconnaissance focuses on collecting information that is widely and openly available from publicly accessible sources. While network traffic sniffing is considered passive, gaining access to the network to place a sniffer in a good network tap location would not be considered passive. Of the choices provided, publicly accessible sources are the best answer to choose. Man-in-the-middle attacks would involve a penetration tester coming in between the traffic source and destination, which would allow its active inception and possible modification. Social engineering is also an active reconnaissance technique that uses deception to trick a user into providing information to an attacker or penetration tester.

24. Question

You were interpreting a Nessus vulnerability scan report and identified a vulnerability in the system with a CVSS attack vector rating of A. Based on this information, which of the following statements would be true?

Exploiting the vulnerability does not require any specialized conditions

The attacker must have access to the local network that the system is connected to

Exploiting the vulnerability requires the existence of specialized conditions

The attacker must have physical or logical access to the affected system

Unattempted

OBJ-3.1: The attack vector explains what type of access that the attacker must have to a system or network and does not refer to the types of specialized conditions that must exist. In this case, the A rating refers to Adjacent, where the attacker must launch the attack from the same shared physical (such as Bluetooth or Wi-Fi network), logical network (such as a local subnet), or a limited administrative domain (such as a VPN or MPLS). An attack vector of Network (N) would allow the attack to extend beyond these options and conduct remote exploitation of the vulnerability. An attack vector of Local (L) would require the attacker to locally exploit the workstation via the keyboard or over an SSH connection. An attack vector of Physical (P) would require the attacker to physically touch or manipulate the vulnerable component themselves, such as conducting a cold boot attack.

25. Question

A cybersecurity analyst is reviewing the logs of a Citrix NetScaler Gateway running on a FreeBSD 8.4 server and saw the following output:

-=-=-=-=—=-=-=-=-=—=-=-=-=-=—=-=-=-=-=—=-=-=-=-=—=-=-=-=-=—=-=-=-=-

10.1.1.1 — — [10/Jan/2020:13:23:51 +0000] "POST /vpn/../vpns/portal/scripts/newbm.pl HTTP/1.1" 200 143 "https://10.1.1.2/" "USERAGENT "

10.1.1.1 — — [10/Jan/2020:13:23:53 +0000] "GET /vpn/../vpns/portal/backdoor.xml HTTP/1.1" 200 941 "-" "USERAGENT"

10.1.1.1 — — [10/Jan/2020:16:12:31 +0000] "POST /vpns/portal/scripts/newbm.pl HTTP/1.1" 200 143 "https://10.1.1.2/" "USERAGENT"

-=-=-=-=—=-=-=-=-=—=-=-=-=-=—=-=-=-=-=—=-=-=-=-=—=-=-=-=-=—=-=-=-=-

What type of attack was most likely being attempted by the attacker?

- SQL injection
- XML injection
- Password spraying
- **Directory traversal**

Unattempted

OBJ-5.2: A directory traversal attack aims to access files and directories 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. The example output provided comes from a remote code execution vulnerability being exploited in which a directory traversal is used to access the files. XML Injection is an attack technique used to manipulate or compromise an XML

application or service's logic. SQL injection is the placement of malicious code in SQL statements via web page input. Password spraying attempts to crack various user's passwords by attempting a compromised password against multiple user accounts.

26. Question

Your company was recently the victim of a cross-site scripting attack. The system administrators claim this wasn't possible since they performed input validation using REGEX to alert on any strings that contain the term "[Ss]cript" in them. Which of the following statements concerning this attack is true?

- An SQL injection must have occurred since their input validation would have prevented <SCRIPT> or <script> from being used
- **The REGEX expression to filter using "[Ss]cript" is insufficient. As an attacker could use SCRIPT or SCRipt or %53CrIPT to evaded it**
- The attacker has modified the logs to cover their tracks and prevent a successful investigation
- The server has insufficient logging and monitoring configured

Unattempted

OBJ-4.5: The most likely explanation is that the REGEX filter was insufficient to eliminate every single possible cross-site scripting attack that could occur. Since cross-site scripting relies on the HTML tags to launch, the system administrators had a good idea of creating input validation using a REGEX for those keywords. Unfortunately, they forgot to include a more inclusive version of this REGEX to catch all variants. For example, simply using [Ss][Cc][Rr][Ii][Pp][Tt] would have been much more secure, but even this would miss %53CrIPT would evade this filter. To catch all the letter S variants, you would need to use [%53%%73Ss], which includes the capital S in hex code, the lower case s in hex code, the capital S, and the lowercase s. While it is possible that an attacker used an SQL injection instead, their REGEX input validation would still have allowed a cross-site scripting attack to occurs, so this option must be eliminated. As for the logging options, both are possible in the real world, but they do not adequately answer this scenario. The obvious flaw in their input validation is their REGEX filter.

