CompTIA Pentest+ (Ethical Hacking) Course & Practice Exam

Study online at https://quizlet.com/_ffy7ik

Jack is assessing the likelihood of reconnaissance activities being performed against his organization. Which of the following would best classify the likelihood of a port scan being conducted against his DMZ?	High
Which of the following types of information is protected by rules in the United States that specify the minimum frequency of vulnerability scanning required for devices that process it?	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. As part of PCI DSS compliance, organizations must conduct internal and external scans at prescribed intervals on any devices or systems that process credit card data.
Which of the following penetration testing methodologies is focused on testing web applications and the people, processes, and technology that support them?	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.
Which of the following is the MOST important thing to receive from the client during the planning for an engagement?	Tolerance to impact
Which of the following would trigger the penetration tester to stop and contact the system owners during an engagement?	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.
You have just concluded a two-month engagement that targeted Dion Training's network. You have a detailed list of findings and have prepared your report for the company. Which of the following reasons explains why you must keep your report confidential and secure?	The findings could be used by attackers to exploit the client's systems
You are a penetration tester hired by an organization that wants you to conduct a risk assessment of their perimeter network. The company-provided Rules of Engagement states that you must do all penetration testing from an external IP address without any prior knowledge of the internal IT system architecture. What kind of penetration test will you perform?	An unknown environment penetration test requires no previous information and usually takes the approach of an uninformed attacker. The penetration tester has no prior information about the target system or network in an unknown environment penetration test. These tests provide a realistic scenario for testing the defenses, but they can be costlier and more time-consuming to conduct as the tester is examining a system from an outsider's perspective.
You have been hired by a corporate client to perform a web application penetration test. After you presented your findings to the client, they have asked you to perform a static code review, update the web server application, and configure a new web application firewall to protect the system. The client organization does not have the additional budget or a written modification to your previously signed contract to support these requests. Which of the following are you experiencing?	Scope creep
What technique is an attacker using if they review data and publicly available information to gather intelligence about the target organization without scanning or other technical information-gathering activities?	Passive reconnaissance
A cybersecurity analyst is attempting to perform an active reconnaissance technique to audit their company's security controls. Which DNS assessment technique would be classified as active?	A zone transfer - DNS zone transfer, also sometimes known by the inducing DNS query type AXFR, is a DNS transaction type. It is one of the many mechanisms available for administrators to replicate DNS databases across a set of DNS servers. DNS zone transfers are an active technique.

You have conducted a Google search for the "site:diontraining.com -site:sales.diontraining.com financial." What results do you expect to receive?	When conducting a Google search, using site:AAA in the query will return results only from that website (AAA). If you use -site:AAA, you will get results not explicitly on the website (AAA). In the case of this question, no results should show up from sales.diontraining.com. All results should only come from diontraining.com. Google results matching "financial" in domain diontraining.com, but no results from the site sales.diontraining.com
As a newly hired cybersecurity analyst, you are attempting to determine your organization's current public-facing attack surface. Which of the following methodologies or tools generates a current and historical view of the company's public-facing IP space?	Shodan
An organization has hired a cybersecurity analyst to conduct an assessment of its current security posture. The analyst begins by conducting an external assessment against the organization's network to determine what information is exposed to a potential external attacker. What technique should the analyst perform first?	Enumeration
What techniques are commonly used by port and vulnerability scanners to enumerate the services running on a target system?	Banner grabbing and comparing response fingerprints
A penetration tester wants to collect software versioning information from servers on the network. The penetration tester has set up a packet sniffer on a victimized host and sent a copy of the network traffic back to their workstation. The penetration tester's objective in this assessment is to emulate an APT and remain stealthy for as long as possible while gathering information. Which of the following should the penetration tester do enumerate the software version used by the server?	Manually analyze the packet captures
You are currently conducting active reconnaissance in preparation for an upcoming penetration test against Dion Training. You want to identify the areas of the company's website that are not crawled by search engines. Which of the following should you review to determine these areas?	A robots.txt file tells search engine crawlers which URLs the crawler should index and access on your site. When conducting active reconnaissance, you may wish to manually evaluate the robots.txt file and then access those portions of the website.
As a cybersecurity analyst conducting vulnerability scans, you have just completed your first scan of an enterprise network comprising over 10,000 workstations. As you examine your findings, you note that you have less than 1 critical finding per 100 workstations. Which of the following statement does BEST explain these results?	Uncredentialed scans are generally unable to detect many vulnerabilities on a device. When conducting an internal assessment, you should perform an authenticated (credentialed) scan of the environment to most accurately determine the network's vulnerability posture. In most enterprise networks, if a vulnerability exists on one machine, it also exists on most other workstations since they use a common baseline or image. If the scanner failed to connect to the workstations, an error would have been generated in the report.
Which of the following vulnerability scanning tools would be used to conduct a web application vulnerability assessment?	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.
Which of the following tools can NOT be used to conduct a banner grab from a web server on a remote host?	FTP cannot be used to conduct a banner grab. A cybersecurity analyst or penetration tester uses a banner grab to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network. This is commonly done using telnet, wget, or netcat.

An organization has hired a cybersecurity analyst to conduct an assessment of its current security posture. The analyst begins by conducting an external assessment against the organization's network to determine what information is exposed to a potential external attacker. What technique should the analyst perform first?1	Scanning and enumeration are used to determine open ports and identify the software and firmware/device types running on the host. This is also referred to as footprinting or fingerprinting. This technique is used to create a security profile of an organization by using a methodological manner to conduct the scanning. If this scan is conducted from outside of the organization's network, it can be used to determine the network devices and information available to an unauthorized and external attacker.
A security analyst conducts a Nmap scan of a server and found that port 25 is open. What risk might this server be exposed to?	Open mail relay
Which attack method is MOST likely to be used by a malicious employee or insider trying to obtain another user's passwords?	Shoulder surfing
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 best describes this type of attack?	Phishing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Phishing attacks target an indiscriminate large group of random people. The email in this scenario appears to be untargeted since it was sent to both customers and non-customers of this particular bank so it is best classified as phishing.
Your organization has been receiving many phishing emails recently, and you are trying to determine why they are effective in getting your users to click on their links. The latest email consists of what looks like an advertisement that is offering an exclusive early access opportunity to buy a new iPhone at a discounted price. Still, there are only 5 phones available at this price. What type of social engineering principle is being exploited here?	Scarcity
You are scheduled to conduct a physical penetration test against an organization. You need to access the building when many other employees are arriving at work in the morning. Which of the following methods would be the MOST effective to utilize?	Tailgating
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?	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.
You are conducting a wireless penetration test against an organization. During your reconnaissance, you discover that their network is known as "BigCorpWireless" has their SSID broadcast is enabled. You configure your laptop to respond to requests for connection to "BigCorpWireless" and park at the far end of the parking lot. At the end of the workday, as people get in their cars in the parking lot, you see numerous smartphones connecting to your laptop over WiFi. Which of the following exploits did you utilize?	Karma attack
A malicious user is blocking cellular devices from connecting to the Internet whenever they enter the coffee shop. If they get their coffee to go and walk at least a block away from the coffee shop, their smartphones will connect to the Internet again. What type of network attack is the malicious user performing?	Frequency jamming is one of the many exploits used to compromise a wireless environment. Frequency jamming is the disruption of radio signals through the use of an over-powered signal in the same frequency range. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. There is no indication that the malicious user has created a rogue AP (which is a form of spoofing) or performing an on-path attack by having users connect through their laptop or device within this scenario.
Which of the following weaknesses exist in WPS-enabled wireless networks?	Brute force occurs within 11,000 combinations

