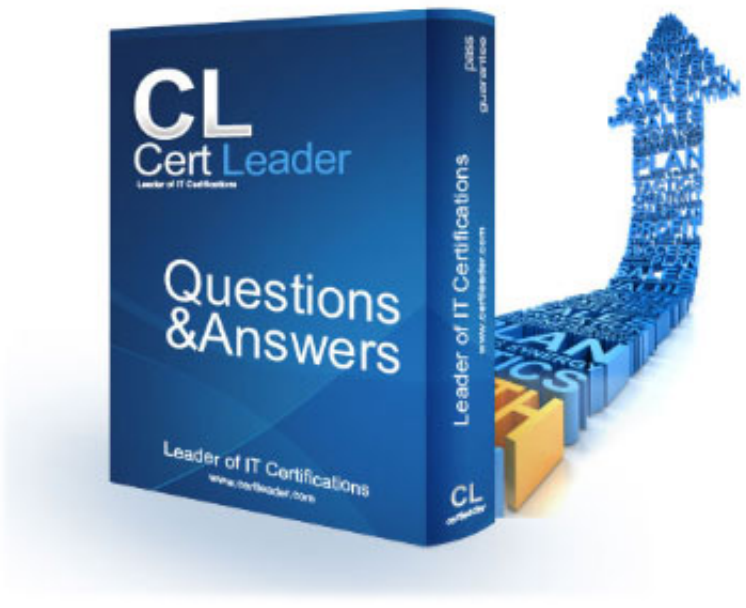
SY0-701 Dumps

CompTIA Security+ Exam

https://www.certleader.com/SY0-701-dumps.html



NEW QUESTION 1
- (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 2
- (Exam Topic 1)
A retail company that is launching @ new website to showcase the company’s product line and other information for online shoppers registered the following URLs:
* www companysite com
* shop companysite com
* about-us companysite com contact-us. companysite com secure-logon company site com
Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

A. A self-signed certificate
B. A root certificate
C. A code-signing certificate
D. A wildcard certificate
E. An extended validation certificate

Answer: D

Explanation:
The company can use a wildcard certificate to secure its website if it is concerned with convenience and cost. A wildcard certificate can secure multiple subdomains, which makes it cost-effective and convenient for securing the various registered domains.
The retail company should use a wildcard certificate if it is concerned with convenience and c1o2s.tA wildcard SSL certificate is a single SSL/TLS certificate that can provide significant time and cost savings, particularly for small businesses. The certificate includes a wildcard character (*) in the domain name field, and can secure multiple subdomains of the primary domain1

NEW QUESTION 3
- (Exam Topic 1)
Which of the following environments would MOST likely be used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics?

A. Test
B. Staging
C. Development
D. Production

Answer: A

Explanation:
The test environment is used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics. References: CompTIA Security+ Study Guide 601, Chapter 2

NEW QUESTION 4
- (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 5
- (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 6
- (Exam Topic 1)
A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?

A. laC
B. MSSP
C. Containers
D. SaaS

Answer: A

Explanation:
laaS (Infrastructure as a Service) allows the creation of virtual networks, automation, and scripting to reduce the area utilized in a datacenter. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 4

NEW QUESTION 7
- (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. A An incident response plan
B. A communications plan
C. A business continuity plan
D. A disaster recovery plan

Answer: B

Explanation:
The organization should use a communications plan to inform the affected parties. A communications plan is a document that outlines how an organization will communicate with internal and external stakeholders during a crisis or incident. It should include details such as who will be responsible for communicating with different stakeholders, what channels will be used to communicate, and what messages will be communicated.
An incident response plan is a document that outlines the steps an organization will take to respond to a security incident or data breach. A business continuity plan is a document that outlines how an organization will continue to operate during and after a disruption. A disaster recovery plan is a document that outlines how an organization will recover its IT infrastructure and data after a disaster.

NEW QUESTION 8
- (Exam Topic 1)
Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?

A. GDPR
B. PCI DSS
C. ISO 27000
D. NIST 800-53

Answer: D

Explanation:
NIST 800-53 provides a catalog of security and privacy controls related to the United States federal information systems. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3: Architecture and Design, pp. 123-125

NEW QUESTION 9
- (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 10
- (Exam Topic 1)
Which of the following BEST describes a technique that compensates researchers for finding vulnerabilities?