27. Question

Which of the following tools provides a penetration tester with a framework to conduct technical social engineering attacks like phishing against an organization's employees?

- Proxychains
- **SET**

- Kismet
- Censys

Unattempted

OBJ-4.2: SET (Social Engineer Toolkit) is an open-source penetration testing framework included with Kali Linux that supports the use of social engineering to penetrate a network or system. Kismet is an 802.11 Layer 2 wireless network detector, sniffer, and intrusion detection system included with Kali Linux. Proxychains is a command-line tool that enables pen testers to mask their identity and/or source IP address by sending messages through intermediary or proxy servers. Censys is a search engine that returns information about the types of devices connected to the Internet.

28. Question

A security analyst wants to implement a layered defense posture for this network, so he uses multiple antivirus defensive layers, including both an end-user desktop antivirus software and an email gateway scanner. What kind of attack would this approach help to mitigate?

- Forensic attack
- ARP spoofing attack
- **Social engineering attack**
- Scanning attack

Unattempted

OBJ-4.2: By utilizing both endpoint protection (desktop antivirus software) and the email gateway scanner, the security analyst works to prevent phishing and other social engineering attacks. Emails are a common attack vector used in social engineering attacks.

29. Question

What tool is used to collect wireless packet data?

- **Aircrack-ng**
- Nessus
- Netcat
- John the Ripper

Unattempted

OBJ-6.1: Aircrack-ng is a complete suite of wireless security assessment and exploitation tools that includes monitoring, attacking, testing, and cracking of wireless networks. This includes packet capture and export of the data collected as a text file or pcap file. John the Ripper is a password cracking software tool. Nessus is a vulnerability scanner. Netcat is used to create a reverse shell from a victimized machine back to an attacker.

30. Question

Which mobile device strategy is most likely to introduce vulnerable devices to a corporate network?

- MDM
- **BYOD**
- COPE
- CYOD

Unattempted

OBJ-7.1: The BYOD (bring your own device) strategy opens a network to many vulnerabilities. People can bring their personal devices to the corporate network, and their devices may contain vulnerabilities that could be allowed to roam free on a corporate network. COPE (company-owned/personally enabled) means that the company provides the users with a smartphone primarily for work use, but basic functions such as voice calls, messaging, and personal applications are allowed, with some controls on usage and flexibility. With CYOD, the user can choose which device they wish to use from a small selection of devices approved by the company. The company then buys, procures, and secures the device for the user. The MDM is a mobile device management system that gives centralized control over COPE company-owned personally enabled devices.

31. Question

You are troubleshooting a user's workstation that is operating extremely slowly. You open the Task Manager and see that only Microsoft Word is currently running, but the CPU and network utilization is consistently running between 95-100%. Which of the following is MOST likely causing this issue?

- The application is not compatible with this OS
- The computer is the victim of a DoS attack
- **The computer has become a zombie**
- The network's firewall is blocking outbound traffic

Unattempted

OBJ-4.3: The workstation has most likely become a zombie. A zombie is any workstation running unauthorized software that directs the device to participate in a DDoS attack as part of a larger botnet. A botnet is a network of computers that have been compromised by a Trojan, rootkit, or worm malware. This workstation would then attempt to flood the victim's computer with requests over the network. These requests would require CPU and network resources to make, causing the utilization to rise to 95-100% resource utilization.

32. Question

What is the term for exploiting a weakness in a user's wireless headset to compromise their smartphone?

- Zero-day attack
- **Bluejacking**
- Multiplexing
- Smurfing

Unattempted

OBJ-6.1: Bluejacking sends unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs, or laptop computers.

33. Question

Yoyodyne Systems has recently bought out its competitor, Whamiedyne Systems, which went out of business due to a series of data breaches. As a cybersecurity analyst for Yoyodyne, you are assessing Whamiedyne's existing applications and infrastructure. During your analysis, you discover the following URL is used to access an application:

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

https://www.whamiedyne.com/app/accountInfo?acct=12345

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

You change the URL to end with 12346 and notice that a different user's account information is displayed. Which of the following type of vulnerabilities or threats have you discovered?

- **Insecure direct object reference**
- XML injection
- SQL injection

Race condition

Unattempted

OBJ-5.2: This is an example of an insecure direct object reference. Direct object references are typically insecure when they do not verify whether a user is authorized to access a specific object. Therefore, it is important to implement access control techniques in applications that work with private information or other sensitive data types. Based on the URL above, you cannot determine if the application is vulnerable to an XML or SQL injection attack. An attacker can modify one or more of these four basic functions in a SQL injection attack by adding code to some input within the web app, causing it to execute the attacker's own set of queries using SQL. An XML injection is similar but focuses on XML code instead of SQL queries. 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 developer's order and timing, which is not the case in this scenario.

