Practice Exam 6

Study online at https://quizlet.com/_fjwtw5

Jonathan's team completed the first phase of their incident response process. They are currently assessing the time to recover from the incident. Using the NIST recoverability effort categories, the team has decided to predict the time to recover, but this requires additional resources. How should he categorize this using the NIST model?	the best choice is supplemented. The NIST keys are to remember that each level has additional unknowns and resources that increase the severity level from regular to supplemented then extended
Your organization's primary operating system vendor just released a critical patch for your servers. Your system administrators have recently deployed this patch and verified the installation was successful. This critical patch was designed to remediate a vulnerability that can allow a malicious actor to execute code on the server over the Internet remotely. You ran a vulnerability scan of the network and determined that all servers are still being reported as having the vulnerability. You verified all your scan configurations are correct. Which of the following might be the reason that the scan report still shows the servers as vulnerable? (SELECT ALL THAT APPLY)	: There are two reasonable choices presented: (1) the vulnerability assessment scan is returning a false positive, or (2) this critical patch did not remediate the vulnerability. It is impossible to know which is based on the description in the question. If the patch was installed successfully
You are conducting an incident response and have already eradicated the malware from a victimized system. Which of the following actions should you perform as part of the recovery phase?	Following an incident, all types of permissions should be reviewed and reinforced. This especially affects file and firewall ACLs and system privileges assigned to the administrative user accounts or groups. This is performed during the recovery phase. During the eradication phase, you would conduct sanitization, secure disposal, and reimaging.
You are conducting a vulnerability assessment when you discover a critical web application vulnerability on one of your Apache servers. Which of the following files would contain the Apache server's logs if your organization uses the default naming convention?	On Apache web servers, the logs are stored in a file named access_log. By default, the file can be located at /var/log/httpd/access_log. This file records all requests processed by the Apache server. The WebSphere Application Server uses the httpd_log file for z/OS, which is a very outdated server from the early 2000s. The http_log file is a header class file in C used by the Apache web server's pre-compiled code that provides the logging library but does not contain any actual logs itself. The file called apache_log is an executable program that parses Apache log files within in Postgres database.
Your company has been contracted to develop an Android mobile application for a major bank. You have been asked to verify the security of the Java function's source code below:	The function uses hard-coded credentials in the function, which is an insecure practice that can lead to compromise. The password for the application is shown in the source code as mR7HCS14@31&#. Even if this was obfuscated using encoding or encryption, it is a terrible security practice to include hard-coded credentials in the application since an attacker can reverse-engineer them.
A cybersecurity analyst is reviewing the logs of a Citrix NetScaler Gateway running on a FreeBSD 8.4 server and saw the following output:	A directory traversal attack aims to access files and directories stored outside the webroot folder. By manipulating variables or URLs that reference files with "dot-dot-slash (../)" sequences and its variations or using absolute file paths
What phase of the software development lifecycle is sometimes known as the acceptance, installation, and deployment phase?	The training and transition phase ensures that end users are trained on the software and entered general use. Because of these activities, this phase is sometimes called the acceptance, installation, and deployment phase. Disposition is focused on the retirement of an application or system. Operations and maintenance are focused on the portion of the lifecycle where the application or system goes into use to provide value to the end-users

	Development is the portion of the lifecycle focused on designing and coding the application or system.
As part of the reconnaissance stage of a penetration test, Kumar wants to retrieve information about an organization's network infrastructure without causing an IPS alert. Which of the following is his best course of action?	The best course of action is to perform a DNS brute-force attack. The DNS brute-force attack queries a list of IPs and typically bypasses IDS/IPS systems that do not alert on DNS queries. A ping sweep or a stealth scan can be easily detected by the IPS, depending on the signatures and settings being used. A DNS zone transfer is also something that often has a signature search for it and will be alerted upon since it is a common attack technique.
Which of the following is the default nmap scan type when you do not provide a flag when issuing the command?	Nmap performs an SYN Scan, though it substitutes a connect scan if the user does not have proper privileges to send raw packets (requires root access on Unix). A UDP scan requires the -sU flag to be issued when launching a nmap scan. A TCP FIN scan requires the -sF flag to be issued when launching a nmap scan
You have run a vulnerability scan and received the following output: Which of the following categories should this be classified as?	This vulnerability should be categories as a web application cryptographic vulnerability. This is shown by the weak SSLv3.0/TLSv1.0 protocol being used in cipher block chaining (CBC) mode. Specifically, the use of the 3DES and DES algorithms during negotiation is a significant vulnerability. A stronger protocol should be used, such as forcing the use of AES.
You are attempting to run a packet capture on a Linux workstation using the tcpdump command. Which of the following would allow you to conduct the packet capture and write the output to a file for later analysis?	The tcpdump command is a command-line packet capture utility for Linux. The tcpdump command uses the -w option to write the capture output results to a file. A .pcap extension normally identifies packet capture files. The tcpdump command uses the -r option to read the contents of a packet capture file The tcpdump command uses the -n option to show network address information in numeric format (does not resolve hostnames The tcpdump command uses the -e option to include the data link (Ethernet) header when performing a packet capture.
Which type of system would classify traffic as malicious or benign based on explicitly defined examples of malicious and benign traffic?	A machine learning (ML) system uses a computer to accomplish a task without being explicitly programmed. In the context of cybersecurity, ML generally works by analyzing example data sets to create its own ability to classify future items presented. If the system was presented with large datasets of malicious and benign traffic, it will learn which is malicious and categorize future traffic presented to it. AI goes beyond ML and can make a more complicated decision than just the classifications made by ML A deep learning system can determine what is malicious traffic without having the prior benefit of being told what is benign/malicious. A generative adversarial network is an underlying strategy used to accomplish deep learning but is not specific to the scenario described.

