C1000-162: IBM Security QRadar SIEM V7.5 Analysis Exam Prep

Study online at https://quizlet.com/_gpa0qw

Which option in QRadar's dashboard creation process helps to visually distinguish critical data from less urgent information in a dashboard widget?	Set conditional formatting for key metrics.
How can you validate that exported CSV data matches the original query results?	Match Records with Source Query
If an offense is triggered by multiple rules, how can you determine which specific rule condition contributed the most to the offense?	Compare the number of events matched by each rule in the offense details.
Which right-click menu option helps to identify how often a suspicious domain has been queried in DNS logs within the last 7 days?	Right-click > "View in Log Activity" > Filter by the domain and time range.
Which of the following best describes the role of the "Network Objects" in QRadar's network hierarchy?	They define IP ranges and specific assets for monitoring
Which query type is best suited to generate a report summarizing all events correlated within an offense?	The "Advanced AQL Query Tool" is best suited for generating a detailed report summarizing all events correlated within an offense. AQL provides flexibility and precision for retrieving offense-specific event data. Options like "Offense Event Summary Query" or "Rule-Driven Query Mechanism" do not exist in QRadar.
Which of the following scenarios would likely require installing a content pack focused on third-party application monitoring?	Integrating security logs from a new cloud service provider
Which type of rule in QRadar is most useful for detecting port scanning activities?	Threshold rule
What is the appropriate QRadar search filter to find logs where an event involves more than 100 failed login attempts?	To find logs where an event involves more than 100 failed login attempts, the correct filter is failedAttempts > 100. This query filters logs based on the number of failed login attempts in the failedAttempts field. Such a filter is useful for detecting brute force attacks or other malicious login activity.
Question 50Incorrect An offense in QRadar shows activity from a previously unknown IP address within the network. What should be the first action to investigate this?	Check for associated log activity from the IP
What is the first step in the QRadar offense triage process when an offense is detected?	Evaluate the credibility and the relevance of the offense
Which QRadar Pulse feature allows analysts to customize widget behavior based on real-time conditions?	Dynamic Thresholds
Which search filter in QRadar should be used to limit results to logs containing specific event names like "Login Failed"?	eventName = 'Login Failed'
Which of the following scenarios would most likely require a review and update of a building block in QRadar?	A change in corporate security policies would most likely require a review and update of building blocks in QRadar. For example, if new policies dictate more stringent monitoring of specific user groups or assets, the building blocks defining those groups or assets need to be updated to align with the new rules. Changes in network infrastructure or QRadar versions do not usually necessitate building block updates unless they impact the scope of monitoring or event classification.
What is the best course of action when an offense is triggered by a non-malicious event, but the same offense might be indicative of future malicious activity?	Investigate and monitor for reoccurrence
What is a likely result of having overly broad conditions in a fully matched rule?	Increased number of false positives
What is required to include customized branding in a shared report?	To include customized branding in a shared report, you must "Add Branding in Report Template." This allows logos and headers to be included. Other options, such as "Custom Branding Feature," are not part of QRadar's functionality.
	They can significantly slow down the event processing performance.

Question 61Incorrect What is a potential pitfall of using overly complex regular expressions when creating custom properties in QRadar?	
What is the main purpose of the FETCH FIRST clause in an AQL query?	The FETCH FIRST clause in AQL limits the number of rows returned by a query, ensuring that the output is manageable and concise. For example, FETCH FIRST 10 ROWS ONLY retrieves the top 10 results. It does not prioritize events by chronology, grouping, or directly optimize performance, though limiting rows can indirectly speed up queries.
A penetration tester is gathering OSINT in an attempt to conduct a phishing campaign against an executive. Which of the following would be the least effective in an OSINT campaign? A.Who they manage B.Email addresses C.Social media profiles D.Web server vulnerabilities	Web server vulnerabilities are not as useful for a targeted phishing campaign. Campaigns are more effective with information like who they manage, email addresses, and profiles. Who the executive manages can sometimes be obtained from the organization's website. Email addresses are absolutely critical during an email phishing campaign. The penetration testers can attempt to either send emails that look similar to legitimate users and domains, or they could try to compromise accounts directly. Social media profiles can have very useful information like date of birth, relationships, interests, and more. They can then use these details in a wordlist to prepare a password cracking attempt with a more targeted approach.
A penetration tester is working on a project and sees a fairly recent VoIP vulnerability has come out. Which of the following records would best help them narrow down potential targets? A.TXT B.NS C.SRV D.MX	Service (SRV) record provides host and port information on services such as voice over IP (VoIP) and instant messaging (IM). Text (TXT) record provides information about a resource such as a server or network in human readable form. Nameserver (NS) record lists the authoritative DNS server for a particular domain. A standard DNS query will use DNS servers to identify the Internet Protocol (IP) address behind a particular domain or resource name. Mail Exchange (MX) record provides the mail server that accepts email messages for a particular domain.
Question A security professional is checking for domains based on certificates that are no longer allowed. What could they check for this? A.ncpa.cpl B.SAN C.SET D.CRL	The Certification Revocation List (CRL) is a list of certificates that in some way have been deemed invalid. Although effective, most online services have moved to the newer OCSP to check the validity of the certificate. Network Connections (ncpa.cpl) is a Control Panel applet for managing adapter devices, including IP address information. A more useful field in a digital certificate from a reconnaissance perspective is the subject alternative name (SAN). SANs can identify specific subdomains that can be covered by the certificate. The Social Engineering Toolkit (SET) is a Python-based collection of tools that can be used when conducting a social engineering PenTest.
Question A software engineer prepares a brief sheet on enumerating websites as part of the company's cybersecurity curriculum. What is not a true statement regarding website enumeration? A.It occurs during the footprinting and reconnaissance stage. B.It is used to identify unlinked URLs or IPs from a website to gain access to unprotected resources. C.It involves discovering resources that are in use D.It is used to discover potential attack vectors and vulnerabilities.	In this scenario, forced browsing, and not website enumeration, is used to identify unlinked URLs or IPs from a website to gain access to unprotected resources. Forced browsing is an attack technique where an attacker manually iterates through possible URLs to find unprotected content.Website enumeration is done during the footprinting and reconnaissance stage. The team will need to determine how the target hosts the site, which can be either self-hosted or cloud-based. Website enumeration involves discovering resources that are in use as well as the underlying technology used to host the server. Website enumeration discovers potential attack vectors and vulnerabilities on a web server. According to OWASP, enumeration is also referred to as Predictable Resource Location, File Enumeration, or Directory Enumeration.
	theHarvester is an intuitive tool that can search a company's visible threat landscape. The tool gathers information on subdomain

Question A penetration tester wants to gather email information for a targeted phishing campaign. Which of the following tools could they use to collect this? A.Shodan B.Dirbuster C.Metagoofil D.theHarvester	names, employee names, email addresses, PGP key entries, and open ports and service banners. Shodan is a search engine designed to locate and index IoT devices that are connected to the Internet. Dirbuster is specifically geared towards website enumeration. There are numerous tools and techniques available to evaluate a website. Metagoofil uses various python libraries such as PdfMiner, GoogleSearch, and Hachoir to scrape the metadata, and then displays the information using Hypertext Markup Language (HTML).
A security professional has just finished setting up a new public-facing web server for their organization. They want to ensure that search engine crawlers don't index certain pages or directories on the site that represent duplicate content in order to avoid potential search penalties, but still allow those pages to be crawled to facilitate link discovery. What is the most direct step the security professional can take to achieve this goal? A.Create a noindex meta tag on each page to be excluded B.Use an access control list (ACL) to restrict access to certain directories C.Configure the web server to block specific user agents D.Set up a robots.txt file to exclude certain pages or directories	Applying a noindex meta tag on each page you want to exclude from search indexing directly informs search engines to not index these pages. This method allows the pages to be crawled, facilitating link discovery, which precisely meets the requirement to manage duplicate content without incurring SEO penalties. While it controls access, an ACL does not address the issue of allowing crawlers to discover links on pages that should not be indexed, missing the target of balancing crawlability with avoiding indexing. Blocking specific user agents doesn't align with the objective of allowing all crawlers to access the pages for link discovery while avoiding indexing due to duplicate content. One can easily create and update a robots.txt file as necessary. But in this scenario, it fails to serve the goal since it prevents crawling of the pages, hindering the discovery of links on those pages.
A security analyst is trying to find older versions of a company's website which contained sensitive information. They are worried that attackers might still be able to find older versions, so they want to try using web search commands. Which web search command would help them search? A.inanchor B.inurl C.site D.cache	Use a standard cache search on a site, and you will see a recent view of the website. To do a quick check simply type cache: in the address bar. For example, cache:https://comptia.org. inanchor searches anchor text. For example, use inanchor:Certification report to search for any pages whose anchor text includes the text "Certification" and have the text "report" anywhere on the page. One would use inurl:Certification report to search for any pages whose URLs include the text "Certification" and have the text "report" anywhere on the page. The security professional would enter the site:comptia.org report to search CompTIA's website only for results including the text "report."
Question A security researcher wants to scan documents against a website for only pdf documents. What metagoofil parameter could they use? A.metagoofil -d B.metagoofil -t C.metagoofil -l D.metagoofil -n	metagoofil -t pdf scans for pdf documents. Metagoofil scrapes the metadata, and then displays the information using Hypertext Markup Language (HTML). metagoofil -d comptia.org scans for documents on Comptia.org. Metagoofil uses various python libraries such as PdfMiner, GoogleSearch, and Hachoir. metagoofil -l 75 searches for 75 documents. The output can then be viewed in a standard browser. Another valuable tool is FOCA, which can discover metadata from a variety of sources. metagoofil -n 25 downloads 25 files. You can download a copy of Metagoofil from GitHub. In addition, the tool is built into Kali Linux.
A penetration tester is conducting an OSINT reconnaissance against key employees to try to find avenues into the network and notice that they belong to specific communities. What social media site promotes products and services in short statements and provides casual customer service? A.Facebook B.LinkedIn C.Twitter D.Instagram	Twitter is used to promote products and services in short statements called tweets, as well as to provide casual customer service and bolster brand loyalty and recognition. Facebook is used for more in-depth marketing and may be more likely to include images, videos, and event scheduling. LinkedIn is used primarily for networking opportunities and job searching. Instagram is used to publish images that market an organization's products, services, and/or brand.
	Reddit is less likely to contain code from developers, though it is possible it could exist on here. The other three options are