You are planning to exploit a network-based vulnerability against an organization as part of a penetration test. You attempted to connect your laptop to the network jack in their conference room. You found yourself in the highly restricted VLAN that the organization allows its visitors to connect to when conducting presentations. This VLAN only allows you to access the internet, not the internal network. You decide you need to conduct VLAN hopping. Which of the following methods would be MOST likely to succeed?	Poison or overflow the MAC table of the switch
An attacker is using a precomputed table of values to attempt to crack your Windows password. What type of password attack is this?	Rainbow table
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?	ARP Spoofing
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 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 NetcatUsing 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 -e ", substituting the details for each parameter in each set of brackets. nc -lp 52154 -e /bin/sh
In 2014, Apple's implementation of SSL had a severe vulnerability that, when exploited, allowed an attacker to gain a privileged network position that would allow them to capture or modify data in an SSL/TLS session. This was caused by poor programming in which a failed check of the connection would exit the function too early. Based on this description, what is this an example of?	This is an example of an improper error handling vulnerability. A well-written application must be able to handle errors and exceptions gracefully. The main goal must be for the application not to fail and allow the attacker to execute code or perform an injection attack. One famous example of an improper error handling vulnerability is Apple's GoTo bug, as described above. For more details on this particular vulnerability, please see CVE-2014-1266.
In which type of attack does the attacker begin with a normal user account and then seek additional access rights?	Privilege escalation attacks seek to increase the access level that an attacker has to a target system. Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.
You are conducting a code review of a program and observe the following calculation of 0xffffffff + 1 was attempted, but the result was returned as 0x0000000. Based on this, what type of exploit could be created against this program?	Integer overflows and other integer manipulation vulnerabilities frequently result in buffer overflows. An integer overflow occurs when an arithmetic operation results in a large number to be stored in the space allocated for it. Integers are stored in 32 bits on the x86 architecture; therefore, if an integer operation results in a number greater than 0xffffffff, an integer overflow occurs, as was the case in this example.
What kind of security vulnerability would a newly discovered flaw in a software application be considered?	A zero-day vulnerability refers to a hole in software unknown to the vendor and newly discovered. This security hole can become exploited by hackers before the vendor becomes aware of it and can fix it.
Which of the following attacks would most likely be used to create an inadvertent disclosure of information from an organization's database?	A SQL injection poses the most direct and more impactful threat to an organization's database. A SQL injection could allow the attacker to execute remote commands on the database server and lead to sensitive information disclosure.
You are penetration test against Dion Training's test server. You have entered the following URL, http://test.diontraining.com/../../../../etc/shadow. What type of attack are you attempting to perform?	Directory traversal
	An XML denial of service (or XML bomb) attempts to pull in entities recursively in a defined DTD and explode the amount of memory used by the system until a denial of service condition

What is a common Service Oriented Architecture Protocol (SOAP) vulnerability?	occurs. Service-Oriented Architecture (SOA) is an architectural paradigm, and it aims to achieve a loose coupling amongst interacting distributed systems. However, SOA is affected by several security vulnerabilities, affecting the speed of its deployment in organizations. SOA is most commonly vulnerable to an XML denial of service.
While conducting a penetration test of a web application, you enter the following URL, http://test.diontraining.com/?param=<data:text/html;base64,PHNjcmlwdD5hbGVydCgnSSBsb3ZlIERpb24gVHJhaW5pbmcnK-Twvc2NyaXB0Pg==. What type of exploit are you attempting?	This is an example of a URL-based XSS (cross-site scripting) attack. A cross-site scripting attack uses a specially crafted URL that includes attack code that will cause information that users enter into their web browser to be sent to the attacker. In this example, everything from ?param onward is part of the attack. If you did have a base64 decoder, you would have found that the parameter being passed would translate to alert('I love Dion Training'), which is a simple method to cause your web browser to create a popup that displays the text "I love Dion Training."
Which of the following tools should a penetration tester use to audit instanced and policies across AWS, Microsoft Azure, and Google Cloud?	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 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 enumerate user accounts, escalate privileges, and other tasks during the post-exploitation phase against an AWS-based cloud architecture?	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.
Your network is currently under attack from multiple hosts outside of the network. Which type of attack is most likely occurring?	DDoS
Jason is conducting a physical penetration test against a company. His objective is to enter the server room that is protected by a lock using a fingerprint reader. Jason attempts to use his finger to open the lock several times without success. He then turns his finger 45 degrees to the left, and the lock authenticates him. What is MOST likely the reason the lock opened?	A biometric lock is difficult to bypass unless the installer incorrectly configures it. If the biometric lock has a high false acceptance rate, it will allow unauthorized people to open the door. The crossover error rate (CER) is the point where the false acceptance and false rejection rates are equal. When charted on a graph, this point can lean more towards accepting false positives or rejecting true positives. If it leans more towards accepting false positives, the sensitivity has decreased to allow less frustration for its users.
During the reconnaissance phase of a penetration test, you have determined that your client's employees all use Android smartphones that connect back to the corporate network over a secure VPN connection. Which of the following methods would MOST likely be the best method for exploiting these?	Use social engineering to trick a user into opening a malicious APK
During the reconnaissance phase of a penetration test, you have determined that your client's employees all use iPhones that connect back to the corporate network over a secure VPN connection. Which of the following methods would MOST likely be the best method for exploiting these?	When targeting mobile devices, you must first determine if the company uses iPhones or Android-based devices. If they are using an iPhone, it becomes much more difficult to attack since iPhone users can only install trusted apps from the App Store. If the user has jailbroken their phone, they can sideload apps and other malware. After identifying a jailbroken device, you can use social engineering to trick the user into installing your malicious code and then take control of their device.
Which mobile device strategy is most likely to introduce vulnerable devices to a corporate network?	The BYOD (bring your own device) strategy opens a network to many vulnerabilities. People can bring their personal devices to the corporate network, and their devices may contain vulnerabilities that could be allowed to roam free on a corporate network.
Syed is developing a vulnerability scanner program for a large network of sensors to monitor his company's transcontinental oil pipeline. What type of network is this?	SCADA (supervisory control and data acquisition) networks work off an ICS (industry control system) and maintain sensors and control systems over large geographic areas.

Dion Training Solutions has just installed a backup generator for their offices that use SCADA/ICS for remote monitoring of the system. The generator's control system has an embedded cellular modem that periodically connects to the generator's manufacturer to provide usage statistics. The modem is configured for outbound connections only, and the generator has no data connection with any of Dion Training's other networks. The manufacturer utilizes data minimization procedures and uses the data to recommend preventative maintenance service and ensure maximum uptime and reliability by identifying parts that need to be replaced. Which of the following cybersecurity risk is being assumed in this scenario?	There is a minimal risk being assumed in this scenario since the cellular modem is configured for outbound connections only. This also minimizes the risk of an attacker gaining remote access to the generator. The generator is logically and physically isolated from the rest of the enterprise network, so even if an attacker could exploit the generator, they could not pivot into the production network.
Which of the following is the biggest weakness with ICS and SCADA systems in a network?	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.
You are preparing for the exploitation of Dion Training's systems as part of a penetration test. During your research, you determined that Dion Training is using application containers for each of its websites. You believe that these containers are all hosted on the same physical underlying server. Which of the following components should you attempt to exploit to gain access to all of the websites at once?	Application containers are virtualized environments designed to package and run a single computing application or service and share the same host kernel. Since they share the same host kernel, they use common libraries, as well. If you can exploit the common libraries, you will gain access to every website on that server, even if they are in an application container (Type 2 Hypervisor)
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 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.
A penetration tester is using a known vulnerability to compromise an Apache webserver. After they gain access to the webserver, what is their next step to pivot to a protected system outside of the screened subnet?	Privilege escalation
Which technique is used with the ProxyChains command to allow a penetration tester to pivot to a new subnet?	ProxyChains is a tool that allows a penetration tester to pivot to a new subnet, but it must be combined with the modification of the penetration tester's routing tables on their machine. For example, assume that the exploited client machine is located in the 192.168.5.0/24 subnet, but you need to access a server in the 10.0.0.0/24 subnet. You would then need to "route add 10.0.0.0 255.255.255.0 1" (1 is the ID of your Meterpreter session). Then, you can run "proxychains " to target the new subnet.
You are conducting a penetration test and have been asked to simulate an APT. You have established TLS network connections from a victimized host in the organization's intranet to your workstation which you are using to attempt data exfiltration from the server. The TLS connection is occurring from an end user's workstation over an ephemeral port to your workstation's listener setup on port 443. You have placed modified versions of svchost.exe and cmd.exe in the victimized host's %TEMP% folder and set up scheduled tasks to establish a connection from the victimized host to your workstation every morning at 3 am. Which of the following types of post-exploitation techniques is being used?	A reverse shell is established when the target machine communicates with an attack machine that is listening on a specific port. Reverse shells are effective in bypassing firewalls, port filtering, and network address translations, unlike a bind shell.
A company has recently experienced a data breach and has lost nearly 1 GB of personally identifiable information about its customers. You have been assigned as part of the incident response team to identify how the data was leaked from the network. Your	