A. Penetration testing
B. Code review
C. Wardriving
D. Bug bounty

Answer: D

Explanation:
A bug bounty is a technique that compensates researchers for finding vulnerabilities in software or systems. A bug bounty program is an initiative that offers rewards, usually monetary, to ethical hackers who report security flaws to the owners or developers of the software or system. Bug bounty programs are often used by companies such as Meta (formerly Facebook), Google, Microsoft, and others to improve the security of their products and services
Bug bounty programs compensate researchers, often financially, for finding vulnerabilities in software, websites, or other technology. These programs provide an additional layer of security testing and incentivize researchers to report vulnerabilities instead of exploiting them.

NEW QUESTION 10
- (Exam Topic 1)
As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

A. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
C. HTTPS:// app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
D. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00

Answer: A

Explanation:
PKI certificates are digital certificates that use public key infrastructure (PKI) to verify the identity and authenticity of a sender and a receiver of data1. PKI certificates can be used to secure web applications with HTTPS, which is a protocol that encrypts and protects the data transmitted over the internet1.
One of the properties of PKI certificates is the domain name, which is the name of the website or web application that the certificate is issued for2. The domain name can be either a specific name, such as app1.comptia.org, or a wildcard name, such as *.comptia.org2. A wildcard name means that the certificate can be used with multiple subdomains of a domain, such as payment.comptia.org or contact.comptia.org2.
Another property of PKI certificates is the validity period, which is the time span during which the certificate is valid and can be used3. The validity period is determined by the certificate authority (CA) that issues the certificate, and it usually ranges from one to three years3. The validity period can be checked by looking at the valid from and valid to dates on the certificate3.
Based on these properties, the certificate that will meet the requirements of rotating annually and only containing wildcards at the secondary subdomain level is A. HTTPS://*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022. This certificate has a wildcard character (*) at the secondary subdomain level, which means it can be used with any subdomain of comptia.org2. It also has a validity period of one year, which means it needs to be rotated annually3.

NEW QUESTION 11
- (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 16
- (Exam Topic 1)
A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?

A. Dumpster diving
B. Shoulder surfing
C. Information elicitation
D. Credential harvesting

Answer: A

Explanation:

Crosscut shredders are used to destroy paper documents and reduce the risk of data leakage through dumpster diving. Dumpster diving is a method of retrieving sensitive information from paper waste by searching through discarded documents.
References:
CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2

NEW QUESTION 17
- (Exam Topic 1)
An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?

A. Data protection officer
B. Data owner
C. Backup administrator
D. Data custodian
E. Internal auditor

Answer: D

Explanation:
The responsibilities of ensuring backups are properly maintained and implementing technical controls to protect data are the responsibilities of the data custodian role. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 7: Securing Hosts and Data, Data Custodian

NEW QUESTION 22
- (Exam Topic 1)
Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

A. Hashing
B. Salting
C. Integrity
D. Digital signature

Answer: A

Explanation:
Hashing is a cryptographic function that produces a unique fixed-size output (i.e., hash value) from an input (i.e., data). The hash value is a digital fingerprint of the data, which means that if the data changes, so too does the hash value. By comparing the hash value of the downloaded file with the hash value provided by the security website, the security analyst can verify that the file has not been altered in transit or corrupted.

NEW QUESTION 24
- (Exam Topic 1)
A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promoting to production?

A. Disable unneeded services.
B. Install the latest security patches.
C. Run a vulnerability scan.
D. Encrypt all disks.

Answer: C

Explanation:
Running a vulnerability scan is the final step to be performed prior to promoting a system to production. This allows any remaining security issues to be identified and resolved before the system is put into production. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3

NEW QUESTION 27
- (Exam Topic 1)
When planning to build a virtual environment, an administrator need to achieve the following,
•Establish polices in Limit who can create new VMs
•Allocate resources according to actual utilization‘
•Require justication for requests outside of the standard requirements.
•Create standardized categories based on size and resource requirements Which of the following is the administrator MOST likely trying to do?