34. Question

In 2014, Apple's implementation of SSL had a severe vulnerability that, when exploited, allowed an attacker to gain a privileged network position that would allow them to capture or modify data in an SSL/TLS session. This was caused by poor programming in which a failed check of the connection would exit the function too early. Based on this description, what is this an example of?

Use of insecure functions

Insecure object reference

Insufficient logging and monitoring

Improper error handling

Unattempted

OBJ-5.2: This is an example of an improper error handling vulnerability. A well-written application must be able to handle errors and exceptions gracefully. The main goal must be for the application not to fail and allows the attacker to execute code or perform an injection attack. One famous example of an improper error handling vulnerability is Apple's GoTo bug, as described above. For more details on this particular vulnerability, please see CVE-2014-1266. Insecure object reference refers to when a reference to an internal implementation object, such as a file or database key, is exposed to users without any other access control. Insufficient logging and monitoring allow attackers to achieve their goals without being detected due to the lack of monitoring and timely response by defenders. The use of insecure functions occurs in the C language when legacy functions like strcpy() are used. These insecure functions can lead to buffer overflow and other exploits being successful against a program.

35. Question

You are troubleshooting an issue with a Windows desktop and need to display the machine's active TCP connections. Which of the following commands should you use?

- ping
- **netstat**
- net use
- ipconfig

Unattempted

OBJ-2.3: The netstat command is used to display active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols) on a Windows machine. This is a useful command when determining if any malware has been installed on the system and maybe maintaining a remote connection with a command and control server.

36. Question

Which type of malware is used to actively attempt to steal confidential information by capturing a user's data when typed into a web browser or other application?

- Rootkit
- **Keylogger**
- Trojan
- Spyware

Unattempted

OBJ-3.3: A keylogger actively attempts to steal confidential information by capturing the data when entered into the computer by the user. This is done by recording keystrokes entered into a web browser or other application. A software keylogger can be run in the background on a victim's computer. A hardware keylogger may be placed between the USB port and the wired keyboard.

37. Question

What should be done NEXT if the final set of security controls does not eliminate all of the risks in a given system?

- You should remove the current controls since they are not completely effective
- **You should accept the risk if the residual risk is low enough**
- You should continue to apply additional controls until there is zero risk
- You should ignore any remaining risk

Unattempted

OBJ-1.1: In most cases, you will be unable to remove all risk. Instead, it would be best to mitigate the risk to a low enough level to accept the residual risk. Removing the controls would add to the risk, which is a bad course of action to select. Ignoring the remaining risk is unacceptable; instead, you should acknowledge what risk remains and accept it if it is low enough. If it is not low enough, you should continue to mitigate the risk by adding additional control measures. It is unlikely you will ever be able to get all risk down to zero, but mitigating to a lower level and then accepting the residual risk is a common industry practice.

38. Question

A company wants to ensure that its mobile devices are configured to protect any data stored on them if they are lost or stolen. Which of the following should you enable and enforce through their MDM?

- **Full storage encryption**
- Enable OS updates
- Enable SSO
- Remove backups

Unattempted

OBJ-7.1: Since the company is concerned with protecting data on the devices, you should enforce full storage encryption on the devices. Even if the device is lost or stolen, the device's data would be inaccessible to the person who stole or found the device. Additionally, the company may wish to enable the capability to conduct remote wipes of the device if they are lost or stolen to protect the data further.

39. Question

Which encryption type MOST likely is used for securing the key exchange during a client-to-server VPN connection?

- TKIP
- **ISAKMP**
- Kerberos
- AES

Unattempted

OBJ-9.1: ISAKMP is used in IPSec, which is commonly used in securing the key exchange during the establishment of a client-to-server VPN connection.

40. Question

A penetration tester wants to build a workstation that will be used to brute force hash digests. Which of the following is the BEST option to ensure sufficient power and speed to crack them?

- 7200-RPM HDD
- Multi-core CPU
- **Dedicated GPU**
- Integrated GPU

Unattempted

OBJ-9.1: Dedicated GPUs are designed to conduct complex mathematical functions extremely quickly. If you want to build a system to perform cracking of a password, hash, or encryption algorithm, it is important to have a high-speed, dedicated GPU. The reason to use a GPU instead of a CPU for password cracking is that it is much faster for this mathematically intensive type of work. Cracking passwords, hashes, and encryption is a lot like mining cryptocurrency in that using dedicated GPUs will give you the best performance.

41. Question

Your company has decided to begin moving some of its data into the cloud. Currently, your company's network consists of both on-premise storage and some cloud-based storage. Which of the following types of clouds is your company currently using?

- Public
- **Hybrid**
- Community

Private

Unattempted

OBJ-8.1: A hybrid cloud is a cloud computing environment that uses a mix of on-premises, private cloud, and third-party public cloud services with orchestration between these platforms.

42. Question

An attacker is using a precomputed table of values to attempt to crack your Windows password. What type of password attack is this?