team has conducted an extensive investigation, and so far, the only evidence of a large amount of data leaving the network is from the email server. One user has sent numerous large attachments out of the network to their personal email address. Upon closer inspection, those emails only contain pictures of that user's recent trip to Australia. What is the most likely explanation for how the data left the network?	The most likely explanation is that the user utilized steganography to hide the leaked data inside their trip photos. Steganography is the process of hiding one message inside another. By hiding the customer's information within the digital photos, the incident response team would not see the data being hidden without knowing to look for it inside the seemingly benign pictures from the trip.
A military defense contracting company has hired your company to conduct a penetration test against their networks. Their company has a strong vulnerability management program in place, but they are concerned that they may still be subject to remote hackers' intrusion. They have asked your company to create a red team with their most skilled hackers and conduct a long-term engagement over 6-12 months. The goal of this assessment is to emulate an attacking group that uses stealth while infiltrating the network, quietly maintaining persistence, and slowly exfiltrating data out of the network over time to determine if their cybersecurity analysts could detect this type of threat. Which of the following type of threat actors will your red team need to emulate?	APT
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 scheduled task 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 configured task. 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: empeacon.bat /sc MINUTE /mo 20 /ru SYSTEM" that will create a task called "beacon" that runs the script at "C: empeacon.bat every 20 minutes as the SYSTEM level user.
Which of the following would trigger the penetration test to stop and contact the system owners during an engagement?	Suppose the team discovers any security breaches, current hacking activity, extremely critical findings on a production server, or a production server becomes unresponsive during exploitation. In that case, the team should stop what they are doing and contact their trusted point of contact within the organization to get further guidance. Deleted log files should be considered an indicator of compromise and should be investigated by the company's security team before you continue with your engagement.
During a penetration test, you conduct an exploit that creates a denial of service condition by crashing the httpd server. What should you do?	If at any point during an assessment, an issue arises due to your actions, then you should immediately stop exploitation and contact the trusted point of contact provided by the organization. You should not continue your exploitation or pivot to another machine. While you may contact the organization's customer service department, you first need to verify if that is part of the allowed communication procedures outlined in the assessment plan. If you are conducting a red team event, the customer service team may be the target and not be informed of the issues directly.
You are working as a penetration tester conducting an engagement against Dion Training's network. You have just conducted a successful exploit of the company's Active Directory server. A few minutes later, you receive a call from the company's trusted agent asking if you have just created a new administrative user named "TheMightOne" in their domain controller. You tell the agent that you did, and he says, "Ok, I will wait to see how long it takes for my team to notice it on their own." Which of the following BEST describes this scenario?	De-confliction is the process of avoiding an early conclusion to an engagement by coordinating the penetration testing team's efforts amongst themselves or with a few key trusted personnel in the client organization. If the penetration tester did not create the account, then the trusted agent would have begun an incident response to hunt down and clear the cause of a new administrative account being created. If this occurred, the penetration test would have been stopped or paused during this incident response.
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	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

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?	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.
During an assessment of the POS terminals that accept credit cards, a cybersecurity analyst notices a recent Windows operating system vulnerability exists on every terminal. Since these systems are all embedded and require a manufacturer update, the analyst cannot install Microsoft's regular patch. Which of the following options would be best to ensure the system remains protected and are compliant with the rules outlined by the PCI DSS?	Since the analyst cannot remediate the vulnerabilities by installing a patch, the next best action would be to implement some compensating controls. If a vulnerability exists that cannot be patched, compensating controls can mitigate the risk. Additionally, the analyst should document the current situation to achieve compliance with PCI DSS.
During a penetration test of your company's network, the assessor came across a spreadsheet with the passwords being used for several servers. Four of the passwords recovered are listed below. Which one is the weakest password and should be changed FIRST to increase the password's complexity?	Password policies often enforce a mixture of standard character types, including uppercase, lowercase, numbers, and symbols. The option 'pa55word' is the weakest choice since it only includes lowercase letters and numbers. The option 'Pa55w0rd' is slightly more complex since it includes uppercase letters, lowercase letters, and numbers. The option 'P@$$W0RD is also similar in complexity since it includes uppercase letters, numbers, and special characters. The most secure option is 'P@5$w0rd' since it includes a mixture of uppercase letters, lowercase letters, numbers, and special characters.
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?	Missing patches
Dion Consulting Group has recently been awarded a contract to provide cybersecurity services for a major hospital chain in 48 cities across the United States. You are conducting a vulnerability scan of the hospital's enterprise network when you detect several devices that could be vulnerable to a buffer overflow attack. Upon further investigation, you determine that these devices are PLCs used to control the hospital's elevators. Unfortunately, there is not an update available from the elevator manufacturer for these devices. Which of the following mitigations do you recommend?	The best recommendation is to conduct the elevator control system's logical or physical isolation from the rest of the production network and the internet. This should be done through the change control process that brings the appropriate stakeholders together to discuss the best way to mitigate the vulnerability to the elevator control system that defines the business impact and risk of the decision
A large, level 1 merchant is looking for a penetration testing firm to conduct their annual external PCI-DSS audit. Which of the following requirements must the firm and its penetration testers have before the merchant hires them to conduct the audit and their Report on Compliance (RoC)?	Qualified Security Assessor (QSA) companies are independent security organizations that have been qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS. QSA Employees are individuals who are employed by a QSA Company and have satisfied and continue to satisfy all QSA Requirements. The CompTIA PenTest+, CISSP, and CISA certifications are industry certifications that recognize an individual's knowledge and experience in assessing vulnerabilities and instituting IT controls in an enterprise environment.
What activity is not a part of the post-engagement cleanup?	Modifying log files
What must be developed to show security improvements over time?	Metrics
What popular open-source port scanning tool is commonly used for host discovery and service identification?	nmap
Which of the following exploitation frameworks contain plugins that can trigger buffer overflows in SCADA systems, such as /exploit/windows/scada/daq_factory_bof that can trigger a stack overflow by sending excessive requests to a service port on the system?	Metasploit is an open-source exploitation framework that uses plugins to add different exploits and functionalities. They are always in the form of a directory structure, like /exploit/windows/scada/daq_factory_bof. This represents the plugin type (exploit), the operating system involved (windows), the service/program (sca-

