UDEMY Pen Test+ Practice Exam 4 Incorrect Answers

Study online at https://quizlet.com/_fjwtsn

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? nmap shodan.io Google hacking Review network diagrams	shodan.io Explanation 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.
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	They may now be vulnerable to a credential stuffing attack Explanation OBJ-2.4: 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.
An organization has hired a cybersecurity analyst to conduct an assessment of their current security posture. The analyst begins by conducting an external assessment against the organization's network to determine what information is exposed to a potential external attacker. What technique should the analyst perform first? DNS query log reviews Intranet portal reviews Enumeration Technical control audits	Enumeration Explanation OBJ-2.1: Scanning and enumeration are used to determine open ports and identify the software and firmware/device types running on the host. This is also referred to as footprinting or fingerprinting. This technique is used to create a security profile of an organization by using a methodological manner to conduct the scanning. If this scan is conducted from outside of the organization's network, it can be used to determine the network devices and information available to an unauthorized and external attacker. A DNS query log review, intranet portal review, or technical control audit would require internal access to the network, which is typically not accessible directly to an external attacker.
After issuing the command "telnet diontraining.com 80" and connecting to the server, what command conducts the banner grab? HEAD / HTTP/1.1	HEAD / HTTP/1.1 Explanation

PUT / HTTP/1.1 HEAD / HTTP/2.0 PUT / HTTP/2.0	OBJ-2.1: To conduct a banner grab using telnet, you first must connect to the server using "telnet webserver 80". Once the connection establishes, you will receive a blank prompt, and you then issue the command "HEAD / HTTP/1.1". It requests the document header from the server and provides information such as the server software version and the server's operating system.
You are a cybersecurity analyst, and your company has just enabled key-based authentication on its SSH server. Review the following log file: -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- BEGIN LOG ---------- Sep 09 13:15:24 diontraining sshd[3423]: Failed password for root from 192.168.3.2 port 45273 ssh2 Sep 09 15:43:15 diontraining sshd[3542]: Failed password for root from 192.168.2.24 port 43543 ssh2 Sep 09 15:43:24 diontraining sshd[3544]: Failed password for jdion from 192.168.2.24 port 43589 ssh2 Sep 09 15:43:31 diontraining sshd[3546]: Failed password for tmartinez from 192.168.2.24 port 43619 ssh2 Sep 09 15:43:31 diontraining sshd[3546]: Failed password for jdion from 192.168.2.24 port 43631 ssh2 Sep 09 15:43:37 diontraining sshd[3548]: Failed password for root from 192.168.2.24 port 43657 ssh2 ---------- END LOG =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-= Which of the following actions should be performed	Disable password authentication for SSH Explanation OBJ-3.4: It is common for attackers to log in remotely using the ssh service and the root or other user accounts. The best way to protect your server is to disable password authentication over ssh. Since your company just enabled key-based authentication on the SSH server, all legitimate users should be logging in using their RSA key pair on their client machines, not usernames and passwords. Based on the logs, you see the server runs SSHv2, so there is no need to disable SSHv1 (it may already be disabled). You don't want to fully disable remote root SSH logins, either, since this would make it difficult for administrators to conduct their work. Finally, based on the logs, it doesn't appear that anonymous SSH logins are an issue, either, as we don't see any anonymous attempts in the logs.
A user receives certificate errors in other languages within their web browser when accessing your company's website. Which of the following is the MOST likely cause of this issue? DoS Reflective DNS Man-in-the-middle ARP poisoning	Man-in-the-middle Explanation OBJ-3.2: A man-in-the-middle attack is a general term when a perpetrator positions himself in a conversation between a user and an application, either to eavesdrop or impersonate one of the parties, making it appear as if a normal exchange of information is occurring. For example, if your user and server are both in the United States (English language), the attacker performing the MITM is from Russia. The user may see a certificate error in Russian instead of English.
Jason is conducting a penetration test against Dion Training's Windows-based network. He wants to laterally move to another host and execute an exploit he previously trick a user into downloading to the C:\Windows\temp directory on the workstation with an IP of 192.168.1.50. He types the following into his terminal: -=-=-=-=-=-=- PS C:\Users\jason> $obj = [activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.Application","192. 168.1.50")) PS C:\Users\jason> $obj.Document.ActiveView.ExecuteShellCommand("C:\Windows\temp\exploit.exe", $null,$null,"7") -=-=-=-=-=-=- Based on these commands, what type of post-exploitation lateral movement did Jason utilize? PsExec RPC/DCOM WMIC Scheduled tasks	RPC/DCOM Explanation OBJ-3.7: Remote Procedure Call (RPC) enables inter-process communication between local and remote processes on Windows. Distributed Component Object Model (DCOM) enables the communication between software components over a network. DCOM applications use RPC as a transport mechanism for client requests. Flaws in DCOM can enable you to execute code on a remote system by assuming user privileges. For example, a DCOM application commonly used to initiate lateral movement is MMC20.Application. This enables users to execute Microsoft Management Console (MMC) snap-in operations on a Windows computer. The MMC20.application includes an ExecuteShellCommand() method that allows for a command's remote execution using a remote computer's shell. In this example, the first command told PowerShell on Jason's machine to select the MMMC snap-in on the remote computer with the IP address of 192.168.1.50. The second command then started the exploit on the remote system with a null current working directory, null parameters passed to the exploit.exe command and started it with a window state of 7. Ultimately, this would launch the exploit.exe