A security professional is looking for an organization's code that might have been posted publicly by developers. Which of the following sources or techniques is least likely to contain accidental posts by a company's developers? A.Reddit B.GitHub C.Bitbucket D.SourceForge	specifically geared towards shared code repositories. GitHub enables teams to work together, regardless of their location, is free to basic users, and has reasonable costs for teams and enterprise users. Bitbucket allows inline comments, a secured workflow, and free to small teams, fee-based for larger groups. SourceForge Is free to everyone, and features discussion forums and issue tracking, as well as a robust code repository that could contain sensitive company information.
A social engineering attack observes a target's behavior without them noticing in order to gain passwords and unauthorized entry to systems. What is this called? A.Dumpster diving B.Piggybacking C.Mantrap D.Shoulder surfing	Shoulder surfing is a social engineering attack in which the malicious actor observes a target's behavior without them noticing. Dumpster diving is the act of searching the contents of trash containers for something of value. One may be able to discover actionable intel that can give you an insight into the target's business operations. Piggybacking is essentially the same thing as tailgating, but in this case, the target knows someone is following behind them. A man trap is a containment area between two separate sets of interlocking doors. This helps to control the flow of personnel into restricted areas.
A security consultant is attempting to look for default passwords for a client's D-Link phones. Which of the following should they use? A.intitle:"DPH" "web login setting" B.inurl:"ccmuser/logon.asp" C.intitle:"Grandstream Device Configuration" password D.inurl:"CallManager"	intitle:"DPH" "web login setting" would be used to find information of D -Link Phones. If they don't have the password, they can search online for the default password to try on the targeted system. inurl:"ccmuser/logon.asp" would be used to find Cisco CallManager instances. They can also try some other Google Hacking to find more information on VoIP phones that you can use to launch the attack. intitle:"Grandstream Device Configuration" password would be used to find information about Grandstream phones. inurl:"CallManager" would not be a valid instance of attempting to find CallManager instances, they would have to search for ccmuser.
Question A team is conducting a physical assessment and uses Styrofoam to mask a certain control. Which control are they likely bypassing? A.Motion sensor B.Fences C.Security badges D.Locks	The team can attempt to block the motion detector by using a piece of cardboard or Styrofoam over the sensor. Many buildings have perimeter security, such as natural barriers or fences, to deter someone from simply entering the property. Cardboard would not be as helpful with this. A radio-frequency identification (RFID) badge system can be used for physical security. These badges hold an individual's authorization credentials and use a proximity reader that reads data when in range. Lock picking uses specialized tools to manipulate the components of a lock in order to gain access to a restricted area.
Question A cyber attacker has managed to manipulate DNS entries, leading victims to a malicious website that looks like a legitimate one, even when they type the correct URL in their browsers. What type of attack is this? A.Phishing B.Pharming C.Baiting D.Malvertising	Pharming is when an attacker entices the victim into navigating to a malicious web page that has been set up to look official. While this would fall under the phishing category, it more specifically falls under pharming. Phishing is a social engineering attack where the malicious actor communicates with the victim from a supposedly reputable source. Baiting is where an attacker will leave bait, such as an infected physical media, in an area where a victim can find the device. Spam can include malvertising, which is an email that looks like a normal ad, but instead includes malicious code.
A security professional wants to use SET for a targeted attack towards personnel. Which of the following can SET NOT do? A.Spear phishing B.Badge cloning	Badge cloning is not currently a capability of The Social Engineering Toolkit (SET), but it does allow for third-party modules. Spear phishing is the first option under social engineering attacks. You can download SET and install it on a Linux, Unix, and Windows machine or use it within Kali Linux. Website attack vectors are the second option under social engineering attacks. SET allows you to select from a number of

C.Website attacks D.Wireless attacks	different options that include attacking websites, mass mailings, and spear phishing attacks. Wireless attacks are the seventh option under social engineering attacks.
Question A penetration tester is trying to use Google Hacking to find more instances of Cisco CallManager. What should they use? A.intitle:"DPH" "web login setting" B.inurl:"ccmuser/logon.asp" C.intitle:"Grandstream Device Configuration" password D.inurl:"CallManager"	inurl:"ccmuser/logon.asp" would be used to find Cisco CallManager instances. They can also try some other Google Hacking to find more information on VoIP phones that you can use to launch the attack. intitle:"DPH" "web login setting" would be used to find information of D -Link Phones. If they don't have the password, they can search online for the default password to try on the targeted system. intitle:"Grandstream Device Configuration" password would be used to find information about Grandstream phones. inurl:"CallManager" would not be a valid instance of attempting to find CallManager instances, they would have to search for ccmuser.
During a penetration testing engagement, one of the team members presents a fictitious situation as real. What is this tactic called? A.Elicitation B.Hoax C.Pretexting D.Phishing	A hoax is another element of social engineering in which the attacker presents a fictitious situation as real. A hoax could be a link that leads to malicious code. Elicitation is acquiring data from the target in order to launch an attack. This is different from information gathered about the target. One social engineering tactic is to use pretexting, whereby the team will communicate, whether directly or indirectly, a lie or half-truth in order to get someone to believe a falsehood. Phishing is a social engineering attack where the malicious actor communicates with the victim from a supposedly reputable source.
A social engineer is communicating, whether directly or indirectly, a lie or half-truth in order to get someone to believe a falsehood. What is this tactic called? A.Elicitation B.Hoax C.Pretexting D.Phishing	One social engineering tactic is to use pretexting, whereby the team will communicate, whether directly or indirectly, a lie or half-truth in order to get someone to believe a falsehood. Elicitation is acquiring data from the target in order to launch an attack. This is different from information gathered about the target. A hoax is another element of social engineering in which the attacker presents a fictitious situation as real. A hoax could be a link that leads to malicious code. Phishing is a social engineering attack where the malicious actor communicates with the victim from a supposedly reputable source.
The Social Engineering Toolkit is being employed for a targeted attack towards personnel. Which of the following can SET NOT do? A.Mass mail attacks B.Infectious media C.Scaling D.PowerShell attacks	Scaling refers to a type of physical security breach where an individual overcomes physical barriers such as fences or walls to gain unauthorized access to a property. This kind of physical intrusion falls outside the scope of the Social Engineering Toolkit, which is designed for digital social engineering attacks. Mass mail attacks are the fifth option under social engineering attacks. You can download SET and install it on a Linux, Unix, and Windows machine or use it within Kali Linux. Infectious media generator is the third option under social engineering attacks. SET allows you to select from a number of different options that include attacking websites, mass mailings, and spear phishing attacks. PowerShell attacks are the ninth option under social engineering attacks.
Question A penetration tester covertly follows an authorized employee who is unaware that anyone is behind them. What is this called? A.Tailgating B.Piggybacking C.Badge cloning D.Scaling	Tailgating is an attack where the malicious actor slips in through a secure area while covertly following an authorized employee who is unaware that anyone is behind them. Piggybacking is essentially the same thing as tailgating, but in this case, the target knows someone is following behind them. Badge cloning is the act of copying authentication data from an RFID badge's microchip to another badge. This can be done through handheld RFID writers.