	da), and the specific exploit (daq_factory_bof). If you see this format in a question, the answer is most likely related to Metasploit.
What tool is used to collect wireless packet data?	Aircrack-ng
You are planning a penetration test against an organization. During your reconnaissance, you determined that they are using encryption on their hard drives to provide data at rest. The organization has agreed to provide you one day of physical access to a standard workstation to bypass the encryption. Which of the following attacks should you use to retrieve their encryption keys?	Cold boot attack - OBJ-3.5: A cold boot attack can be used by an attacker who has physical access to a computer whose hard drive is encrypted. During a cold boot attack, it is possible to retrieve the encryption keys after starting the computer from its powered down state. When the operating system begins to load, you may capture the encryption keys stored in temporary memory by performing a RAM dump on the system and analyzing its contents.
A penetration tester has exploited an FTP server using Metasploit and now wants to pivot to the organization's LAN. What is the best method for the penetration tester to use to conduct the pivot?	Create a route statement in meterpreter - OBJ-4.2: Since the penetration tester has exploited the FTP server from outside the LAN, they will need to set up a route statement in meterpreter. Metasploit makes this very simple since it also has an autoroute meterpreter script that will allow us to attack this second network through our first compromised machine (the FTP server) and then create the routes needed.
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?	Perform an SSL stripping attack - OBJ-3.3: 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.
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?	OBJ-5.3: 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 Consulting Group has been hired to analyze the cybersecurity model for a new videogame console system. The manufacturer's team has come up with four recommendations to prevent intellectual property theft and piracy. As the cybersecurity consultant on this project, which of the following would you recommend they implement first?	Ensure that each individual console has a unique key for decrypting individual licenses and tracking which console has purchased which game - OBJ-5.3: Ensuring that each console has a unique key will allow the console manufacturer to track who has purchased which games when using digital rights management licensing. This can be achieved using a hardware root of trust, such as a TPM module in the processor. While encrypting the games during distribution will provide some security, the games could be decrypted and distributed by unauthorized parties if the encryption key were ever compromised. The recommendation of making the game arbitrarily large will frustrate both authorized and unauthorized, which could negatively impact sales, so it is a poor recommendation to implement. Visibly watermarking everything will only aggravate the user, provide a negative customer experience, and not help fight software piracy.
You want to exploit the NETBIOS name service on a Windows-based network. Which of the following tools should you use?	OBJ-4.2: Responder provides a fake server and relay tool that is included with Kali Linux. It responds to LLMNR, NBT-NS (NETBIOS), POP, IMAP, SMTP, and SQL queries to recover sensitive information such as user names and passwords. Responder is configured to listen for LLMNR/NBNS queries and respond with itself as the desired destination. When the client then tries to connect, it prompts the user to log on based on the client's protocol, thus harvesting the user's credentials. 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. The arpspoof software provided by the dsniff library is used by an attacker to perform an ARP spoofing attack on the victim.
A penetration tester is emulating an insider threat during an engagement. The penetration tester was given access to a regular user account and a basic Windows 10 client on the network. The penetration tester did not receive any network diagrams, maps, or target IP address. Their goal is to identify any possible Windows domain controllers on the intranet.diontaining.com domain. Which of the following commands should they use from the command prompt to achieve their goal?	nslookup -type=any _ldap._tcp.intranet.diontraining.com nslookup -type=any _kerberos._tcp.intranet.diontraining.com
You are conducting a wireless penetration test against an organization. You have been monitoring the WPA2 encrypted network for almost an hour but have been unable to successfully capture a handshake. Which of the following exploits should you use to increase your chances of capturing a handshake?	Deauthentication attack
What techniques are commonly used by port and vulnerability scanners to enumerate the services running on a target system?1	Banner grabbing and comparing response fingerprints OBJ-2.1: Service and version identification are often performed by conducting a banner grab or by checking responses for services to known fingerprints for those services. UDP response timing and other TCP/IP stack fingerprinting techniques are used to identify operating systems only. Using nmap -O will conduct an operating system fingerprint scan, but it will not identify the other services being run.
Judith is conducting a vulnerability scan of her data center. She notices that a management interface for a virtualization platform is exposed to her vulnerability scanner. Which of the following networks should the hypervisor's management interface be exposed to ensure the best security of the virtualization platform?	Management network - OBJ-5.3: The management interface should only be exposed to an isolated or dedicated network used for the management and configuration of the network device and platforms only. This would also help reduce the likelihood of an attack against the virtualization platform or the hypervisor itself. The external zone (internet), internal zone (LAN), or screened subnet (formerly called a DMZ) should not have the management interface exposed to them.
You have been contracted to perform a known-environment web application assessment. You believe the best way to exploit the application is to provide it with a specially crafted XML file. The application normally allows users to import XML-based files and then parses them during ingestion. Which of the following support resources should you request from the organization before starting your assessment?	An XSD file OBJ-1.1: Since the scenario states that you will create a specially crafted XML file for the assessment, you will need to know the XML file structure the web application expects. An XML Schema Definition (XSD) is a recommendation that enables developers to define the structure and data types for XML documents. If the company provides this support resource to you, you will know the exact format expected by the application, which can save you a lot of time, and the organization a lot of expense during the assessment. Since this scenario stated that this was a known-environment assessment, it would be acceptable to ask for the penetration tester to ask for the organization's XSD document as a support resource.
You are planning an engagement with a new client. The client wants your penetration testers to target their web and email servers that are hosted in a screened subnet and are accessible to visitors over the Internet. Which target type best describes these targets?	External - OBJ-1.3: An external target type best describes these targets since the question doesn't clearly describe if the servers are first-party or third-party hosted. An external target type is an asset that can be accessed from outside of the organization. For example, if the webserver is visible on the Internet, it is considered an external target. An internal target type means that assets can be accessed from within the organization. This can either be physically or logically from within the network, and it best simulates an insider threat. This target type can also be used to simulate an external hacker who has gained credentials on the network, such as using a spear phishing attack. First-party hosted targets are assets hosted by the client organization themselves. Third-party hosted targets are assets hosted by a vendor, partner, or cloud service provider.

A new piece of malware attempts to exfiltrate user data by hiding the traffic and sending it over a TLS-encrypted outbound traffic over random ports. What technology would be able to detect and block this type of traffic?	Application-aware firewall OBJ-5.3: A web application firewall (WAF) or application-aware firewall would detect both the accessing of random ports and TLS encryption and identify it as suspicious. An application-aware firewall can make decisions about what applications are allowed or blocked by a firewall, and TLS connections are created and maintained by applications. A stateless packet inspection firewall allows or denies packets into the network based on the source and destination IP address or the traffic type (TCP, UDP, ICMP, etc.). A stateful packet inspection firewall monitors the active sessions and connections on a network. The process of stateful inspection determines which network packets should be allowed through the firewall by utilizing the information it gathered regarding active connections as well as the existing ACL rules. Neither a stateless nor stateful inspection firewall operates at layer 6 or layer 7, so they cannot inspect TLS connections. An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. An IDS only monitors the traffic on the network, it cannot block traffic.
Jason is conducting a penetration test against Dion Training's Windows-based network. He wants to laterally move to another host and execute an exploit he previously trick a user into downloading to the C:\Windows\temp directory on the workstation with an IP of 192.168.1.50. He types the following into his terminal: Based on these commands, what type of post-exploitation lateral movement did Jason utilize?	OBJ-3.7: Remote Procedure Call (RPC) enables inter-process communication between local and remote processes on Windows. Distributed Component Object Model (DCOM) enables the communication between software components over a network. DCOM applications use RPC as a transport mechanism for client requests. Flaws in DCOM can enable you to execute code on a remote system by assuming user privileges. For example, a DCOM application commonly used to initiate lateral movement is MMC20.Application. This enables users to execute Microsoft Management Console (MMC) snap-in operations on a Windows computer. The MMC20.application includes an ExecuteShellCommand() method that allows for a command's remote execution using a remote computer's shell. In this example, the first command told PowerShell on Jason's machine to select the MMMC snap-in on the remote computer with the IP address of 192.168.1.50. The second command then started the exploit on the remote system with a null current working directory, null parameters passed to the exploit.exe command and started it with a window state of 7. Ultimately, this would launch the exploit.exe program on the remote machine using the local administrator account.Jason is conducting a penetration test against Dion Training's Windows-based network. He wants to laterally move to another host and execute an exploit he previously trick a user into downloading to the C:\Windows\temp directory on the workstation with an IP of 192.168.1.50. He types the following into his terminal:
Cybersecurity analysts are experiencing some issues with their vulnerability scans aborting because the previous day's scans are still running when the scanner attempts to start the current day's scans. Which of the following recommendations is LEAST likely to resolve this issue?	Reduce the sensitivity of scans - OBJ-2.2: If the cybersecurity analyst were to reduce the scans' sensitivity, it still would not decrease the time spent scanning the network and could alter the effectiveness of the results received. In this scenario, the scans, as currently scoped, are taking more than 24 hours to complete with the current resources. The analyst could reduce the scans' scope, thereby scanning fewer systems or vulnerabilities signatures and taking less time to complete. Alternatively, the analyst could reduce the scans' frequency by moving to a less frequent schedule, such as one scan every 48 hours or one scan per week. The final option would be to add additional vulnerability scanners to the process. This would allow the two scanners to work together to divide the workload and complete the task within the 24-hour scan frequency currently provided.
	/etc/shadow - OBJ-3.5: The /etc/shadow file stores the actual password in an encrypted format (more like the hash of the password) for the user's account with additional properties related to the user password. Basically, it stores secure user account infor-