	program on the remote machine using the local administrator account.
An organization is conducting a cybersecurity training exercise. What team is Jason assigned to if he has been asked to monitor and manage the defenders' and attackers' technical environment during the exercise? Red team White team Blue team Purple team	White team Explanation OBJ-1.3: Jason is assigned to the white team. The white team acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission. A red team is a group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. A blue team is a group of people responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers. The purple team is made up of both the blue and red teams to work together to maximize their cyber capabilities through continuous feedback and knowledge transfer between attackers and defenders.
What type of scan will measure the size or distance of a person's external features with a digital video camera? Iris scan Retinal scan Facial recognition scan Signature kinetics scan	Facial recognition scan Explanation OBJ-2.5: A face recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. One way to do this is by comparing selected facial features from the image and a face database. By measuring the external facial features, such as the distance between your eyes and nose, you can uniquely identify the user. A retinal scan is a biometric technique that uses unique patterns on a person's retina blood vessels. Iris recognition or iris scanning is the process of using visible and near-infrared light to take a high-contrast photograph of a person's iris. A signature kinetics scan measures a user's action when signing their name and compares it against a known-good example or baseline.
Jason is conducting a physical penetration test against a company. His objective is to enter the server room that is protected by a lock using a fingerprint reader. Jason attempts to use his finger to open the lock several times without success. He then turns his finger 45 degrees to the left, and the lock authenticates him. What is MOST likely the reason the lock opened? The crossover error rate is tuned towards true negatives The biometric lock is set to fail open after five invalid attempts The biometric lock is set to fail closed after five invalid attempts The crossover error rate is tuned towards false positives	The crossover error rate is tuned towards false positives Explanation OBJ-2.4: A biometric lock is difficult to bypass unless the installer incorrectly configures it. If the biometric lock has a high false acceptance rate, it will allow unauthorized people to open the door. The crossover error rate (CER) is the point where the false acceptance and false rejection rates are equal. When charted on a graph, this point can lean more towards accepting false positives or rejecting true positives. If it leans more towards accepting false positives, the sensitivity has decreased to allow less frustration for its users.
Which technique would provide the largest increase in security on a network with ICS, SCADA, or IoT devices? Installation of anti-virus tools Use of a host-based IDS or IPS Implement endpoint protection platforms	User and entity behavior analytics Explanation OBJ-2.5: Since ICS, SCADA, and IoT devices often run proprietary, inaccessible, or unpatchable operating systems, the traditional tools used to detect the presence of malicious cyber activity in normal enterprise networks will not function properly. Therefore, user and entity behavior analytics (UEBA) is best suited to detect and classify known-good behavior from these systems to create a baseline. Once a known-good baseline is established, deviations can be detected and analyzed. UEBA may be heavily dependent on advanced computing techniques like artificial intelligence and machine learning and may have a higher false-positive rate. As