	Scaling applies to perimeter security such as natural barriers or fences, to deter someone from simply entering the property.
A PenTesting team supplied an organization with a report of findings and recommendations based on a recent penetration test. Who is responsible for making decisions on whether or not to heed the report's recommendations? A.C-Suite B.Third-Party stakeholders C.Technical Staff D.Developers	C-Suite are senior executives that are likely to be responsible for making decisions based on the results and recommendations from the PenTesters report. Third-Party stakeholders are the people not directly involved with the client but who may still be involved in a process related to the penetration test report. Technical Staff are the personnel that maintains the systems and are responsible for implementing or aiding in implementing some of the solutions to the issues found during the penetration test. Developers are the personnel responsible for creating and maintaining a solution, usually referring to the software development of an application, website, or something similar.
A C-Suite has convened to make decisions on the results and recommendations found in the PenTest report. Who is in this group? (Select all that apply.) A.Chief Technical Officer B.Developers C.Regulators D.Chief Information Security Officer	The Chief Technical Officer is in this group as C-Suite refers to top-level management personnel, usually with "chief" in their name, such as CEO, CTO, CIO, CSO, CISO, etc. The Chief Information Security Officer is in this group as C-Suite refers to top-level management personnel, usually with "chief" in their name, such as CEO, CTO, CIO, CSO, CISO, etc. Developers are the personnel responsible for creating and maintaining a solution, usually referring to the software development of an application, website, or something similar. Regulators are third-Party stakeholders and are not directly involved with the client but who may still be involved in a process related to the penetration test report.
Question A PenTesting team has submitted a report of findings and recommendations for a recent penetration test. Who will be responsible for implementing these recommendations? A.Third-Party stakeholders B.C-Suite C.Technical Staff D.Developers	Technical Staff are the personnel that maintains the systems and are responsible for implementing or aiding in implementing some of the solutions to the issues found during the penetration test. Third-Party stakeholders are the people not directly involved with the client but who may still be involved in a process related to the penetration test report. C-Suite refers to senior executives that are likely to be responsible for making decisions based on the results and recommendations. Developers are the personnel responsible for creating and maintaining a solution, usually referring to the software development of an application, website, or something similar.
Question An organization is reviewing the contents of a report and has questions about the framework that the PenTesters used to conduct the penetration test. What section of the report is the organization referring to? A.Scope B.Attack narrative C.Findings D.Methodology	The organization is referring to the methodology section of the report which is a high-level description of the standards or framework the PenTesters followed to conduct the penetration test. The scope section of the report details the scope that the organization and PenTesters defined for the activity during the pre-engagement phase and includes any deviation from the original scope and the reason(s) for it. The attack narrative is a detailed explanation of the steps taken while performing the activities and the process performed by the penetration testing team. The findings section shows the issues the PenTesters identified during the activity with a table that identifies the vulnerability, the threat level, the risk rating, and whether the PenTesters exploited the vulnerability.
Question The C-Suite is reviewing a report section that details the issues that PenTesters discovered during the most recent test and the attack vectors they successfully exploited. What section of the report is this? A.Scope B.Attack narrative	This is the findings section of the report which shows the PenTesters identified during the activity and includes elements such as critical vulnerabilities, attack vectors successfully exploited, and other results. The scope section of the report details the scope that the organization and PenTesters defined for the activity during the pre-engagement phase and includes any deviation from the original scope and the reason(s) for it. The attack narrative is a detailed explanation of the steps taken while performing the activities and the process performed by the

C.Findings
D.Executive summary

penetration testing team.
An executive summary is a high-level and concise overview of the penetration test, its findings, and its impact.

Question
An organization is reading a section of a report after a recent PenTest and is reviewing the data points that the report shows contributed to the quantified vulnerability results. What is the organization reviewing?
A.Conclusion
B.Metrics
C.Measures
D.Appendix

The organization is reviewing the measures which are the specific data points that contribute to a metric, or quantifiable measurement of the status of results or processes.
The conclusion section wraps up the report. It should include a general summary statement about failures and successes, with supporting evidence written in a sentence or two.
Metrics are quantifiable measurements of the status of results or processes, and the report generally expresses them on a scale, for example, from 1 to 10.
The appendix includes any supporting evidence, or attestation of findings and may include printouts of test results, screenshots of network activity, and other evidence obtained during testing.

Question
An organization is reviewing a report from a recent PenTest. Which section of the report will help the organization understand the relationship between the PenTest findings and their implications to the organization?
A.Risk appetite
B.Risk prioritization
C.Business impact analysis
D.Risk rating

The business impact analysis involves estimating the implications to the client's organization if a malicious actor were to target the issues identified during the activity.
Risk appetite refers to the amount and type of potential vulnerabilities and threats the organization is willing to tolerate and endure.
Risk rating is the process of assigning quantitative values to the identified risks that organization's complete by following a reference framework, which is a method to consistently rate findings.
Risk prioritization is the process of adjusting the final rating of vulnerabilities to the client's needs. The PenTesters and client need to work together to prioritize the results of testing.

An organization is working to determine their risk appetite. What kinds of issues will the organization need to consider? (Select all that apply.)
A.Catastrophic losses
B.Asset availability
C.Employee turnover
D.Personnel harm

In determining risk appetite, the organization will need to consider what losses would be catastrophic to the organization and its business operations.
In determining risk appetite, the organization will need to consider what assets, processes, information, or technology must be available at all times.
In determining risk appetite, the organization will need to consider if there are any circumstances that could result in Personnel harm to anyone dealing with the organization.
In determining risk appetite, the organization will not need to consider employee turnover. Employee turnover is an onboarding and offboarding issue.

Question
An organization underwent a penetration test and insisted that the PenTesters include the organization's investor on the reported findings. What group does the investor belong to?
A.C-Suite
B.Third-Party stakeholders
C.Technical Staff
D.Developers

The investor is a third-Party stakeholder that is not directly involved with the client but who may still be involved in a process related to the penetration test report.
C-Suite refers to top-level management personnel, usually with "chief" in their name, such as CEO, CTO, CIO, CSO, CISO, etc.
Technical Staff are the personnel that maintains the systems and are responsible for implementing or aiding in implementing some of the solutions to the issues found during the penetration test.
Developers are the personnel responsible for creating and maintaining a solution, usually referring to the software development of an application, website, or something similar.

A PenTesting team discovered a backdoor in an organization's application. Who will the organization expect to create a solution for patching the backdoor?
A.Third-Party stakeholders
B.C-Suite
C.Technical Staff
D.Developers

Developers are the personnel responsible for creating and maintaining a solution, usually referring to the software development of an application, website, or something similar.
Third-Party stakeholders are the people not directly involved with the client but who may still be involved in a process related to the penetration test report.
C-Suite refers to senior executives that are likely to be responsible for making decisions based on the results and recommendations.
Technical Staff are the personnel that maintains the systems and are responsible for implementing or aiding in implementing some of the solutions to the issues found during the penetration test.

Question
An organization wants to implement video surveillance in all of its buildings but is concerned that threat actors may access the video feeds. Which of the following will NOT help the organization

Wi-Fi attacks can disconnect the cameras from the network and lose video feed so organizations should use wired over Wi-Fi connections, not Wi-Fi. Some of the best practices for video surveillance involve network segregation, frequent patching of the camera firmware, and using wired over Wi-Fi connections. Some of the best practices for video surveillance involve frequent patching of the camera firmware, using wired over Wi-Fi connections, and network segregation. As attackers with access to the video feed will gain vital information of the inside operations, organizations should always implement physical controls to keep access to video surveillance secure.	
An organization is following the recommendations in a PenTesting report and is moving people to different jobs within the organization in the afternoons. What operational control does this represent? A.Time of day restrictions B.Mandatory vacations C.Job rotation D.User training	This represents job rotation which is the practice of cycling employees through different assigned roles and helps with improving the understanding that staff has in the overall business. Time of day restrictions are types of security controls that rely on normal operating hours for users and limit the access they have when the users don't usually need it. Mandatory vacations is making employees take their vacation as users are more likely to make mistakes when they are tired, stressed, or more likely to leave the organization. User training involves requiring end-user cybersecurity training for all employees so users can identify why it is important that everyone does their part in keeping the organization and its assets secure.
An administrator is implementing a solution that will control sensitive information in the organization. What solution is the administrator configuring? A.Certificate management B.Certificate pinning C.Key rotation D.Secret management	The administrator is configuring a secret management solution which is a platform that controls passwords, key pairs, and other sensitive information that organizations must store securely. Certificate management is the process of properly administering digital security certificates and includes managing proper storage and transmission of the certificate and the suspension and revocation of them. Certificate pinning is the process of assigning a specific certificate to a particular element to avoid man-in-the-middle-attacks. Key rotation is the process of periodically generating and implementing new access keys to a server/service. Many of the recommendations for passwords also apply to keys.
Which of the following demonstrate policy recommendations a PenTesting company may provide to a client? (Select all that apply.) A.Enable channels of communication B.Implement physical security controls C.Implement KPIs D.Review policies and procedures	Enable channels of communication is a policy recommendation as both end-users and managers will provide key information regarding the implementation of a security policy. Implement key performance indicators (KPIs) is a policy recommendation so management can monitor the effectiveness of controls, see security process improvements and return on investment (ROI), and intervene in consistently weak areas. Review policies and procedures is a policy recommendation to see if technical controls are working as expected. Implement physical security controls is not considered a policy recommendation in this context because physical security measures, such as locks, security guards, and surveillance cameras, are generally categorized separately from policy recommendations that a PenTesting company would provide, which focus more on procedural and technical aspects rather than physical security implementations.
Question An administrator is installing patches and updates, disabling unused ports, and uninstalling software that the organization doesn't use anymore. What is the administrator engaged in? A.Sanitization B.Hardening	The administrator is engaged in system hardening which is the process of securing a device or application, usually to match the standards of the current system or network. Sanitization is the process of stripping user-supplied input of unwanted or untrusted data so that the application can safely process that input. Escaping, also referred to as encoding, substitutes special characters in HTML markup with representations that the industry

C.Escaping
D.Process-level remediation

refers to as entities.
Process-level remediation is the concept of resolving a finding by changing how the system uses it or implements it, therefore changing it at the process level.