Hybrid

Brute-force

Rainbow table

Dictionary

Unattempted

OBJ-3.2: A rainbow table is a tool for speeding up attacks against Windows passwords by precomputing possible hashes. A rainbow table is used to authenticate users by comparing the hash value of the entered password against the one stored in the rainbow table. Using a rainbow table makes password cracking a lot faster and easier for an attacker.

43. Question

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

SHA-2

NTLM

MD-5

RIPEMD

Unattempted

OBJ-9.1: RIPEMD 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.

44. Question

Which of the following hashing algorithms results in a 128-bit fixed output?

- SHA-2
- RIPEMD
- **MD-5**
- SHA-1

Unattempted

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

45. Question

Your company is adopting a new BYOD policy for tablets and smartphones. Which of the following would allow the company to secure the sensitive information on personally owned devices and the ability to remote wipe corporate information without the user's affecting personal data?

- Touch ID
- Face ID
- Long and complex passwords
- **Containerization**

Unattempted

OBJ-7.1: Containerization is the logical isolation of enterprise data from personal data while co-existing in the same device. The major benefit of containerization is that administrators can only control work profiles that are kept separate from the user's personal accounts, apps, and data. This technology basically creates a secure vault for your corporate information. Highly targeted remote wiping is supported with most container-based solutions.

46. Question

As a newly hired cybersecurity analyst, you are attempting to determine your organization's current public-facing attack surface. Which of the following methodologies or tools generates a current and historical view of the company's public-facing IP space?

- Review network diagrams
- nmap
- Google hacking
- **shodan.io**

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. The nmap scanning tool can provide an analysis of the current state of public exposure but has no mechanism to determine the history, nor will it give the same depth of information that shodan.io provides. Google Hacking can determine if a public exposure occurred over public-facing protocols, but it cannot conclusively reveal all the exposures present. Google hacking relies on using advanced Google searches with advanced syntax to search for information across the internet. Network diagrams can show how a network was initially configured. Unless the diagrams are up-to-date, which they usually aren't, they cannot show the current "as is" configuration. If you can only select one tool to find your attack surface's current and historical view, shodan is your best choice.

47. Question

Which of the following tools is used by a penetration tester to conduct open-source intelligence (OSINT)?

- Nessus
- AirCrack-NG
- **Maltego**
- Empire

Unattempted

OBJ-2.1: Maltego is an OSINT tool that is used to gather information from public resources. It has a graphical user interface (GUI) that visualizes the information gathered to help a penetration tester make logical connections between the different data sets collected.

48. Question

A cybersecurity analyst at Yoyodyne Systems just finished reading a news article about their competitor, Whamiedyne Systems, being hacked by an unknown threat actor. Both companies sell to the same basic group of consumers over the internet since their products are used interchangeably by consumers. Which of the following is a valid cybersecurity concern for Yoyodyne Systems?

- The attacker will conduct a man-in-the-middle attack
- The same vulnerability will be compromised on their servers
- The attacker will conduct a SQL injection against their database
- **They may now be vulnerable to a credential stuffing attack**

Unattempted

OBJ-5.1: The largest and most immediate cybersecurity concern that the analyst should have is credential stuffing. Credential stuffing occurs when an attacker tests username and password combinations against multiple online sites. Since both companies share a common consumption group, it is likely that some of Yoyodyne's consumers also had a user account at Whamiedyne. If the attackers compromised the username and passwords from Whamiedyne's servers, they might attempt to use those credentials on Yoyodyne's servers, too. There is no definitive reason to believe that both companies are using the same infrastructure. Therefore, the same vulnerability that was exploited by the attacker may not exist at Yoyodyne. The question doesn't mention an SQL database. Therefore, there is no direct threat of an SQL injection. A man-in-the-middle (MitM) attack occurs when the attacker sits between two communicating hosts and transparently captures, monitors, and relays all communications between the host. Nothing in this question indicates that a MitM was utilized or is a possible threat.

49. Question

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

- **Wait for a malicious email attachment to be opened**
- **Take advantage of a software, hardware, or human vulnerability**
- Select backdoor implant and appropriate command and control infrastructure for operation
- A backdoor/implant is placed on a victim's client
- **Wait for a user to click on a malicious link**
- A webshell is installed on a web server

Unattempted

OBJ-1.1: During this phase, activities taken during the exploitation phase are conducted against the target's system. Taking advantage of or exploiting an accessible vulnerability, waiting for a malicious email attached to be opened, or waiting for a user to click on a malicious link is all part of the exploitation phase. The installation of a web shell, backdoor, or implant is all performed during the installation phase. Selecting a backdoor implant and appropriate command and control infrastructure occurs during the weaponization phase.

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 →

CONTACT FORM

Important Links

REFUND POLICY

REFUND REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

Privacy Policy