User and entity behavior analytics	the name suggests, the analytics software tracks user account behavior across different devices and cloud services. Entity refers to machine accounts, such as client workstations or virtualized server instances, and embedded hardware, such as the Internet of Things (IoT) devices. Traditional technologies include anti-virus tools, host-based IDS and IPS, and endpoint protection platforms.
An independent cybersecurity researcher has contacted your company to prove a buffer overflow vulnerability exists in one of your applications. Which technique would have been most likely to identify this vulnerability in your application during development? Dynamic code analysis Pair programming Manual Peer Review Static code analysis	Static code analysis Explanation OBJ-2.2: Buffer overflows are most easily detected by conducting a static code analysis. Manual peer review or pair programming methodologies might have been able to detect the vulnerability. Still, they do not have the same level of success as a static code analysis using proper tools. DevSecOps methodology would also improve the likelihood of detecting such an error but still rely on human-to-human interactions and human understanding of source code to detect the fault. Dynamic code analysis also may have detected this if the test found exactly the right condition. Still, again, a static code analysis tool is designed to find buffer overflows more effectively.
Question 43: IncorrectWhich type of monitoring would utilize a network tap? Router-based Active Passive SNMP	Passive Explanation OBJ-3.2: Network taps are devices that allow a copy of network traffic to be captured for analysis. They conduct passive network monitoring and visibility without interfering with the network traffic itself. Active monitoring relies on scanning targeted systems, not a network tap. Router-based monitoring would involve looking over the router's logs and configuration files. SNMP is used to monitor network devices but is considered active monitoring and doesn't rely on network taps.
Question 54: IncorrectYou are reviewing the logs in your IDS and see that entries were showing SYN packets received from a remote host targeting each port on your web server from 1 to 1024. Which of the following MOST likely occurred? Remote host cannot find the right service port SYN flood Port scan UDP probe	Port scan Explanation OBJ-3.2: Based on the description provided, this is most likely a port scan. Using a tool like nmap, an attacker can create an SYN scan across every port in a range against the desired target. A port scan or SYN scan may trigger an alert in your IDS. While scanners support more stealthy scans, default scans may connect to each port sequentially. The other options are incorrect because a remote host will typically connect to only a single port associated with a service. An SYN flood normally sends many SYNs to a single system. Still, it doesn't send them to unused ports, and a UDP probe will not send SYN packets.
You are analyzing a Python script that isn't functioning properly. You suspect the issue is with the string manipulation being used in the code. Review the following Python code snippet: -=-=-=-=-=- #!/usr/bin/pythons = "DionTraining.com"print(s[4::-1]) -=-=-=-=-=- Based on your analysis, what should be displayed on the screen by the print command? DionT oc.g TnoiD moc.	TnoiD Explanation OBJ-4.4: When evaluating the code s[4::-1], you would receive "TnoiD" in response. Within Python, characters in a string can be accessed by their index location. If the string (s) is "DionTraining.com", then each letter from left to right is referenced as s[0] to s[15]. For example, if you enter s[5], you would receive the letter "r" in response. The format for the array is [start:end:increment], so s[4::-1] is evaluated as starting with the 4th position (T in DionTraining.com since computers start counting at 0), count until it reaches the beginning or end of the word, and then increment by one position each time to the left (since it was -1). This would display the 4th position (T), 3rd position (n), 2nd position (o), 1st position (i), the zero position (D), and then stop