Question
An organization is using mobile device management to ensure that its mobile infrastructure is secure. What are some common features of mobile device management solutions? (Select all that apply.)
A.Fingerprint login
B.Profiles
C.Remote lock
D.Encrypted containers

A common feature of mobile device management solutions is configuring devices with specific profiles according to access control policies.
A common feature of mobile device management solutions is enabling devices to use remote access technologies including remote lock and wipe capabilities.
A common feature of mobile device management solutions is constructing an encrypted container on devices in which to keep sensitive organization data.
Implementing a fingerprint login is not a common feature of mobile device management solutions although enforcing a security policy layer on applications is a common feature of mobile device management.

An organization is implementing physical controls to secure access to its location. Which of the following are physical controls? (Select all that apply.)
A.Access control vestibule
B.System hardening
C.Biometric controls
D.Video surveillance

An access control vestibule is a physical control which is the area in which an organization manages the ingress of people according to their permission to enter the building itself or different areas of it.
Biometric controls are physical controls which are enhanced forms of access control that rely on particular body features, such as the fingerprint or iris.
Video surveillance is a physical control which involves monitoring through the use of cameras. A particular consideration for security is the use of networked surveillance for remote feed access.
System hardening is a technical control which is the process of securing a device or application, usually to match the standards of the current system or network.

An organization is following the recommendations on a PenTesting report by issuing all employees an RFID access card that each employee must use to proceed through the mantrap. What kind of control is this?
A.Biometric Control
B.Physical Access Control
C.Video Surveillance Control
D.Role-based Access Control

This is a physical access control measure in the form of an access control vestibule which is the area in which the organization manages the ingress of people according to their permission to enter the building itself or different areas of it.
Biometric controls are enhanced forms of access control that rely on particular body features, such as the fingerprint or iris.
Video surveillance involves monitoring through the use of cameras. A particular consideration for security is the use of networked surveillance for remote feed access.
Role-Based Access Control is the security approach to restricting the availability of a technological resource to authorized users only.

An organization wants to enhance its security posture with multifactor authentication. Currently, they use only passwords for authentication. Which options, when combined with the existing password system, create a true multifactor authentication system? (Select all that apply.)
A.Implement biometric authentication like fingerprint or facial recognition
B.Use a security token to generate time-based one-time passwords
C.Require a smart card for access
D.Hash the existing password

Implementing biometric authentication like fingerprint or facial recognition adds a 'Something you are' factor. This, combined with a password ('Something you know'), meets the multifactor requirement. Using a security token to generate time-based one-time passwords establishes multifactor authentication. It introduces 'Something you have,' like a hardware token or mobile device generating time-based codes. This, combined with a password, meets the multifactor requirement. Requiring a smart card for access adds another layer of 'Something you have.' This, combined with a password ('Something you know'), meets the multifactor requirement. Hashing the existing password doesn't add a new type of authentication factor to the system. It remains in the 'Something you know' category.

An organization wants to implement biometric controls to secure their most sensitive information. What types of biometric controls are available for use? (Select all that apply.)

The organization can implement a facial recognition feature as a biometric control to secure their most sensitive information. The system must recognize the face to authorize the user.
The organization can implement a fingerprint reader as a biometric control to secure their most sensitive information. The system must recognize the fingerprint to authorize the user.

A.Security question B.Facial recognition C.Fingerprint D.Retina scanner	The organization can implement a retina scanner as a biometric control to secure their most sensitive information. The system must recognize the user's iris to authorize the user. A security question is not a biometric control, it is a technical control that organizations can use as part of a multifactor authentication strategy.
A PenTester is cleaning up after a penetration test. What must the PenTester do to remove a Meterpreter payload from a target system? A.Delete the file B.Shred the file C.Reboot the system D.Manually uninstall	Because Metasploit files reside in memory, the PenTester would only need to reboot the target system in order to automatically remove it. A PenTester does not need to delete Metasploit payload files because they reside in memory, although for exploit files that do not reside in memory a superficial deletion of the file may not be enough to rid the system of it. Shredding Metasploit payloads is irrelevant because these files reside in memory, so a simple reboot is all that the system needs to remove them. Metasploit payloads reside in memory so the PenTester would not need to delete them, but the PenTester may need to manually uninstall other exploit tools.
Question A PenTester created an account in an organization's financial accounting system for testing, but the finance system does not provide a method to delete the account. Where will the PenTester need to remove this account when cleaning up after an exploit? A.User database B.AD C.Local machine D.DC	Systems that place a strong emphasis on an audit trail or a change history might not provide a delete account feature. In this case, the PenTester may need to remove the accounts from the user database. Since the PenTester created the account in the finance system, the account would not be an Active Directory (AD) domain account so the PenTester could not delete it there. Since the PenTester created the account in the finance system, the account would not be on the local system so the PenTester could not delete it there. Since the PenTester created the account in the finance system, the account would not be on the Active Directory (AD) domain controller (DC).
A PenTesting company is in the follow-up phase of a client engagement. Which follow-up action is the most significant component of gaining client acceptance? A.Client acceptance B.Attestation of findings C.Retest D.Lessons learned	Attestation of findings is the most significant component of gaining client acceptance, as the client must believe that what the PenTesters have said about their people, processes, and technology is accurate. Client acceptance occurs during the formal hand-off process where the PenTesters will need to get confirmation from the client that they agree that the testing is complete and that they accept the findings. The purpose of a retest is to analyze the progress made in applying the mitigations to the attack vectors that the PenTesters found during the penetration test. The primary goal of a lessons learned report (LLR) or after-action report (AAR) is to improve the PenTest processes and tools.
A PenTesting company has provided an organization with a cost-benefit analysis to analyze the strengths and weaknesses of alternatives and determine the best options available. Where would the PenTesting company include the cost-benefit analysis? A.Client acceptance B.Attestation of findings C.Retest D.Lessons learned	The cost-benefit analysis is part of the client acceptance which is a formal hand-off process where the client agrees that the testing is complete and that they accept the findings as presented in the report. Attestation provides evidence that the findings detailed in the PenTest report are true. By signing off on the report given to the client, the PenTesters are attesting that the information in the report is authentic. The purpose of a retest is to analyze the progress made in applying the mitigations to the attack vectors that the PenTesters found during the penetration test. The primary goal of a lessons learned report (LLR) or after-action report (AAR) is to improve the PenTest processes and tools.
	The organization is in the retest phase. During this time the focus should be on researching vulnerabilities for which the team could not recommend a mitigation tactic.