Where should a forensic analyst search to find a list of the wireless networks that a laptop has previously connected to with a company-owned laptop?	The Windows registry keeps a list of the wireless networks that a system has previously connected to. The registry keys can be found in the directory of HKLM\Software\Microsoft\Windows-NT\CurrentVersion\NetworkList\Profiles. This is stored in Local Machine because it logs a copy of every access point connected to all users of the machine, not just the currently logged in user.
You are analyzing DNS logs looking for indicators of compromise associated with the use of a fast-flux network. You are already aware that the names involved in this particular fast-flux network are longer than 50 characters and always end in a .org top-level domain. Which of the following REGEGX expressions would you use to filter DNS traffic that matches this?	The correct REGEX is \b[A-Za-z0-9\.\-]{50,251}+\.org to use as a filter in this case. The first phrase before the + sign indicates to match between 50 and 251 instances of any of the preceding letters (A-Z, a-z, 0-9, period, and the minus symbol).
According to Lockheed Martin's white paper "Intel Driven Defense," which of the following technologies could degrade an adversary's effort during the actions on the objectives phase of the kill chain?	During the adversary's actions on objective phase, the adversary is already deep within the victim's network and has defeated all security mechanisms. If the adversary is attempting to exfiltrate data, implementing a quality of service approach could potentially slow down the rate at which information could be exfiltrated. This is considered a degradation to their effort by purposely manipulating service quality to decrease their transfer speeds. Honeypots could deceive an enemy during the actions on objective phase as the adversary may unknowingly take actions against a honeypot instead of their real objectives, but this would be classified as deception and not degradation NIPS technologies serve to disrupt C2 channels, not degrade them. Audit logs may detect actions an adversary has taken after the fact but will not degrade the actions themselves.
Which software development model emphasizes individuals and interactions over processes and tools, customer collaboration over contract negotiation, and working software over comprehensive documentation?	The principles of the Agile Manifesto characterize agile software development. The Agile Manifesto emphasizes individuals and interactions over the processes and tools that Spiral and Waterfall rely on. It also focuses on working software, customer collaboration, and responding to change as key elements of the Agile process. The waterfall model is a breakdown of project activities into linear sequential phases. Each phase depends on the deliverables of the previous one and corresponds to a specialization of tasks. Rapid Application Development (RAD) is a form of agile software development methodology that prioritizes rapid prototype releases and iterations. Unlike the Waterfall method, RAD emphasizes software and user feedback over strict planning and requirements recording. Spiral development is a risk-driven software development model that guides a team to adopt elements of one or more process models, such as incremental, waterfall, or evolutionary prototyping.
An organization wants to choose an authentication protocol that can be used over an insecure network without implementing additional encryption services. Which of the following protocols should they choose?	The Kerberos protocol is designed to send data over insecure networks while using strong encryption to protect the information. RADIUS, TACACS+, and PAP are all protocols that contain known vulnerabilities that would require additional encryption to secure them during the authentication process.