UDEMY Pen Test+ Practice Exam 4 Incorrect Answers

Study online at https://quizlet.com/_fjwtsn

Which of the following tools is used to cross-compile code on a Kali Linux machine to run on a Windows client? Metasploit Ollydbg MSFvenom APK studio	MSFvenom Explanation OBJ-4.2: MSFvenom is a combination of Msfpayload and Msfencode, putting both of these tools into a single Framework instance. This tool allows a Kali Linux user to cross-compile code as an executable for a Windows client or Android device. MSFvenom is part of the Metasploit framework.
You are working as part of a penetration testing team conducting engagement against Dion Training's network. You have been given a list of targets in a text file called servers.txt. Which of the following Nmap commands should you use to find all the servers from the list with ports 80 and 443 enabled and save the results in a greppable file called results.txt? nmap -p80,443 -sL servers.txt -oX results.txt nmap -p80,443 -iL servers.txt -oX results.txt nmap -p80,443 -iL servers.txt -oG results.txt nmap -p80,443 -sL servers.txt -oG results.txt	nmap -p80,443 -iL servers.txt -oG results.txt Explanation OBJ-4.1: The command (nmap -p80,443 -iL servers.txt -oG results.txt) will only perform an nmap scan against ports 80 and 443. The -iL option will scan each of the listed server's IP addresses. The -oG option will save the results in a greppable format to the file results.txt while still displaying the normal results to the shell. The option of -sL will only list the servers to scan. It will not actually scan them. The option of -oX is for outputting the results to a file in an XML format.
Consider the following REGEX search string: -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- \b(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\. (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- Which of the following strings would NOT be included in the output of this search? 1.2.3.4 001.02.3.40 37.259.129.207 205.255.255.001	37.259.129.207 Explanation OBJ-4.4: The \b delimiter indicates that we are looking for whole words for the complete string. The REGEX is made up of four identical repeating strings, (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.". For now, let us refer to these octets, such as the ones used in internet protocol version 4 addresses. Each octet will allow the combination of 25[0-5] OR (|) 2[0-4][9-] OR numbers 00-99 is preceded by (?) a 0 or 1, or just a single number followed by a ".". Since the period is treated as a special character in a REGEX operator, the escape character (\) is required to enable the symbol to act as a dot or period in the output. This sequence repeats four times, allowing for all variations of normal IP addresses to be entered for values 0-255. Since 259 is outside the range of 255, this is rejected. More specifically, character strings starting with 25 must end with a number between 0 and 5 (25[0-5]). Therefore, 259 would be rejected. Now, on exam day, if you received a question like this, you can try to figure out the pattern as explained above, or you can take the logical shortcut. The logical shortcut is to look at the answer first and see that they all look like IP addresses. Remember, grep and REGEX are used by a cybersecurity analyst to search logs for indicators of compromise (like an IP address), so don't be afraid to take a logical guess if you need to conserve time during your exam. So, which one isn't a valid IP address? Clearly, 37.259.129.107 is not a valid IP address, so if you had to guess as to what wouldn't be an output of this complex-looking command, you should guess that one!
Which of the following vulnerabilities can be prevented by using proper input validation? (Select ANY that apply) Cross-site scripting	Cross-site scripting SQL injection Directory traversal XML injection Explanation OBJ-5.3: Proper input validation can prevent cross-site scripting,

SQL injection Directory traversal XML injection	SQL injection, directory traversal, and XML injections from occurring. When an application accepts string input, the input should be subjected to normalization or sanitization procedures before being accepted. Normalization means that a string is stripped of illegal characters or substrings and converted to the accepted character set. This can prevent SQL and XML injections from occurring. Input validation is also good at preventing cross-site scripting (XSS) in forms that accept user input. Directory traversals can be prevented by conducting input validation in file paths or URLs accepted from a user. This prevents a canonicalization attack from disguising the nature of the malicious input that could cause a directory traversal.

