Security+ Exam Review

Study online at https://quizlet.com/_fi2w57

A cybersecurity analyst just finished conducting an initial vulnerability scan and is reviewing their results. To avoid wasting their time on results that are not really a vulnerability, the analyst wants to remove any false positives before remediating the findings. Which of the following is an indicator that something in their results would be a false positive? A. A finding that shows the scanner compliance plug-ins are not up to date B. Items classified by the system as Low or as For Informational Purposes Only	B. When conducting a vulnerability scan, it is common for the report to include some findings that are classified as "low" priority or "for informational purposes only." These are most likely false positives and can be ignored by the analyst when starting their remediation efforts.
You're investigating a suspected compromise. You have noticed several files that you don't recognize. How can you quickly and effectively check if the files have been infected with malware?	Submit the files to an open-source intelligence provider like VirusTotal
Windows file servers commonly hold sensitive files, databases, passwords, and more. What common vulnerability is usually used against a Windows file server to expose sensitive files, databases, and passwords?	Missing patches Missing patches are the most common vulnerability found on both Windows and Linux systems.
During your annual cybersecurity awareness training in your company, the instructor states that employees should be careful about what information they post on social media. According to the instructor, if you post too much personal information on social media, such as your name, birthday, hometown, and other personal details, it is much easier for an attacker to conduct which type of attack to break your passwords?	Cognitive password attack
You just received a notification that your company's email servers have been blacklisted due to reports of spam originating from your domain. What information do you need to start investigating the source of the spam emails? A. Firewall logs showing the SMTP connections B. The full email header from one of the spam messages	B. You should first request a copy of one of the spam messages, including the full email header. By reading through the full headers of one of the messages, you can determine where the email originated from, whether it was from your email system or external, and if it was a spoofed email or a legitimate email.
The Pass Certs Fast corporation has recently been embarrassed by several high profile data breaches. The CIO proposes improving the company's cybersecurity posture by migrating images of all the current servers and infrastructure into a cloud-based environment. What, if any, is the flaw in moving forward with this approach?	This approach only changes the location of the network and not the attack surface of it
When conducting forensic analysis of a hard drive, what tool would BEST prevent changing the hard drive contents during your analysis?	Hardware write blocker
Which of the following would a virtual private cloud infrastructure be classified as?	Infrastructure as a Service
What platform as a service is a well-written set of carefully developed and tested scripts to orchestrate runbooks and generate consistent server builds across an enterprise?	Infrastructure as Code (IaC)
Which of the following hashing algorithms results in a 256-bit fixed output? A. SHA-2 B. NTLM C. SHA1	A. SHA-2 creates a 256-bit fixed output
A corporate workstation was recently infected with malware. The malware was able to access the workstation's credential store and steal all the usernames and passwords from the machine. Then, the malware began to infect other workstations on the network using the usernames and passwords it stole from the first workstation. The IT Director has directed its IT staff to develop a	Install an anti-virus or anti-malware solution that uses heuristic analysis

plan to prevent this issue from occurring again. What is the best way to prevent this from recurring?	
A financial services company wants to donate some old hard drives from their servers to a local charity. Still, they are concerned about the possibility of residual data being left on the drives. What secure disposal method would you recommend the company use?	Cryptographic erase
Users connecting to an SSID appear to be unable to authenticate to the captive portal. What is most likely causing the issue?	RADIUS Captive portals usually rely on 802.1x, and 802.1x uses RADIUS for authentication.
You want to provide controlled remote access to the remote administration interfaces of multiple servers hosted on a private cloud. What type of segmentation security solution is the best choice for this scenario?	Jumpbox Installing a jumpbox as a single point of entry for the administration of servers within the cloud is the best choice for this requirement. The jumpbox only runs the necessary administrative port and protocol (typically SSH). Administrators connect to the jumpbox then use the jumpbox to connect to the admin interface on the application server.
You have been asked to install a computer in a public workspace. Only an authorized user should use the computer. What requirement should you implement to prevent unauthorized users from accessing the network with this computer?	Require authentication on wake-up
David noticed that port 3389 was open on one of the POS terminals in a store during a scheduled PCI compliance scan. Based on the scan results, what service should he expect to find enabled on this terminal?	RDP RDP uses port 3389
Your email client has been acting strangely recently. Every time you open an email with an image embedded within it, the image is not displayed on your screen. What is the cause of this issue most likely?	Incorrect security settings on the email client
What access control method provides the most detailed and explicit type of access control over a resource?	Attribute-based access control (ABAC) provides the most detailed and explicit type of access control over a resource because it is capable of making access decisions based on a combination of subject and object attributes, as well as context-sensitive or system-wide attributes.
What type of digital forensic investigation is most challenging out of the 2 choices due to the on-demand nature of the analyzed assets? A. Cloud services B. Mobile devices	A. The on-demand nature of cloud services means that instances are often created and destroyed again, with no real opportunity for forensic recovery of any data.
You received an incident response report indicating a piece of malware was introduced into the company's network through a remote workstation connected to the company's servers over a VPN connection.What control should be applied to prevent this type of incident from occurring again?	NAC Network Access Control (NAC) is an approach to computer security that attempts to unify endpoint security technology (such as anti-virus, host intrusion prevention, and vulnerability assessment), user or system authentication, and network security enforcement.
You are in the recovery steps of an incident response. Your analysis revealed that the attacker exploited an unpatched vulnerability on a public-facing web server as the initial intrusion vector in this incident. Which of the following mitigations should be implemented first during the recovery? A. Disable unused user accounts and reset the admin credentials B. Scan the network for additional instances of this vulnerability and patch the affected assets	B. scanning for additional instances of this vulnerability should be performed first