Which file on a Linux system is modified to set the maximum number of days before a password must be changed?	mation. All fields are separated by a colon (:) symbol. It contains one entry per line for each user listed in the /etc/passwd file. The last 6 fields provide password aging and account lockout features.
Which of the following vulnerabilities is the greatest threat to data confidentiality?	Web application SQL injection vulnerability - OBJ-5.1: Each vulnerability mentioned poses a significant risk, but the greatest threat comes from the SQL injection. An SQL injection could allow an attacker to retrieve our data from the backend database directly. Using this technique, the attacker could also alter the data and put it back, and nobody would notice everything that had been changed, thereby also affecting our data integrity. The HTTP TRACE/TRACK methods are normally used to return the full HTTP request to the requesting client for proxy-debugging purposes and allow the attacker to access sensitive information in the HTTP headers. Since this only exposes information in the headers, it minimizes the risk to our system's data confidentiality. An SSL server with SSLv3 enabled is not ideal since this is an older encryption type, but it still provides some confidentiality. The phpinfo information disclosure vulnerability prints out detailed information on both the system and the PHP configuration. This information by itself doesn't disclose any information about the data stored within the system, though, so it isn't a great threat to our data's confidentiality.
Dion Training wants to install a perimeter device on the network to block any FTP commands that an attacker might try to send over port 25. Which of the following devices would allow for deep packet inspection to catch this type of activity?	Web application firewall - OBJ-5.3: An application-aware firewall or web application firewall (WAF) can make decisions about what applications are allowed or blocked by a firewall, as opposed to simply using IP addresses and port numbers, by applications by inspecting the data contained within the packets. This is also known as deep packet inspection (DPI). A web proxy is a server application that acts as an intermediary between a client requesting a resource and the server providing that resource. A web proxy is used to monitor, inspect, or block web traffic between a client and a remote server, not FTP traffic. A layer 3 switch, or multilayer switch, is a switch that is capable of performing the functions of a router. Layer 3 switches allow for the use of ACLs, but only at layer 3 and therefore could not inspect the packets containing FTP commands being sent over port 25. A network protocol analyzer is a tool used to monitor data traffic and analyze captured signals as they travel across communication channels. While a protocol analyzer could be used to observe the FTP commands being sent over port 25, it would not be able to block them.
As part of the reconnaissance stage of a penetration test, Kumar wants to retrieve information about an organization's network infrastructure without causing an IPS alert. Which of the following is his best course of action?	Perform a DNS brute-force attack - OBJ-3.2: The best course of action is to perform a DNS brute-force attack. The DNS brute-force attack queries a list of IPs and typically bypasses IDS/IPS systems that do not alert on DNS queries. A ping sweep or a stealth scan can be easily detected by the IPS, depending on the signatures and settings being used. A DNS zone transfer is also something that often has a signature search for it and will be alerted upon since it is a common attack technique.
You are planning an engagement with a new client. The organization is hosting a domain controller and a web server in its on-premise data center. The domain controller is only accessible to those directly connected to the organization's intranet, but the webserver is located in a screened subnet that is accessible from the Internet. Which target types BEST described these two servers?	First-party hosted - OBJ-1.3: A first-party hosted target type best describes these targets since the question includes both internal (domain controller) and external (webserver) assets as part of the target scope, but both are hosted by the organization itself. First-party hosted targets are assets hosted by the client organization themselves. Third-party hosted targets are assets hosted by a vendor, partner, or cloud service provider. An external target type is an asset that can be accessed from outside of the organization. For example, if the webserver is visible on the Internet, it is considered an external target. An internal target type means that assets can be accessed from within the organization. This can either be physically or logically from within the network, and it best simulates an insider threat. This target type can also be used to

	simulate an external hacker who has gained credentials on the network, such as using a spear phishing attack.
Tim is working to prevent any remote login attacks to the root account of a Linux system. What method would be the best option to stop attacks like this while still allowing normal users to connect using ssh?	Change sshd_config to deny root login - OBJ-5.3: Linux systems use the sshd (SSH daemon) to provide ssh connectivity. If Tim changes the sshd_config to deny root logins, it will still allow any authenticated non-root user to connect over ssh. The sshd service has a configuration setting that is named PermitRootLogin. If you set this configuration setting to no or deny, all root logins will be denied by the ssh daemon. If you didn't know about this setting, you could still answer this question by using the process of elimination. An iptables rule is a Linux firewall rule, and this would block the port for ssh, not the root login. Adding root to the sudoers group won't help either since the sudoers group allows users to login as root. If you have a network IPS rule to block root logins, the IPS would have to see the traffic being sent within the SSH tunnel. This is not possible since SSH connections are encrypted end-to-end by default. Therefore, the only possible right answer is to change the sshd_config setting to deny root logins.
An outside organization has completed a penetration test for a company. One of the report items states that an attacker may have the ability to read TLS traffic from the webserver due to a software bug. What is the MOST likely mitigation for this reported item?	Ensure patches are deployed - OBJ-5.3: A patch is designed to correct a known bug or fix a known vulnerability. Since the server is allowing an attacker to read TLS traffic, which should be encrypted and unreadable, this is a software bug in the webserver's code that must be fixed using a patch. An intrusion detection system is a device or software application that monitors and reports on any malicious activity or policy violations on a network or system. An IDS would not mitigate or stop the attacker from reading the TLS traffic, it would only report that it is occurring. A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules to establish a barrier between a trusted and untrusted network. If you configured the firewall to block traffic on port 443 (HTTPS/SSL/TLS), it would block all of the webserver's legitimate users, as well. A virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. A VPN would not stop an attacker from being able to read the TLS traffic from the webserver.
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 best describes this type of attack?1	Phishing - OBJ-3.1: Phishing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Phishing attacks target an indiscriminate large group of random people. The email in this scenario appears to be untargeted since it was sent to both customers and non-customers of this particular bank so it is best classified as phishing. Spear phishing is the fraudulent practice of sending emails from a seemingly known or trusted sender to induce targeted individuals to reveal confidential information. Whaling is an email-based or web-based form of phishing that targets senior executives or wealthy individuals. A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly.

What kind of attack is an example of IP spoofing?	On-path attack - OBJ-3.2: 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.
You are working as part of a penetration testing team targeting Dion Training's Linux-based network. You want to determine if you can crack the password on their remote authentication servers. Which of the following tools should you use?	Medusa - OBJ-4.2: Medusa is a command-line-based free password cracking tool often used in brute force password attacks on remote authentication servers. W3AF (Web Application Attack and Audit Framework) is a Python tool included in Kali Linux that tries to identify and exploit any web app vulnerabilities. CeWL is a ruby app that crawls websites to generate word lists for use with other password crackers. Mimikatz is an open-source tool that enables you to view credential information stored on Microsoft Windows computers.
Which aspect of information security does Requirement 6 of PCI DSS primarily focus on?	Encryption
In the context of penetration testing, what does "Network Environmental Considerations" primarily refer to?	Factors influencing the security and functionality of network infrastructure
Which open-source methodology emphasizes the importance of conducting security testing in a manner that mirrors real-world attacks and is aligned with the principles of the scientific method?	The Open-source Security Testing Methodology Manual (OSSTMM) emphasizes the importance of conducting security testing in a manner that mirrors real-world attacks. It follows the principles of the scientific method, providing a structured approach to security testing.
Which consideration in Rules of Engagement helps determine whether the testing team can perform tests that involve exploiting vulnerabilities in a production environment?	Other restrictions
What does "Permission to Attack" refer to in the context of penetration testing?	Consent from the client to conduct testing activities
Which parameter in Rules of Engagement is crucial for addressing legal and compliance considerations related to penetration testing activities?	Other restrictions ("Other restrictions" in Rules of Engagement may include considerations related to the level of access granted to the testing team during a penetration testing engagement. This ensures that access is granted only to the extent necessary for the testing objectives.)
Which methodology is known for emphasizing the importance of understanding the attacker's mindset and simulating real-world attack scenarios to identify vulnerabilities?	PTES - The Penetration Testing Execution Standard (PTES) emphasizes the importance of understanding the attacker's mindset. It advocates for simulating real-world attack scenarios to identify vulnerabilities and weaknesses in an organization's security defenses.
Why is it essential for a penetration testing team to undergo background checks before engaging in ethical hacking activities?	To assess the programming languages used by team members