Your team is developing an update to a piece of code that allows customers to update their billing and shipping addresses in the web application. The shipping address field used in the database was designed with a limit of 75 characters. Your team's web programmer has brought you some algorithms that may help prevent an attacker from trying to conduct a buffer overflow attack by submitting invalid input to the shipping address field. Which pseudo-code represents the best solution to prevent this issue?
 	
if (shippingAddress = 75) {update field} else exit
 	
if (shippingAddress != 75) {update field} else exit
 	
if (shippingAddress >= 75) {update field} else exit (Incorrect)
 	
if (shippingAddress <= 75) {update field} else exit
	if (shippingAddress <= 75) {update field} else exit
	
	Explanation
	OBJ-5.3: To ensure that the field is not overrun by an input that is too long, input validation must occur. Checking if the shipping address is less than or equal to 75 characters before updating the field will prevent a buffer overflow from occurring in this program. If the input is 76 characters or more, then the field will not be updated, and the algorithm will exit the function.

Your company failed a recent security audit. The IT Directory has issued a new policy dictating that all workstations must be locked when not in use for more than 2 minutes. A password must be entered before booting up the operating system, and that the hard drive is fully encrypted. You have been asked to configure the corporate workstations to enforce these new security measures. Which THREE of the following should you configure FIRST? Enable strong passwords Enable BitLocker Require multifactor authentication Enable a UEFI password Require the use of smart cards Enable a screen lock	Enable BitLocker Enable a UEFI password Enable a screen lock Explanation OBJ-5.3: These requirements can be met by enabling BitLocker to encrypt the hard drive, enable a UEFI password to require a password to be entered before booting an operating system, and enabling a screen lock that turns on after 2 minutes of inactivity.
A company has implemented the capability to send all log files to a central location by utilizing an encrypted channel. The log files are sent to this location to be reviewed. A recent exploit has caused the company's encryption to become insecure. What would be required to resolve the exploit? Utilize an FTP service Install recommended updates Send all log files through SMTP Configure the firewall to block port 22	Install recommended updates Explanation OBJ-5.3: If the encryption is insecure, then we must look for encryption software updates or patches. If they are available, we must install them.

Jay is replacing his organization's current vulnerability scanner with a new tool. As he begins to create the scanner's configurations and scanning policy, he notices a conflict in the settings recommended between different documents. Which of the following sources must Jay follow when trying to resolve these conflicts? NIST guideline documents Vendor best practices Corporate policy Configuration settings from the prior system	Corporate policy Explanation OBJ-1.2: Policies are formalized statements that apply to a specific area or task. Policies are mandatory, and employees who violate a policy may be disciplined. Guidelines are general, non-mandatory recommendations. Best practices are considered procedures that are accepted as being correct or most effective but are not mandatory to be followed. Configuration settings from the prior system could be helpful, but this is not a mandatory compliance area like a policy. Therefore, Jay should first follow the policy before the other three options if there is a conflict.
Following an engagement, the penetration testing team has generated many recommendations for additional controls and items to be purchased to prevent future recurrences. Which of the following approaches BEST describes what the organization should do next? Immediately procure and install all of them because the adversary may attack at any time Contract an outside security consultant to provide an independent assessment of the network and outsource the remediation efforts Create a prioritized list with all of the recommendations for review, procurement, and installation Conduct a cost/benefit analysis of each recommendation against the company's current fiscal posture	Create a prioritized list with all of the recommendations for review, procurement, and installation Explanation OBJ-5.3: Since an engagement has just finished, it is important to act swiftly since its results are a point-in-time assessment. The organization should still take a defined and deliberate approach to choosing the proper controls and risk mitigations. Therefore, execution through a rational business management process is the best approach, including creating a prioritized list of recommendations. Once this list has been created, the organization can conduct a cost/benefit analysis of each recommendation and determine which controls and items will be implemented in the network-based upon resource availability in terms of time, person-hours, and money. This process does not need to be a long term study or filled with complexity. Instead, it should be rapidly conducted due to the probability that an attacker may compromise the network using the same vulnerabilities the penetration testing team found in their engagement.