You are conducting an intensive vulnerability scan to detect which ports might be open to exploitation. During the scan, one of the network services becomes disabled and impacts the production server. Which of the following sources of information would provide you with the most relevant information for you to use in determining which network service was interrupted and why? A. Syslog B. Firewall log	A. The Syslog server is a centralized log management solution. By looking through the logs on the Syslog server, the technician could determine which service failed on which server since all the logs are retained on the Syslog server from all of the network devices and servers.
During an assessment of the POS terminals that accept credit cards, a cybersecurity analyst notices a recent Windows operating system vulnerability exists on every terminal. Since these systems are all embedded and require a manufacturer update, the analyst cannot install Microsoft's regular patch. Which of the following options would be best to ensure the system remains protected and are compliant with the rules outlined by the PCI DSS? A. Build a custom OS image that includes the patch B. Identify, implement, and document compensating controls	B. Since the analyst cannot remediate the vulnerabilities by installing a patch, the next best action would be to implement some compensating controls. If a vulnerability exists that cannot be patched, compensating controls can mitigate the risk.
Hilda needs a cost-effective backup solution that would allow for the restoration of data within a 24 hour RPO. The disaster recovery plan requires that backups occur during a specific timeframe each week, and then the backups should be transported to an off-site facility for storage. What strategy should Hilda choose to BEST meet these requirements? A. Create a daily incremental backup to tape B. Configure replication of the data to a set of servers located at a hot site	A. Since the RPO must be within 24 hours, daily or hourly backups must be conducted.
What term describes the amount of risk an organization is willing to accept?	Risk appetite
A cybersecurity analyst is analyzing what they believe to be an active intrusion into their network. The indicator of compromise maps to suspected nation-state group that has strong financial motives, APT 38. Unfortunately, the analyst finds their data correlation lacking and cannot determine which assets have been affected, so they begin to review the list of network assets online. The following servers are currently online: PAYROLL_DB, DEV_SERVER7, FIREFLY, DEATHSTAR, THOR, and DION. Which of the following actions should the analyst conduct first?	Conduct a data criticality and prioritization analysis
Janet, a defense contractor for the military, performs an analysis of their enterprise network to identify what type of work the Army would be unable to perform if the network were down for more than a few days. Which of the following was Janet trying to identify? A. single point of failure B. Mission essential function	B. Mission essential functions are things that must be performed by an organization to meet its mission. For example, the Army being able to deploy its soldiers is a mission-essential function. If they couldn't do that because a network server is offline, then that system would be considered a critical system and should be prioritized for higher security and better defenses.
What is the biggest disadvantage of using single sign-on (SSO) for authentication?	It introduces a single point of failure
Your company has just finished replacing all of its computers with brand new workstations. Colleen, one of your coworkers, has asked the company's owner if she can have the old computers that are about to be thrown away. Colleen would like to refurbish the old computers by reinstalling a new operating system and donate them to a local community center for disadvantaged children in the neighborhood. The owner thinks this is a great idea but is concerned that the private and sensitive corporate data on the old computer's hard drives might be placed at risk of exposure. You have been asked to choose the best solution to sanitize or destroy the data while ensuring the computers will still be usable by the community center. What type of data destruction or sanitization method do you recommend?	Wiping

What access control methods provides the most detailed and explicit type of access control over a resource?	ABAC