Which open-source methodology provides a framework for security testing and is focused on assessing the security of information systems through a comprehensive set of guidelines?	The Open-source Security Testing Methodology Manual (OSSTMM) is an open-source methodology that provides a framework for security testing. It is focused on assessing the security of information systems through a comprehensive set of guidelines.
Which aspect of the "Target list/in-scope assets" is relevant when conducting a penetration test on a company's physical facilities?	Physical locations
Which GDPR principle requires organizations to limit the processing of personal data to what is necessary for the intended purpose?	Data minimization - The principle of data minimization under GDPR stipulates that organizations should only process personal data that is necessary for the intended purpose. This involves collecting and retaining the minimum amount of data required to achieve a specific goal. For instance, if an online retailer only needs a customer's name and address for shipping purposes, collecting additional information, such as marital status or birthdate, would violate the principle of data minimization. Adhering to this principle not only enhances privacy but also reduces the risk associated with the unnecessary processing of personal data. By implementing data minimization practices, organizations demonstrate their commitment to responsible and ethical handling of information, aligning with GDPR's overarching objective of protecting individuals' privacy rights.
Which methodology provides a structured approach to security assessments and is designed to guide security professionals in conducting assessments across various domains, including technical, operational, and managerial areas?	ISSAF - The Information Systems Security Assessment Framework (ISSAF) provides a structured approach to security assessments. It is designed to guide security professionals in conducting assessments across various domains, including technical, operational, and managerial areas.
When assessing the security of "Application Programming Interfaces (APIs)" in a penetration test, what aspect is considered in the "Target list/in-scope assets"?	The programming languages used in API development
Why is it important to differentiate between cloud and self-hosted environments in passive reconnaissance?	Cloud environments may have distributed and dynamic resources
How does passive reconnaissance differ between cloud and self-hosted environments?	Cloud environments may have distributed and dynamic resources
What is the primary purpose of DNS lookups in passive reconnaissance?	DNS lookups play a pivotal role in passive reconnaissance by revealing critical information about a target's infrastructure. When an attacker performs DNS lookups, they query Domain Name System (DNS) servers to obtain details such as IP addresses associated with a domain. For instance, resolving the domain "example.com" to an IP address like "192.168.1.1" provides insights into the target's web servers or network architecture. This information is invaluable for mapping out the target's digital footprint and potential attack vectors. Consider a scenario where an ethical hacker is tasked with assessing the security of a corporate network. By conducting DNS lookups, they can identify not only the web servers but also other services like mail servers or subdomains. This meticulous reconnaissance aids in formulating a comprehensive penetration testing strategy, ensuring that all possible points of entry are considered. In essence, DNS lookups serve as the foundation for passive reconnaissance, allowing security professionals to gather intelligence discreetly and plan their assessments strategically.
What type of data is commonly found in password dumps?	Password dumps often contain plain-text passwords that have been leaked or exposed in security breaches. These dumps pose a significant risk as attackers can use the obtained passwords for unauthorized access to various accounts, emphasizing the importance of secure password management practices.
What is the primary goal of URL enumeration during active reconnaissance?	Identifying web application vulnerabilities

What information can be obtained from analyzing web logs during a reconnaissance exercise?	Analyzing web logs during reconnaissance provides insights into user activity on web servers, including details such as accessed resources and user interactions.
How does a company's reputation impact its security posture?	Negative reputation may attract more cyber attacks
During active reconnaissance, what does URL enumeration help in discovering?	URL enumeration in active reconnaissance helps in discovering web application vulnerabilities. By identifying and cataloging the URLs associated with web applications, security professionals can target their efforts towards assessing and securing these applications against potential exploits.
Which API type is commonly associated with exchanging data in XML format and is susceptible to security vulnerabilities?	Extensible Markup Language-Remote Procedure Call (XML-RPC) - Extensible Markup Language-Remote Procedure Call (XML-RPC) is an API type commonly associated with exchanging data in XML format. XML-RPC APIs are susceptible to security vulnerabilities, including injection attacks and data manipulation. For example, an attacker might exploit XML-RPC vulnerabilities to inject malicious code into XML requests, leading to unauthorized access or manipulation of data. Understanding and testing for XML-RPC vulnerabilities are crucial for penetration testers to help organizations secure their APIs against XML-based attacks.
What type of privilege escalation involves gaining access to additional resources or systems at the same privilege level?	Horizontal privilege escalation
What is the main characteristic of Spear Phishing in social engineering attacks?	Focusing on specific high-profile individuals within an organization - Spear Phishing in social engineering attacks involves focusing on specific high-profile individuals within an organization. Attackers conduct thorough research to tailor their attacks to the individual, increasing the chances of success. For example, an attacker might gather information about an employee's role and use that knowledge to craft a convincing and personalized phishing email. Understanding the characteristics of spear phishing is crucial for individuals and organizations to recognize and mitigate these targeted attacks.
What characterizes an on-path attack in the context of wireless attacks?	Positioning the attacker between the communicating entities to intercept or manipulate data
What is the primary goal of eavesdropping in wireless attacks?	Eavesdropping in wireless attacks involves the unauthorized interception of wireless communications to capture sensitive information. Attackers may passively listen to data transmissions, aiming to gather confidential information, such as login credentials, personal data, or business-related communications. For example, an attacker might use tools like Wireshark to capture and analyze unencrypted wireless traffic, extracting valuable information from the intercepted data. Understanding and testing for eavesdropping vulnerabilities are essential for penetration testers to help organizations secure their wireless networks against unauthorized data access.
What is the primary concern associated with Lack of Code Signing in application security?	The Lack of Code Signing in application security refers to the absence of digital signatures to verify the integrity and authenticity of code. Without proper code signing, attackers may inject malicious code into applications, leading to potential compromise. For example, an attacker might exploit the lack of code signing to tamper with application binaries, introducing malicious code that can compromise the security of the system. Understanding and testing for Lack of Code Signing vulnerabilities are crucial for penetration testers to help organizations secure their applications against unauthorized code injection.
	Nmap is a post-exploitation tool commonly used for performing network segmentation testing to identify potential routes for lateral movement within a network. It is a versatile network scanning tool that helps attackers discover open ports, services, and vulnerabil-

What post-exploitation tool is commonly used for performing network segmentation testing to identify potential routes for lateral movement within a network?	ities in network devices. For example, an attacker might use Nmap to conduct a thorough scan of network segments to find potential paths for lateral movement. Understanding and being cautious of tools like Nmap are crucial for organizations to detect and mitigate post-exploitation activities related to network segmentation testing.
How do relay attacks exploit vulnerabilities in wireless networks?	Relay attacks in wireless networks involve exploiting weaknesses in authentication mechanisms by intercepting and relaying communication between entities. Attackers position themselves between legitimate parties, capturing authentication attempts and relaying them to gain unauthorized access. For instance, an attacker might use a relay attack to intercept an authentication handshake between a user and a wireless access point, forwarding the handshake to authenticate themselves and gain access to the network. Understanding and testing for relay attack vulnerabilities are crucial for penetration testers to help organizations secure their wireless networks against unauthorized access.
What is the primary objective of Boolean SQL injection in application-based attacks?	Manipulating SQL queries without direct visibility into the results Boolean SQL injection involves manipulating SQL queries without direct visibility into the results by exploiting boolean-based conditions. Attackers use this technique to extract information based on whether a given condition is true or false. For example, an attacker might use boolean SQL injection to determine if a specific user exists in a database by manipulating the query conditions. Understanding and testing for Boolean SQL injection vulnerabilities are crucial for penetration testers to help organizations secure their applications against information extraction attacks.
Which tool is commonly used for intercepting and modifying HTTP/HTTPS traffic, analyzing and testing web applications, and identifying security vulnerabilities?	Web proxies - Web proxies are commonly used tools for intercepting and modifying HTTP/HTTPS traffic, analyzing and testing web applications, and identifying security vulnerabilities. These tools allow penetration testers to inspect and manipulate requests and responses between clients and servers. For example, a penetration tester might use a web proxy to intercept and modify requests to uncover vulnerabilities such as injection attacks or insecure data transmission. Understanding and using web proxies are crucial skills for penetration testers to assess the security of web applications.
How do New Technology LAN Manager (NTLM) relay attacks compromise network security?	Leveraging captured authentication tokens to impersonate users
What is the primary concern associated with Cross-Site Request Forgery (CSRF) in application security?	Cross-Site Request Forgery (CSRF) in application security involves forging requests on behalf of an authenticated user without their consent. Attackers may trick users into unknowingly submitting malicious requests, potentially leading to actions performed on their behalf. For example, an attacker might craft a malicious website that, when visited by an authenticated user, triggers actions on a targeted web application without the user's consent. Understanding and testing for CSRF vulnerabilities are crucial for penetration testers to help organizations secure their applications against unauthorized actions initiated by attackers.
Which tool is commonly used for intercepting and modifying HTTP/HTTPS traffic, analyzing and testing web applications, and identifying security vulnerabilities, particularly during manual testing?	SQLmap is a powerful tool specifically designed for automating the detection and exploitation of SQL injection vulnerabilities in web applications. It allows penetration testers to identify and exploit SQL injection flaws, providing detailed information about the underlying database structure. For example, a penetration tester might use SQLmap to automate the process of identifying and exploiting SQL injection vulnerabilities in a web application's database, potentially gaining unauthorized access to sensitive information. Understanding and using SQLmap is crucial for penetration testers to effectively assess the security of web applications against SQL injection attacks.