A PenTesting company is researching vulnerabilities for which the team could not recommend a mitigation tactic. Which phase of follow-up actions is the organization in? A.Client acceptance B.Planning for Retest C.Attestation of findings D.Lessons learned	Client acceptance occurs during the formal hand-off process where the PenTesters will need to get confirmation from the client that they agree that the testing is complete and that they accept the findings. Attestation of findings is the most significant component of gaining client acceptance, as the client must believe that what the PenTesters have said about their people, processes, and technology is accurate. The primary goal of a lessons learned report (LLR) or after-action report (AAR) is to improve the PenTest processes and tools.
What are some actions a PenTesting company may need to perform for an organization as a follow-up? (Select all that apply.) A.Research vulnerabilities B.Schedule tests C.Work with the security team D.Clean up the environment	As a follow-up activity, the PenTesting company may need to research and test new vulnerabilities that your team discovered during the test or for which the team could not recommend a mitigation tactic. The PenTesting company may need to schedule additional tests with the client organization as a follow-up activity to reporting. The organization's security team will implement the PenTesting company's recommended mitigations and the PenTesting company may need to support that as a follow-up activity to reporting. Cleaning up the environment is part of the post-engagement cleanup to ensure that there are no artifacts leftover that an attacker could exploit, it is not a follow-up activity.
A PenTesting team has undergone a debrief and is discovering things that will help them improve their tools and processes. Which follow-up phase does this fall under? A.Client acceptance B.Retest C.Attestation of findings D.Lessons learned	This falls under the lessons learned phase where the primary goal of a lessons learned report (LLR) or after-action report (AAR) is to improve the PenTest processes and tools. Client acceptance occurs during the formal hand-off process where the PenTesters will need to get confirmation from the client that they agree that the testing is complete and that they accept the findings. During the retest phase, the focus should be on researching vulnerabilities for which the team could not recommend a mitigation tactic. Attestation of findings is the most significant component of gaining client acceptance, as the client must believe that what the PenTesters have said about their people, processes, and technology is accurate.
A PenTesting team completed a penetration test and submitted their report to the organization. What will the team's next steps be? (Select all that apply.) A.Restore original log files B.Restore original files C.Make backups D.Document exploits	Restoring any original log files is an activity the PenTesting team would perform after completing testing and submitting their report. After the PenTesting team completes testing and submits their report, they will restore any original files that the team modified or otherwise compromised. After completing testing and submitting their report, the PenTesting team would not make backups, instead, they would restore a clean backup copy of any applications that the team compromised. The PenTesting team documented all exploits and submitted them in the report so this is not an activity the team would need to repeat until they performed new testing.
A PenTester has completed testing on a Windows system and is cleaning up. Where will the PenTester go to remove any keys or scheduled tasks? (Select all that apply.) A./etc/init.d/ B.crontab C.HKLM D.HKCU	When cleaning up a Windows system, the PenTester must make sure they remove any values they added to the HKLM Run Registry keys that start a shell on a Windows system during boot. When cleaning up a Windows system, the PenTester must make sure they remove any values they added to the HKCU Run Registry keys that start a shell on a Windows system during boot. On Linux, depending on the distribution, scripts in /etc/init.d/ and /etc/systemd/ are examples of shell run-on-boot functionality. PenTesters would use a crontab file to schedule tasks on a Linux system and Windows Task Scheduler to schedule tasks on a Windows system.
A PenTester is writing a script to shred data on drives by overwriting the storage with new data several times. Which of the following statements are true when it comes to shredding data on drives?	When PenTesters shred data on HDDs (Hard Disk Drives) it is faster and more reliable because the process of writing to a hard drive is reliable.

(Select all that apply.) A.Shredding data on HDDs is slower because the write algorithm reduces wear B.Shredding data on HDDs is faster because the write process is more reliable C.Shredding data on SSDs is slower because the write algorithm reduces wear D.Shredding data on SSDs is faster because the write process is more reliable	When PenTesters shred data on SSDs (Solid State Drives) it is slower and less reliable because SSD write algorithms may write to different locations to reduce wear. Shredding data on HDDs is not slower than SSDs. It is faster because the write process for HDDs is predictable and ensures coverage for the entire disk. Shredding data on SSDs is slower and less reliable than HDDs because SSD write algorithms may write to different locations to reduce wear.
Management has gathered the team leaders at 515support.com and outlined the importance of conducting a PenTesting exercise. Your supervisor has asked the group why PenTesting is important. How would you respond?	Formalized pentesting provides a way to evaluate cyber heatlh and resiliency with the goal of reducing overall organizational risk
Management at 515support.com has been working hard at ensuring employees are well trained in identifying a phishing email. Concurrently the IT team has implemented strong spam filters to prevent phishing emails from getting to their employees. What is the RISK of employees falling victim to a phishing attack using the following information? 75% = THREAT of a phishing email reaching an employee 40% = VULNERABLE employees that might fall for a phishing attack	Knowing that RISK = THREAT x VULNERABILITY, there is a 30% chance the employees will fall victim to a phishing attack
When using a structured approach to PenTesting, each step will serve a purpose with the goal of identifying an infrastructure's defenses by identifying and exploiting any known vulnerabilities. List the four main steps of the CompTIA PenTesting process.	The CompTIA PenTesting process goes through a series of steps that include: Planning and scoping Information gathering and vulnerability scanning Attacks and exploits Reporting and communication
Threat actors follow the same main process of hacking as a professional PenTester: Reconaissance, Gain Access, Maintain Access and Cover Tracks. What steps are added during a structured PenTest?	Answers will vary. Formalized PenTesting includes 1) Planning and scoping along with 2) analysis and reporting
Part of completing a PenTesting exercise is following the imposed guidelines of various controls, laws and regulations. Summarize key takeaways of PCI-DSS.	Answers will vary. Payment Card Industry Data Security Standard (PCI DSS) specifies the controls that must be in place to securely handle credit card data. Controls include methods to minimize vulnerabilities, employ strong access control, along with consistently testing and monitoring the infrastructure.
With PCI DSS a merchant is ranked according to the number of transactions completed in a year. Describe a level 1 merchant.	A level 1 merchant is a large merchant with over six million transactions per year.
With PCI DSS, a level 1 merchant must have the external auditor perform the assessment by an approved	Quality Security Assessor (QSA)
Another regulation that affects data privacy is GDPR, which outlines specific requirements on how consumer data is protected. Listed two to three components of GDPR.	Some of the components of this law include: Require consent - means a company must obtain your permission to share your information Rescind consent - allows a consumer to opt out at any time Global reach - GDPR affects anyone who does business with residents of the EU and Britain Restrict data collection to only what is needed to interact with the site Violation reporting - a company must report a breach within 72 hours
What should a company with over 250 employees do to be compliant with the GDPR?	Under GDPR, a company with over 250 employees will need to audit their systems take rigorous steps to protect any data that is processed in their systems, either locally managed or in the cloud
A couple of colleagues thought it would be a good idea to share guidance on how the PenTesting team should conduct themselves during the PenTesting process. What topics should be covered so	Answers will vary. The team will clearly need to understand that they are to maintain confidentiality before, during, and after a PenTest exercise. Once the testing begins the team will want to

that all members exhibit professional behavior before, during and after the PenTest?	proceed with care and notify the team lead if they have observed any illegal behavior.
The team is involved with planning a PenTest exercise for 515support.com. Management is concerned that the loading dock is vulnerable to a social engineering attack, whereby someone can gain access to the building by asking someone who is on a smoking break. Prior to conducting the tests, what should the team do to prepare for the test?	Answers will vary. Prior to beginning the test they should ask appropriate questions, such as: Who will notify security personnel that the team is using a social engineering exercise to enter the building? How many individuals should be testing to see if this type of exploit is possible? Can you provide a nonworking key card to make the ploy more believable?
The team is involved with planning a PenTest exercise for 515support.com. Management has asked the team to run a series of scans at a satellite facility. Once the team is onsite and begins testing, one of the team members shows you the result of the vulnerability scan. After examining the scan, you realized the team member has scanned the wrong network. How should you proceed?	Answers will vary. Although this was an accident, you should immediately notify the team lead, as the test was outside of the scope of the PenTest.
515support.com has an established interactive website, that customers can visit, place orders, and schedule on-site visits. Because the site accepts cedit cards, they have asked the team to PenTest the companies' web applications and web services. To further define the scope of the project, what type of information will your team need from the stakeholders?	Answers will vary. When testing web applications and web services, the team should define some guidelines. For example, the team should have the client provide a percentage or discrete value of total web pages or forms that require user interaction. In addition, the team should obtain different roles and permissions for certain applications.
Many companies recognize the vulnerabilities that exist when dealing with cloud assets and have turned to professional PenTesters to test the strength of the security mechanisms. 515support.com has asked the team to test several of their cloud assets. What should the team do prior to testing company assets within the cloud?	Answers will vary. Prior to testing in the cloud, the team will need to obtain the proper permissions from the provider and determine what type of testing will be allowed. They will also need to understand what portions are off-limits. In addition, the team will need to get a complete understanding of what is hosted, and how the cloud is used, so they can identify points of weakness.
When dealing with testing physical locations, what type of location might represent a softer target as they are less likely to have as many security controls as headquarters?	An off-site asset provides a service for an organization but is not necessarily located at the same place. Off-site locations may be an easier target because of lack of stringent security measures.
When entering into a PenTesting engagement, what are some good practice guidelines for managing time?	Answers may vary. The team should focus on the task at hand, avoid distractions, adhere to the timeline, and keep the status meetings short and to the point. In addition, make sure everyone knows when to ask for help, so they don't spend too much time on any single task.
While scanning a subnetwork, a client came up and asked Gamali if he could check his web application to see if it were vulnerable to a Cross Site Scripting (XSS) attack. Gamali replied, "Let me take a look at my paperwork to see who is testing web applications." The client stated, "oh this was included, but I just completed the app and thought you can do a quick check." How should Gamali respond?	Answers may vary. Gamali should explain that if the test is not specifically in the scope of the PenTest, he cannot do the test due to legal reasons. He can then offer to check with the team lead to see what options they may have.
The management team at 515support.com has provided a list of approved tools to be used during the PenTest. Ra'Ta needs to conduct a packet sniffing exercise on one of the subnetworks to see if he can see any passwords or other information in plaintext. However, when checking, he did not see Wireshark, a tool he needed to complete the test. Ra'Ta is frustrated as he assumed Wireshark was on the list and asks you what to do. How should you respond?	Answers may vary. Explain that if it isn't on the list, he can't use the tool unless approval is granted. However, you can offer to take a look at the list to see if there are any other tools such as TCPDump, that can achieve the same goal
In the contract for 515web.net, the timeline restrictions are defined as follows: Testing will be conducted from 8:00 A.M. to 6:00 P.M. U.S. Eastern Time, Monday-Friday. Team member Eleene tells you she is planning on running a stress test on the web server on Saturday morning. What is your response?	Answers may vary: If the contract specifies the stress test can only be conducted from 8:00 AM to 6:00 PM U.S. Eastern Time, Monday-Friday, you should recommend that the team member reschedule the stress test to a time that falls within the specified testing hours to ensure compliance with the rules of engagement and contract.