You have been tasked to create some baseline system images to remediate vulnerabilities found in different operating systems. Before any of the images can be deployed, they must be scanned for malware and vulnerabilities. You must ensure the configurations meet industry-standard benchmarks and that the baselining creation process can be repeated frequently. What vulnerability scanner option would BEST create the process requirements to meet the industry-standard benchmarks?	Security Content Automation Protocol (SCAP) is a multi-purpose framework of specifications supporting automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement. It is an industry standard and supports testing for compliance.
Which of the following will an adversary do during the installation phase of the Lockheed Martin kill chain? (SELECT FOUR)	During the installation phase, the adversary is taking actions to establish a footprint on the target system and is attempting to make it difficult for a defender to detect their presence. The attack may also attempt to confuse any attempts to remove the adversary from the system if the detection of their presence occurs. Due to this, an attacker will attempt to install multiple backdoors, implants, web shells, scheduled tasks, services, or AutoRun keys to maintain their access to the target. Timestomping is also conducted to hide the presence of malware on the system. Opening up two-way communication with an established C2 infrastructure occurs in the command and control phase. Collecting user credentials occurs in the actions on objectives phase.
You have been asked to review the SIEM event logs for suspected APT activity. You have been given several indicators of compromise, such as a list of domain names and IP addresses. What is the BEST action to take to analyze the suspected APT activity?	You should begin by analyzing the event's trends while manually reviewing them to determine if any of the indicators match. If you only searched through the event logs using the IP addresses, this would not be sufficient as many APTs hide their activity by compromising and using legitimate networks and their IP addresses. If you only use the IP addresses to search the event logs, you would miss any events correlated only to the domain names. If you create an advanced query will all of the indicators, your search of the event logs will find nothing because no single event will include all of these IPs and domain names. Finally, while scanning for vulnerabilities known to have been used by the APTs is a good practice, it would only be effective in determining how to stop future attacks from occurring, not determine whether or not an attack has already occurred.
James is working with the software development team to integrate real-time security reviews into some of their SDLC processes. Which of the following would best meet this requirement?	Pair programming is a real-time process that would meet this requirement. It utilizes two developers working on one workstation, where one developer reviews the code being written in real-time by the other developer While the other three options can also provide a security review, none are considered "real-time" since they are asynchronous processes performed after the coding has already been completed.
	OAuth 2 is explicitly designed to authorize claims and not to authenticate users. The implementation details for fields and attributes within tokens are not defined. Open ID Connect (OIDC) is an authentication protocol that can be implemented as special types of OAuth flows with precisely defined token fields. Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service

Which protocol is paired with OAuth2 to provide authentication of users in a federated identity management solution?	provider. SAML is an XML-based markup language for security assertions. Active Directory Federation Services (ADFS) is a software component developed by Microsoft that can run on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries. Kerberos is a computer network authentication protocol that works based on tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.
Your company is adopting a cloud-first architecture model. Management wants to decommission the on-premises SIEM your analysts use and migrate it to the cloud. Which of the following is an issue with using this approach?	If there are legal or regulatory requirements that require the company to host their security audit data on-premises, then moving to the cloud will not be possible without violating applicable laws.
Following an incident, the incident response team has generated many recommendations for additional controls and items to be purchased to prevent future recurrences. Which of the following approaches best describes what the organization should do next?	Since an incident has just occurred, it is important to act swiftly to prevent a reoccurrence. The organization should still take a defined and deliberate approach to choosing the proper controls and risk mitigations. Therefore, execution through a rational business management process is the best approach, including creating a prioritized list of recommendations. Once this list has been created, the organization can conduct a cost/benefit analysis of each recommendation and determine which controls and items will be implemented in the network based upon resource availability n terms of time, person-hours, and money. This process does not need to be a long-term study or filled with complexity. Instead, it should be rapidly conducted due to the probability that an attacker may compromise the network again.
Which of the following methods could not be used to retrieve the key from a forensic copy of a BitLocker encrypted drive?	BitLocker information is not stored in the Master Boot Record (MBR). Therefore, you cannot retrieve the key from the MBR. BitLocker keys can also be retrieved via hibernation files or memory dumps. The recovery key may also be retrieved by conducting a FireWire attack on the mounted drive using a side-channel attack known as a DMA attack.
Which of the following is the biggest advantage of using Agile software development?	Agile development can react quickly to changing customer requirements since it allows all phases of software development to run in parallel instead of a linear or sequenced approach. Waterfall development, not agile development, is a structured and phase-oriented model. A frequent criticism is that the agile model can allow developers to lose focus on the project's overall objective. Agile models do not necessarily produce better, more secure, or more efficient code than other methods
A cybersecurity analyst is reviewing the logs of a proxy server and saw the following URL, http://test.diontraining.com/index.php?id=1%20OR%2017-7%3d10. What type of attack has likely occurred?	This is an example of a Boolean-based SQL injection. This occurs when data input by a user is interpreted as a SQL command rather than as normal data by the backend database. In this example, notice that the statement being parsed as part of the URL after the equal sign is equivalent to 1 or 17-7=10. This means the portion of the statement that is 17-7=10 would return a value of 1 (since it is true). Then, we are left to compute

	if 1 = 1, and since it does, the SQL database will treat this as a positive authentication.
CIO has recently made a purchasing decision to install a new security appliance that will automatically sandbox all attachments as they enter the enterprise network to run dynamic and static code analysis on them. Which of the following questions about the appliance should you consider as the SOC manager responsible for operating this new appliance for the company? (SELECT FOUR)	you must consider if you have the right people and procedures to use the new application effectively. The appliance will also need to receive security patches, feature updates, and signature definition files routinely to remain effective and secure. At later stages of analysis, your security team may need to determine why a false-positive or false-negative occurred, which requires detailed alerts or reports from the machine