What is the primary objective of deauthentication attacks in wireless networks?	Disrupting wireless networks by disconnecting clients from access points - Deauthentication attacks in wireless networks involve sending deauthentication frames to disconnect clients from access points, disrupting their connectivity. Attackers may use this technique to force users to reconnect, potentially allowing the attacker to capture sensitive information during the reauthentication process. For example, an attacker might launch a deauthentication attack in a public Wi-Fi environment, causing users to disconnect and reconnect to a malicious access point controlled by the attacker. Understanding and testing for deauthentication vulnerabilities are essential for penetration testers to help organizations secure their wireless networks against disruptions and unauthorized access.
In a scenario where an organization wants to ensure the confidentiality and integrity of data transmission over the network, which technical control is most appropriate?	Certificate management - To ensure the confidentiality and integrity of data transmission over the network, implementing certificate management is the most appropriate technical control. Certificate management involves the proper issuance, distribution, and maintenance of digital certificates for secure communication. For example, if a penetration test reveals vulnerabilities related to insecure transmission of sensitive data, implementing certificate management ensures that secure and authenticated connections are established using digital certificates, reducing the risk of data interception and tampering.
What is the significance of deconfliction in communication during a penetration test?	Ensuring coordination and avoiding interference with other security activities
Which component of a written report outlines the specific criteria and framework used for assessing and assigning risk ratings to identified vulnerabilities?	Risk rating (reference framework) - The "Risk rating (reference framework)" section establishes the criteria and framework employed to assess the severity of identified vulnerabilities. This ensures consistency in risk evaluation and facilitates a standardized approach to prioritize remediation efforts. For example, if a vulnerability is assessed using the Common Vulnerability Scoring System (CVSS), this section would explain how the CVSS metrics were applied to determine the risk rating. A clear and well-defined reference framework in this section enhances the report's credibility and aids stakeholders in understanding the basis for risk prioritization.
Which administrative control is focused on defining and enforcing rules related to the strength and complexity of user passwords?	Minimum password requirements
Which section of a written report provides a detailed narrative of the steps taken during the simulated attacks, including the tools and techniques employed?	Attack narrative - The "Attack narrative" section serves as a detailed account of the simulated attacks performed during the penetration test. It provides insights into the methods, tools, and techniques used to exploit vulnerabilities. For instance, if the penetration test involves exploiting a web application vulnerability, the attack narrative would describe the specific steps taken to compromise the application, such as SQL injection or cross-site scripting. This section is valuable for technical staff and developers, offering a deeper understanding of the simulated attacks and aiding in the identification of security weaknesses.
Which section of a written report is specifically designed for technical staff and developers to gain insights into the discovered vulnerabilities and recommended remediation?	Remediation
Which part of a written report presents additional information, such as raw data, logs, or supplemental details that support the findings and analysis?	The "Appendix" section serves as a repository for supplementary information that bolsters the findings and analysis presented in the main body of the report. This can include raw data, logs, or detailed technical documentation. For example, if the report highlights a critical vulnerability in a server's configuration, the "Appendix" may contain detailed logs illustrating the exploitation process. This section is crucial for technical audiences, allowing them to delve deeper into the evidence supporting the identified security issues.

In the context of penetration testing, what triggers the need for status reports?	Critical findings - The discovery of critical findings triggers the need for status reports during a penetration test. Status reports communicate the urgency and severity of identified vulnerabilities, allowing stakeholders to stay informed and take appropriate actions.
Question 68Incorrect In an organization where individuals are assigned specific responsibilities for defining, implementing, and maintaining security controls, which administrative control is in place?	Policies and procedures
In the penetration testing process, what is the primary reason for deconfliction during communication?	Avoiding interference with other security activities
When engaging in post-engagement cleanup, what is the primary reason for client acceptance?	To express satisfaction with the testing process and deliverables
In an organization where employees follow a set of documented guidelines for handling sensitive information, which administrative control is being enforced?	Policies and procedures are administrative controls that provide documented guidelines for employees to follow in various aspects of their work. In the context of handling sensitive information, these policies outline the proper procedures for data protection, sharing, and storage. For example, if employees are required to follow a specific process for encrypting and transmitting sensitive data, it is an implementation of policies and procedures to maintain information security.
Which web application tool is known for its active and passive scanning capabilities, helping identify security vulnerabilities in web applications?	Burp Suite is a comprehensive web application testing tool with both active and passive scanning capabilities. It aids in identifying security vulnerabilities such as cross-site scripting (XSS), SQL injection, and other web-related vulnerabilities.
Which credential testing tool is specifically designed for brute-force attacks and dictionary attacks on various protocols, including HTTP, FTP, and SSH?	Patator is a versatile credential testing tool designed for performing brute-force and dictionary attacks on a wide range of protocols, including HTTP, FTP, and SSH. Its flexibility and support for multiple attack scenarios make it a valuable tool for penetration testers assessing password security across different services.
Which tool is widely utilized for network vulnerability scanning and is known for its extensive database of known vulnerabilities?	Nessus
Which credential testing tool is commonly used for offline password cracking by utilizing precomputed hash tables?	John The Ripper - John the Ripper is a well-known credential testing tool used for offline password cracking. It utilizes precomputed hash tables (rainbow tables) and various attack modes to crack password hashes efficiently. John the Ripper is versatile and supports a wide range of hash algorithms.
Which tool is commonly used for cracking password hashes through brute-force attacks or dictionary attacks?	Hashcat
Which cloud tool is focused on policy enforcement and compliance checking in cloud environments, helping organizations maintain secure and compliant cloud infrastructures?	Cloud Custodian is a cloud tool focused on policy enforcement and compliance checking in cloud environments. It helps organizations maintain secure and compliant cloud infrastructures by identifying and addressing policy violations within cloud deployments.
Shells, such as Bash and PowerShell (PS), are programming languages commonly used for scripting in penetration testing	False - Shells like Bash and PowerShell (PS) are not programming languages; they are command-line interfaces used for executing commands and scripts. Programming languages, such as Python and Ruby, are more commonly used for scripting in penetration testing.
Nmap scripting is commonly used to enumerate ciphers during a penetration test, providing insights into the encryption algorithms supported by services.	True Nmap scripting is commonly employed in penetration testing to enumerate ciphers, revealing the encryption algorithms supported by various services. This information helps assess the security of communication channels and identify potential weaknesses in encryption.
Which miscellaneous tool is focused on performing post-exploitation activities, including lateral movement, privilege escalation, and credential theft in Windows environments?	CrackMapExec CrackMapExec is a tool focused on performing post-exploitation activities in Windows environments. It includes features for lateral movement, privilege escalation, and credential