Which flow parameter in QRadar is essential for identifying possible internal reconaissance activities?	Source and Destination IP Addresses
When analyzing a building block that defines network ports, which of the following would be an indication that a rule might require an update?	A new application uses a port not defined in the building block
Which of the following best describes a scenario where an anomaly rule would outperform a threshold rule in QRadar?	Detecting a sudden drop in traffic to a critical server
Which right-click investigation action is most suitable for tracing the origin of a suspicious process execution found in an offense?	Right-click > "View Process Tree" > Trace parent processes.
Which QRadar feature is used to generate a detailed offense report with event and flow data?	Advanced Reporting Tool
When maintaining a dashboard, what is the advantage of setting automatic notifications for widget search results?	It triggers real-time alerts when specific thresholds are reached
When using a reference set-based filter in an AQL query, which function is necessary to check if an event property matches an entry in the reference set?	ISIN()
Which scenario best indicates the need to deploy a QRadar content pack in a security operations center (SOC)?	Preparing the SIEM to monitor and report on advanced persistent threats (APT) using MITRE ATT&CK framework
What is the primary method for sharing a generated report with another QRadar user?	Distribute PDF via email
What function in AQL retrieves the top 5 usernames based on the number of login attempts?	ORDER BY count DESC FETCH FIRST 5 ROWS ONLY
How would you exclude events that match a specific set of IP addresses using an AQL query?	WHERE NOT sourceIP IN ("10.0.0.1", "192.168.1.1")
What is the first step in creating a scheduled report in QRadar?	Select time range for data
When analyzing an offense triggered by a failed login attempt, which indicator would most likely suggest that the offense is a false positive?	Multiple failed login attempts from a single internal IP address
How does QRadar treat events that only partially match a rule but have potential relevance to security analysts?	They are marked with lower relevance but still logged
Which factor is the most critical to consider when evaluating why an offense was triggered by a rule that monitors multiple event types?	The timeframe within which the events occurred
Which quick search feature in QRadar allows you to view all events related to a specific offense quickly?	Use "View Linked Events"
How does QRadar handle partially matched rules in terms of data retention and visibility for future offenses?	Partially matched events are stored indefinitely and can be used in future correlation rules
Which QRadar feature allows exporting search results in CSV or XML form directly?	Export from Actions Menu
Which data format should a custom property be configured to extract when focusing on identifying sensitive information leakage in email headers?	Email Address
Which of the following should be prioritized when analyzing IoCs related to phishing attacks?	Identifying malicious file hashes attached to emails
Which filter would you use to limit the results to logs generated by QRadar rule violations?	ruleTriggered = TRUE
How can misconfigured building blocks lead to false negatives in QRadar?	By excluding critical user activities from rule evaluation
Which of the following regular expressions would be best for matching a specific port number (e.g., port 8080) in log entries?	port \s8080
	APT41

Which of the following threat groups has been known for leveraging spear-phishing techniques to gain initial access, as described in the MITRE framework?	
Which feature in QRadar allows you to detect anomalies by comparing current network traffic to historical patterns?	Behavioral Analysis
In QRadar, which type of reference set would be most appropriate for storing and checking unique user IDs seen in login events?	String-based reference set
When creating offense names for QRadar, which of the following strategies will most help in identifying false positives?	Using a standard prefix for offenses triggered by non-critical events
What is a common cause of inconsistent data across QRadar Pulse widgets?	Differing saved search parameters
Which QRadar filter would help exclude logs where the source IP is an internal address (10.0.0.0/8)?	sourceIP NOT LIKE '10.%'
Which tool in QRadar is most helpful when identifying and troubleshooting 'unknown' events?	Log Source Management app
How does QRadar handle events from a log source that has not yet been fully defined in the system?	The system automatically classifies them under the 'Unknown' log source
In QRadar, what is the main advantage of using the "Saved Searches" option when building a dashboard?	It simplifies the process of adding pre-configured searches to widgets.
Compare the difference between a Statement of Work (SOW) and a Master Services Agreement (MSA).	The Master Service Agreement is a contract that establishes precedence and guidelines for any business documents that are executed between two parties. Once you have a MSA to solidify the legal terms between the parties, you can then create one or more SOW to outline project-specific services and payment terms.
Outline a couple of laws that require an organization to maintain the confidentiality of an organization's information	The Gramm-Leach-Bliley Act requires financial institutions ensure the security and confidentiality of client information and take steps to keep customer information secure. Driver's Privacy Protection Act governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule establishes national standards to protect the privacy of individuals' medical records.
When the team begins to finalize the documentation to provide the PenTest, what are the elements that are included in the contracts?	Some of the elements should include details on the following: Project scope and a definition of the work that is to be completed. Compensation specifics that include invoicing and any reports required when submitted. Requirements for any permits, licensing, or certifications. Safety guidelines and environmental concerns Insurances such as general and liability.
When searching for basic information on a target, such as the details on the leadership of an organization, what is one option you can use?	Answers will vary. To find some basic information on a target, the team can try the "about us" page of a company website
While searching the social media profiles of a target organization, the team reads a series of Facebook posts by a network administrator. The employee is dissatisfied with their colleagues and complains that they have a lax attitude toward securing and monitoring the network. How could the team use this information?	The team can focus on finding the weaknesses that may exist due to the negligent employees.
Using DNS is common during the footprinting and reconaissance phase of the PenTest. What protocol can be used to search for organizational information?	When an entity registers a domain name, the registrant will need to provide information, such as organizational and key contact details. The team can use the whois protocol to search for these details.
Your team is tasked in evaluating the source code for 515web.net. They know that they are using a source-code repository. How should you proceed?	The team should check source-code repository sites such as GitHub, Bitbucket, and SourceForge. Once there, they should examine the code to see if the developers had added sensitive

	information in their code, such as usernames and passwords, or other information that can be used to frame an attack.
You have heard that there might possibly be a leadership change in the target's infrastructure. You are fairly sure that there was a press release in the past week about the change, but there is no longer a trace of the story. What can you try to locate this information?	The team could start with searching cached pages, and then try a search using the Wayback Machine.
In order to do a more targeted search, the team is going to use Google Hacking. What advanced operators should the team enter in the search if they are looking for spreadsheets or documents with results that include the text "confidential" on 515support.com?	site: 515support.com confidential filetype:xls OR filetype:docx
When searching 515support.com's webpage, the team checks the robots.txt file. To make sure the web-crawlers don't index the wp-admin directory, what should be added to the file?	Disallow: /wp-admin/
Digital certificates used in SSL/TLS communications are another public resource that can aid in the PenTest process. What are two resources the team can use to discover more information on the company?	The team can search for information on the targets certificate information using an online SSL checker along with the Certificate Transparency (CT) framework.
Once the team has gathered the intel on the target, you'll want to determine the best plan of attack when preparing the attack phase of the PenTest. List some of the guidelines that will help your team be better prepared.	Use gathered technology information to identify potential vulnerabilities and consider ways to weaponize them in future phases. Focus on findings that are actionable and relevant. Determine how public IP addresses map to resources like web servers that you can later target. Leverage information from third-party sites to learn more about an organization and its people and consider ways the information can be used in a social engineering test. Document your findings for future reference.
How can you identify rules with the highest event count using QRadar's metrics?	Sort By Event Count Column
Which step is required to share a scheduled report with a specific user group?	Assign Group Permissions
When investigating a potential security breach, why is the 'Start Time' and 'End Time' parameter of flow data important to QRadar?	It provides context for determining the duration of suspicious activity
Which of the following IoCs is most likely to be observed when malware tries to evade detection on a system?	Processes executing with names that mimic legitimate services
How can the performance of a customized search in QRadar be optimized when dealing with large datasets?	By narrowing the search to a shorter time window
When analyzing an offense in QRadar, which of the following actions provides the most immediate insight into suspicious behavior originating from a specific IP address?	Correlating the IP address with threat intelligence
When an offense involves multiple events from different log sources, how does QRadar aggregate and display the data to simplify triage?	By grouping events based on correlation rules
What is the correct approach for detecting recurring patterns of login failures over several days using time series analysis?	Configure a BUCKET(startTime, 1 DAY) and look for spikes.
What action ensures reports are saved for later access in QRadar?	Configure Report Retention Tab
What is the primary benefit of setting a "Time Filter" in QRadar dashboard widgets?	It improves the visualization of historical data trends
Which user role is required to create and manage dashboards in QRadar Pulse?	Security Analyst
What is the correct QRadar search filter to only show logs that contain a specific username, such as 'admin'?	username = 'admin'
Which MITRE ATT&CK technique is most likely to be associated with an insider threat actor, such as the group known as "The Shadow Brokers"?	