	theft, making it a valuable tool for red teaming and penetration testing.
Which Wireless tool is commonly used for creating rogue access points, enabling security professionals to simulate wireless attacks and test network defenses?	The Rogue access point tool is specifically designed for creating rogue wireless access points. It enables security professionals to simulate wireless attacks, assess network defenses, and evaluate how connected devices respond to potentially malicious access points.
Which steganography tool is specifically designed for concealing information within MIDI files, allowing users to embed data in musical compositions?	Coagula is a steganography tool specifically designed for concealing information within MIDI files. It enables users to embed data in musical compositions, providing a unique approach to steganography within the realm of audio files. (Review Coagula vs. Sonic Visualizer)
Enumerating ciphers during a penetration test is essential for identifying vulnerabilities in web applications.	False; Enumerating ciphers during a penetration test is more focused on assessing the encryption algorithms supported by services rather than identifying vulnerabilities in web applications.
Boolean operators are used to manipulate and combine text strings in scripting.	False
Which tool is commonly employed during a penetration test to perform comprehensive vulnerability assessments on network infrastructure?	OpenVAS - Open Vulnerability Assessment Scanner (Open VAS) is frequently used for network infrastructure vulnerability assessments during penetration tests. Open VAS identifies vulnerabilities, misconfigurations, and potential security risks in servers and network devices. For instance, using Open VAS to scan a target network: bashCopy code openvas-cli --target example.com --scan Open VAS provides detailed reports on discovered vulnerabilities, allowing penetration testers to prioritize and address potential risks. Its use in vulnerability assessments enhances the overall security posture of the network infrastructure
Which debugger is known for its ability to analyze and modify the runtime behavior of Windows applications and is commonly used for reverse engineering?	OllyDbg - OllyDbg is a popular debugger for Windows applications, commonly used for reverse engineering and analyzing the runtime behavior of executable files. It allows security professionals and researchers to inspect and modify the code during runtime, making it a valuable tool for understanding and manipulating software behavior.
Enumerating assets in penetration testing involves scanning for open ports and identifying potential vulnerabilities.	False - Enumerating assets in penetration testing involves identifying and listing target resources, such as servers and network devices. It is not directly related to scanning for open ports or identifying vulnerabilities.
Which OSINT tool is known for its capability to visualize and analyze relationships between different entities, such as individuals, organizations, and infrastructure?	Maltego is an OSINT tool that excels in visualizing and analyzing relationships between different entities. It provides graphical representations of the connections between individuals, organizations, and infrastructure, aiding in the understanding of complex relationships during the reconnaissance phase. (Review Maltego)
Lists in scripting are collections of elements, each identified by an index or a key.	Lists in scripting are collections of elements, and each element is identified by an index. They provide an ordered and indexed way to store and manipulate data.
Which debugger is known for its capability to analyze and reverse engineer binary code, providing a graphical interface for disassembling and debugging?	IDA Pro; Interactive Disassembler (IDA Pro) is a powerful debugger known for its capability to analyze and reverse engineer binary code. It provides a graphical interface for disassembling and debugging executable files, allowing security professionals and researchers to explore and understand the internals of software. IDA Pro is widely used for in-depth analysis of binary code during reverse engineering and vulnerability research.
	Kismet - Kismet is a Wireless tool used for the passive detection, tracking, and analysis of wireless networks and their associated clients. It operates in a passive mode, capturing wireless traffic to

Which Wireless tool is commonly used for the passive detection, tracking, and analysis of wireless networks and their associated clients?	identify network names, encryption types, and connected clients without actively transmitting data.
Which steganography tool is known for its capability to hide data within whitespace in text files, providing a covert communication method within text-based content?	Snow is a steganography tool known for its capability to hide data within whitespace in text files. It provides a covert communication method within text-based content, allowing users to conceal information within textual data.
Comma-separated values (CSV) is a data structure commonly used for data serialization and interchange.	False; CSV is commonly used for storing and retrieving data in a tabular format, not for data serialization and interchange. JSON is more commonly used for such purposes.
Query throttling	By using query throttling, we can be more sneaky when we're conducting our scans and limit them to certain hours. For example, I can throttle my queries so I only send one scan per hour during the regular work day. But then I might send 25 scans per hour between 9:00 PM and 5:00 AM. By running these scans outside of normal business hours, I may be able to avoid detection by a cybersecurity analyst. By enabling query throttling, I'm also going to be able to avoid tripping alerts on the network's IDS and IPS sensors by stretching out those scans over a longer period of time
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)	1) Configure the thermostat to connect to the wireless network using WPA2 encryption and a long, strong password, 2) Configure the thermostat to use a segregated part of the network by installing it into a screened subnet
Dion Training conducts weekly vulnerability scanning of their network and patches any identified issues within 24 hours. Which of the following best describes the company's risk response strategy?	Mitigation
You are analyzing a Python script that isn't functioning properly. You suspect the issue is with the string manipulation being used in the code. Review the following Python code snippet: Based on your analysis, what should be displayed on the screen by the print command?	Train, OBJ-5.2: When evaluating the code s[-12:-7], you would receive "Train" in response. Within Python, characters in a string can be accessed by their index location. If the string (s) is "DionTraining.com", then each letter from left to right is referenced as s[0] to s[15]. If you want to reference it from right to left, you simply use a negative number, such as s[-12:-7]. The format for the array is [start:end:increment], so s[-12:-7] is evaluated as starting with the 12th position from the right (T in DionTraining.com), count until it reaches the 7th position from the right, incrementing by the default value of 1 each time. This would display, from the end of the word, the 12th position (T), 11th position (r), 10th position (a), 9th position (i), and 8th position (n), and then stop. Note that when counting positions from the right, you begin counting at 1. When counting from the left, you start with position 0 and work up from there.
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?	Mandatory vacation policy
You are watching as a penetration tester is conducting an engagement against Dion Training's network. You see the following commands and output in their terminal: Which of the following vulnerabilities is the penetration tester trying to exploit?	Unsecure SUDO vulnerability, OBJ-3.7: This penetration tester is attempting to exploit an unsecured SUDO vulnerability. First, they ran the find command and specified that it should look for permissions that follow the numerical representation of the SUID bit permission (+4000). It also looked for any files owned by the root user and were considered regular files (f), then it displays them to the screen. There were 4 files found in this example, one of which was the /usr/bin/sudo file. Next, the penetration tester attempted to perform a chmod against the /usr/bin/sudo file and set its permissions to 4111. If they were successful, this would change the permissions to allow the user, the group, and everyone else on this computer to execute the sudo command.

	When the sudo command is run, because it has the SUID bit set, the user can run the command as the root user. For this reason, the /usr/bin/sudo should have its permissions set to 4411 and not 4111.
The local electric power plant contains both business networks and ICS/SCADA networks to control their equipment. Which technology should the power plant's security administrators look to implement first as part of configuring better defenses for the ICS/SCADA systems?	Intrusion prevention system (implementing an Intrusion Prevention System. ICS/SCADA machines utilize very specific commands to control the equipment and to prevent malicious activity. You could set up strict IPS rules to prevent unknown types of actions from being allowed to occur. Log consolidation is a good idea, but it won't prevent an issue and therefore isn't the most critical thing to add first. Automated patch management should not be conducted, as ICS/SCADA systems must be tested before conducting any patches. Often, patches will break ICS/SCADA functionality. Anti-virus software may or may not be able to run on the equipment, as well, since some ICS/SCADA systems often do not rely on standard operating systems like Windows)
You are analyzing a Python script that isn't functioning properly. You suspect the issue is with the string manipulation being used in the code. Review the following Python code snippet: Based on your analysis, what should be displayed on the screen by the print command? (2)	OBJ-5.2: When evaluating the code s[4::-1], you would receive "TnoiD" in response. Within Python, characters in a string can be accessed by their index location. If the string (s) is "DionTraining.com", then each letter from left to right is referenced as s[0] to s[15]. For example, if you enter s[5], you would receive the letter "r" in response. The format for the array is [start:end:increment], so s[4::-1] is evaluated as starting with the 4th position (T in DionTraining.com since computers start counting at 0), count until it reaches the beginning or end of the word, and then increment by one position each time to the left (since it was -1). This would display the 4th position (T), 3rd position (n), 2nd position (o), 1st position (i), the zero position (D), and then stop.
An attacker uses the nslookup interactive mode to locate information on a Domain Name Service (DNS). What command should they type to request the appropriate records for only the name servers?	OBJ-2.1: The nslookup command is used to query the Domain Name System to obtain the mapping between a domain name and an IP address or to view other DNS records. The "set type=ns" tells nslookup only reports information on name servers. If you used "set type=mx" instead, you would receive information only about mail exchange servers.
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. Which exploit is the website vulnerable to based on the results?	SQL injection - OBJ-2.4: The most common type of code injection is SQL injection. An SQL injection attempts to modify one or more of an SQL query's four basic functions: select, insert, delete, or update. Two common methods of performing an SQL injection are either using a single apostrophe (') or submitting an always true statement like 1=1. In the scan results, you can see that a statement of "1 OR 17 - 7 = 10" was used. Notice that %20 is the ASCII encoded equivalent of the space character. As a penetration tester, you need to be familiar with common ASCII encoded text used in URLs equivalents like %20 (space), %5c (\), and %2F (/) to identify SQL injections and file inclusions.