Exfiltration Over Web Service The Shadow Brokers have been linked to exfiltration over web services, a technique used to steal sensitive data and upload it to cloud storage or external servers. This activity is a classic example of insider threat behavior where compromised or malicious insiders use trusted access to siphon data out of an organization undetected.	
What approach is used in QRadar to process 'unknown' events and eventually assign them to the correct log source?	Manual inspection of raw data and event reclassification
Which QRadar feature allows an analyst to correlate offenses from a specific IP with potential vulnerabilities associated with that IP?	Vulnerability and Asset Correlation
Question 33Incorrect During a forensic investigation, which of the following payload details is most critical for identifying the source of an exploit attempt?	The Shellcode within the payload body is most critical for identifying the source of an exploit attempt, as it contains the actual code used in the attack. The Referer and User-Agent headers provide context about the request origin but not the exploit itself.
Which benefit is unique to Ariel logs searches compared to other Ariel search types?	Access to unprocessed raw data
What key consideration should be taken into account when creating a custom property to extract data from encrypted log payloads?	Verify the encryption format and develop a decryption method.
In IBM QRadar, which feature allows the user to quickly investigate and visualize relationships between network activities?	Network Activity Graph
Which AQL function is used to join event data and flow data based on common fields like IP addresses?	join
Which of the following is the correct method to create a reference set-based filter that matches multiple event properties in a single query?	Use the ISIN() function in combination with the OR operator for each property.
When analyzing a building block related to host definitions, which of the following is a common use case for such a building block?	To exclude internal IP addresses from external threat detection rules
How can you include offense rule details in a generated report?	Select Rule Details in Fields
In QRadar, what is the most efficient way to ensure that high-volume log sources do not overwhelm a dashboard widget?	Apply a filter to limit the log sources by volume.
When performing an advanced search, what is the purpose of using the "coalesce" function in an AQL query?	To replace null values with a default value
How can custom offense naming mechanisms improve the effectiveness of automated response systems in QRadar?	By allowing the system to trigger playbooks based on offense names
Which keyword is essential to filter events based on fields that start with a specific prefix?	In AQL, the LIKE operator is used with a prefix and a wildcard character % to filter fields starting with a specific value. For example, SELECT * FROM events WHERE username LIKE "admin%" filters events where the username starts with "admin." Options like STARTSWITH, PREFIX, and MATCH are not valid AQL keywords.
Your team is tasked with gathering metadata from various documents, to locate any sensitive information, such as Excel spreadsheets containing sensitive data on the employees. What tools can they use?	The team could use either Metagoofil or FOCA to gather metadata from various documents
The team leader has tasked your group to test the targets physical security. The target has a main building, loading docks, a parking garage, and a warehouse. Which OSINT could provide the team with valuable intel?	When planning a physical PenTest, the team can use Shodan to attempt to locate the feed of a security camera outside the target's facilities. If successful, the team can get a better picture of the premises and any possible defenses that are in place.
Your team is tasked with preparing a social engineering attack on the target. One of the team members suggests they research commonalities between the target and a sister organization. What tool do you feel would be a good choice to aggregate and graph this type of information?	Maltego is the best choice for this exercise, as when searching, the results of query are placed in graphs and then links are established between each node. This will enable the team to analyze how the target and the sister organization are connected.
Geraint states he understands some of the phases of the lifecycle of a vulnerability but admits he doesn't know all of the phases. How would you explain the lifecycle to Geraint?	

Stage 1: Discover is when the vulnerability is identified. At this point, a malicious actor may create an exploit. Stage 2: Coordinate is when the vulnerability is defined, listed, and published in the CVE and CWE so that vendors and anyone involved is aware of the vulnerability. Stage 3: Mitigate is when vendors and software designers develop a patch, which is then released to the public. Stage 4: Manage is when the patch has been released and each individual organization applies the patch in order to remediate or mitigate the vulnerability. Stage 5: Document is the final phase, in that the results are recorded, and everyone takes a moment to reflect on lessons learned, in order to prevent further exposure.	
What is a zero-day and why are they so dangerous?	Answers may vary. A zero-day vulnerability is when the vendor is aware of a security flaw, but a patch has not been developed or applied on an affected system. At this point, a malicious actor can craft an attack and take advantage of the zero-day vulnerability.
Why is mapping a network an important step in the PenTesting process?	Having a topology map of the network is valuable to the PenTest team because it outlines your choice of tools and strategies. For example, you cannot conduct an ARP scan or spoof a MAC address on a remote network without direct access to that network.
During the scoping organizational/customer requirements meeting the stakeholders listed several network devices that included three Network Load Balancers. How will this affect the scanning process?	During scanning, it's important for the team to identify any devices such as load balancers that can misdirect probes or attacks
One of your team members, Giles, states that the client has listed a WAF that is in use on the network. He asks you what a WAF is and how is it used. How do you respond?	A WAF is a web application firewall that is specifically designed to monitor web applications and guard against common attacks such as cross-site scripting and SQL Injection attacks.
During the PenTest, the team may need to assess whether or not they are able to create an exploit that can bypass the antivirus protection. How can they achieve this?	One way to achieve this is by using the Social Engineering Toolkit (SET) in Kali Linux. Using SET along with Metasploit, the team can create a malicious payload, such as a virus, worm, or Trojan, and embed the payload in a PDF.
During the footprinting and reconnaissance phase, the team will have used a variety of OSINT tools and security search engines such as Shodan to gather information. What other tool can the team use to scan remote targets for hosts, services, and other details?	When testing for vulnerabilities, one tool the team can use is Censys, an attack surface analyzer that is similar to Shodan, to identify exposed systems.
When testing for vulnerabilities, one tool the team can use is Censys, an attack surface analyzer that is similar to Shodan, to identify exposed systems.	During the footprinting and reconnaissance phase, the team will have used a variety of OSINT tools and security search engines such as Shodan to gather information. What other tool can the team use to scan remote targets for hosts, services, and other details?
Packet crafting involves altering a normal IP packet before transmitting it on a network. Why would the PenTesting team use packet crafting software?	The team might use packet crafting to do the following: Set unusual TCP flags to see if a firewall allows the packet Fragement packets so that a malicious signature is not recognized by the IDS Create fragmented packets that cannot be reassembled, which can consume all of a target's CPU time and cause either a system crash or denial of service (DoS).
Web servers are often public-facing, whereas database servers are almost always on the private network. The web server will then have a backend connection to the database server. What are the listening ports for database servers using SQL?	Most database servers using SQL will listen on TCP port 1433 or UDP port 1434.
The team is ready to scan identified targets on the network. Kimora, one of the junior members of the team isn't sure of the correct process the team should use when scanning the LAN. How would you describe this process?	The team will first scan the LAN for listening hosts and then, once identified, the team will scan the ports of any listening hosts to determine which services are listening
When port scanning, the team can either do a full connect or stealth scan to identify listening services. What is the difference?	

A full connect scan will connect with the host and learn as much about the target as possible, however this type of scan can be noisier and alert devices of a possible intrusion. In contrast, a stealth scan doesn't create as much noise on the network so the team will have a better chance of remaining undetected.	
Describe the difference between a non-credentialed scan or credentialed vulnerability scan	A credentialed scan uses credentials such as usernames and passwords and is able to take a deep dive during the vulnerability scan to produce more information while auditing the network. In contrast, a non-credentialed scan has fewer permissions and can only find missing patches or updates.
Catrina needs to test the network to see if she can obtain credentials, files, images, messages, and data traveling over the network. What tool can she use to achieve this goal?	Catrina can use Wireshark, a packet sniffing tool. Packet sniffing can take advantage of cleartext protocols and data traveling across the network. The analyst can learn a great deal about the network by monitoring protocols such as: TCP, ARP, SMTP, HTTP, and others.
Raihan explains to the team that the PCI DSS requirements of an organization must require the CDE be properly segmented. What does this mean?	They must test the network to ensure that an out-of-scope network will not have the ability to communicate with the CDE.
During active reconnaissance, the team will gather MAC addresses in order to launch an ARP poisoning attack. Explain this attack method.	This attack deliberately maps an incorrect MAC address to a correct IP address, which poisons the ARP cache. This then allows an attacker to insert themselves in a man-in-the-middle attack between two legitimate hosts
Which of the following scenarios is least likely to be a false positive when triggered by a rule monitoring for data exfiltration?	Large outbound file transfers during off-peak hours to an external IP
Which of the following techniques is most appropriate for determining if an internal IP address has been compromised during offense analysis?	Examining historical offenses involving the same IP
Which step ensures all offense-related rules are included in an advanced report?	Select All Event Columns
Which widget configuration would be most useful for displaying a count of offenses that meet specific criteria, such as severity or category?	A numerical widget displaying the total count of filtered offenses.
Which QRadar feature allows you to analyze and fine-tune a building block to ensure that it includes relevant events?	Rule Tester
A building block contains a definition for critical internal servers. Which rule logic would best utilize this building block to detect potential attacks?	Correlate failed login attempts followed by successful connections to these critical servers
What happens if an unrecognized log source sends data to QRadar SIEM?	QRadar creates a default log source for processing
An offense involving multiple IP addresses includes one that has never triggered an offense before. How should this IP be prioritized in the investigation?	Prioritized for analysis to determine its role in the offense
Which feature enables analysts to filter events correlated in an offense by their severity?	Event Filter in Offense Page
What is the purpose of the "Refresh Interval" setting when configuring an external feed for a reference set?	To define how frequently QRadar updates the reference set with new data from the feed
What QRadar feature helps ensure that events contributing to a partially matched rule are still available for future analysis?	Historical Correlation
Which of the following regex patterns can detect a URL in QRadar log data?	^https?://[\w\-\.]+\.\w{2,6}$
What is the advantage of using a building block to manage host definitions for different network zones (e.g., DMZ, internal, external)?	It allows specific security policies to be applied to each zone within multiple rules
In QRadar, which method would you use to automatically populate a reference set with IP addresses from network traffic logs?	Creating a custom rule that adds IP addresses to the reference set when a condition is met

How can you automate exporting search results to CSV on a recurring schedule in QRadar?	Configure a Scheduled Report
Which step is necessary to verify that a rule's logic accurately reflects the intended security scenario after it has triggered an offense?	Perform a test run of the rule using historical event data
What option ensures that sensitive information is not included in a shared report?	Restrict Fields in Template
Which technique should be used to decode a suspicious base64 encoded string found in the payload to determine if it contains malicious content?	Copy the string and manually decode it using an external tool
Which setting should be configured to ensure that a QRadar pulse widget shows data relevant only to a specific geographic region?	Apply a filter based on IP location
Which keyword is required in a quick search to identify logs generated from a specific log source?	logSourceName = "Name"
How can right-click actions be used to identify if an offense's source IP is part of a known botnet?	Right-click > "Check IP Reputation" > Check if listed in botnet categories.
What is the primary advantage of using a saved search in QRadar when analyzing security incidents?	It ensures consistency and repeatability in analysis
During reconaissance, the PenTest will focus on discovering open and unsecured WAPs the target might have in place. Explain how wardriving can be used during this process.	War-driving is a technique that involves driving or walking around to search for open access points using a laptop or smartphone
While searching for open access points, one of the team members suggests using WiGLE. Explain what it is and how it can help during the PenTest process.	WiGLE is an OSINT tool to help during the reconnaissance phase of PenTesting as it can be used to identify open access points. In addition, it can also be used in satellite view to visualize the physical location and nearby landmarks.
During a wireless assessment of a manufacturing plant, the team will need to assess the main buildings along with several outbuildings spanning over 16 acres. What type of antenna will work best in this environment?	Answers will vary. An appropriate selection would be a nine dBi omnidirectional antenna.
Kaison, the newest member of your team, asks why the team uses Nmap when there are other scanners available today. What is your response?	Nmap is a powerful open-source scanner that can be used in a variety of ways that include: Host and service discovery Operating system fingerprinting Gathering MAC addresses Detecting vulnerable hosts
One of the team members suggests that when scanning the payroll department it might be more efficient to activate all scripts in the vulnerability category using script=vuln. Knowing that network performance is essential, how would you respond?	If the target has a healthy amount of bandwidth, and the client agrees, the team can scan using multiple concurrent scanners, which will speed up the scanning process. However, the team will need to monitor the network as this type of aggressive scanning can result in an overburdened network.
Allison was trying to scan 8080, 443, and port 80 using the command nmap -p [8080, 443,80] scanme.nmap.org and told you the command didn't work. What is wrong with the command?	The command won't work because it is not written correctly and will return a bad pattern error. The correct syntax for this command is nmap -p 8080,443,80 scanme.nmap.org.
Which of the following is an example of a port definition building block in QRadar?	A list of non-standard ports used by custom applications
Which option ensures that sensitive data is excluded when exporting search results?	Applying "Data Masking Rules" ensures sensitive information is excluded during export, maintaining data security. Other options like "Secure Export Mode" or "Data Sanitization Feature" do not exist in QRadar's export functionality.
Which time series configuration would you use to compare event trends over the last week, divided into daily intervals?	To compare event trends over the last week, divided into daily intervals, the best correct configuration is BUCKET(startTime, 1 DAY). This query groups events by 24-hour periods, allowing for a daily breakdown of event activity. Using daily intervals is useful for understanding fluctuations in event data over a larger time frame.

If an offense has a high relevance score, but a low severity score, what does this imply about the magnitude?	The magnitude will be medium due to the mixed impact of the two scores
What is the most likely consequence of a significant volume of 'unknown' events in a QRadar deployment?	Missed opportunities to detect important security incidents
How can the offense description help in identifying the rule condition that triggered an offense?	It summarizes the unique attributes which matched the rule conditions - the offense description helps in identifying the rule condition that triggered an offense by summarizing the unique attributes which matched the rule conditions. This information provides a high-level overview of why the offense was triggered, making it easier to trace back to the specific rule logic and conditions involved.
What is the most effective way to troubleshoot a QRadar Pulse Widget that is failing to display data?	Restart the QRadar system services
Which AQL function would you use to extract specific fields from event data in QRadar?	SELECT
What is the difference between a fully matched rule and a partially matched rule in QRadar?	Fully matched rules generate offenses; partially matched rules do not. In QRadar, a fully matched rule occurs when all defined conditions within the rule are met, triggering an offense. In contrast, a partially matched rule means that some, but not all conditions have been satisfied. This partial match indicates potential malicious activity but does not trigger an offense until additional conditions are met.
What is a common challenge when triaging offenses with low credibility and low relevance scores?	They are usually false positives
When should an analyst use an Ariel offense instead of an events or flows search?	To review triggered correlation rules - Offenses searches in Ariel are tailored to identify triggered correlation rules and offenses in QRadar. Packet-level analysis is performed using flows searches, raw log reviews are done with logs searches, and traffic volume statistics are handled through flows searches.
What is a key benefit of using drill-down capabilities in QRadar Pulse dashboards?	Rapidly access detailed event data from a widget
What happens when a QRadar rule uses multiple building blocks, and one of the building blocks is misconfigured?	The rule fails to trigger any offenses
What is the main purpose of defining a network hierarchy in QRadar?	To help QRadar understand internal versus external traffic
In IBM QRadar, which of the following is a benefit of using reference sets?	Overall explanation Reference sets in QRadar are dynamic lists that can be used in correlation rules to enhance real-time threat detection. For example, a reference set might contain a list of malicious IP addresses, and QRadar can immediately detect any matching IPs in network traffic. By allowing real-time updates, reference sets make it easier to adapt rules as new threat intelligence becomes available, improving the accuracy and effectiveness of incident detection.
Which feature is most useful for keeping track of high-priority offenses across different departments in a single QRadar dashboard?	Apply filters to each offense widget based on department
When an offense is triggered by a large number of failed email delivery attempts, which scenario would most likely indicate a false positive	Failed email delivery attempts corresponding to recently migrated email server are likely a false positive. Misconfigurations during server migrations often cause delivery failures. Other scenarios such as random external domains or unknown IP addresses are more indicative of malicious activity or potential spamming attempts
Which of the following would be a reason to create a rule in QRadar that correlates both Event and Flow Data?	To identify data exfiltration attempts by correlating large file downloads (Event) with outbound connections to unknown IPs (Flow)
When multiple offenses are generated from the same IP address over a short period, what should the analyst's primary action be?	

Merge the offenses and investigate as a single incident. When multiple offenses are generated from the same IP address, it is often indicative of a larger or recurring issue. Merging the offenses allows the analyst to investigate as a single incident, ensuring all correlated activities are examined together to provide a comprehensive view of the potential threat.	
When analyzing payloads for SQL injection attacks, which of the following patterns in the payload should trigger suspicion?	