A. Implement IaaS replication
B. Product against VM escape
C. Deploy a PaaS
D. Avoid VM sprawl

Answer: D

Explanation:
The administrator is most likely trying to avoid VM sprawl, which occurs when too many VMs are created and managed poorly, leading to resource waste and increased security risks. The listed actions can help establish policies, resource allocation, and categorization to prevent unnecessary VM creation and ensure proper management. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 3.6 Given a scenario, implement the appropriate virtualization components.

NEW QUESTION 31
- (Exam Topic 1)

A company recently experienced a major breach. An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor, who is not held to the same security contral standards. Which of the following is the MOST likely source of the breach?

A. Side channel
B. Supply chain
C. Cryptographic downgrade
D. Malware

Answer: B

Explanation:
A supply chain attack occurs when a third-party supplier or business partner is compromised, leading to an attacker gaining unauthorized access to the targeted organization's network. In this scenario, the dedicated business partner connection to a vendor was used to exfiltrate customer credit card data, indicating that the vendor's network was breached and used as a supply chain attack vector.

NEW QUESTION 36
- (Exam Topic 1)
Which of the following environments can be stood up in a short period of time, utilizes either dummy data or actual data, and is used to demonstrate and model system capabilities and functionality for a fixed,
agreed-upon duration of time?

A. PoC
B. Production
C. Test
D. Development

Answer: A

Explanation:
A proof of concept (PoC) environment can be stood up quickly and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon duration of time. This environment can utilize either dummy data or actual data. References: CompTIA Security+ Certification Guide, Exam SY0-501

NEW QUESTION 41
- (Exam Topic 1)
Which of the following environment utilizes dummy data and is MOST to be installed locally on a system that allows to be assessed directly and modified easily wit each build?

A. Production
B. Test
C. Staging
D. Development

Answer: D

Explanation:
The environment that utilizes dummy data and is most likely to be installed locally on a system that allows it to be assessed directly and modified easily with each build is the development environment. The development environment is used for developing and testing software and applications. It is typically installed on a local system, rather than on a remote server, to allow for easy access and modification. Dummy data can be used in the development environment to simulate real-world scenarios and test the software's functionality. References: https://www.techopedia.com/definition/27561/development-environment

NEW QUESTION 43
- (Exam Topic 1)
A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

A. A new firewall rule is needed to access the application.
B. The system was quarantined for missing software updates.
C. The software was not added to the application whitelist.
D. The system was isolated from the network due to infected software

Answer: C

Explanation:
The most likely cause of the document-scanning software program not responding when launched by the end user is that the software was not added to the application whitelist. An application whitelist is a list of approved software applications that are allowed to run on a system. If the software is not on the whitelist, it may be blocked from running by the system's security policies. Adding the software to the whitelist should resolve the issue and allow the program to run. References: https://www.techopedia.com/definition/31541/application-whitelisting

NEW QUESTION 44
- (Exam Topic 1)
A company was compromised, and a security analyst discovered the attacker was able to get access to a service account. The following logs were discovered during the investigation:

```
User account 'JHDoe' does not exist...
User account 'VMAdmin' does not exist...
User account 'tomcat' wrong password...
User account 'Admin' does not exist...
```

Which of the following MOST likely would have prevented the attacker from learning the service account name?

A. Race condition testing
B. Proper error handling
C. Forward web server logs to a SIEM
D. Input sanitization

Answer: D

Explanation:
Input sanitization can help prevent attackers from learning the service account name by removing potentially harmful characters from user input, reducing the likelihood of successful injection attacks. References:
- CompTIA Security+ Certification Exam Objectives 2.2: Given a scenario, implement secure coding techniques.
- CompTIA Security+ Study Guide, Sixth Edition, pages 72-73

NEW QUESTION 46
- (Exam Topic 1)
Which of the following controls would be the MOST cost-effective and time-efficient to deter intrusions at the perimeter of a restricted, remote military training area? (Select TWO).

A. Barricades
B. Thermal sensors
C. Drones
D. Signage
E. Motion sensors
F. Guards
G. Bollards

Answer: AD

Explanation:
Barricades and signage are the most cost-effective and time-efficient controls to deter intrusions at the perimeter of a restricted, remote military training area. References:
- CompTIA Security+ Study Guide Exam SY0-601, Chapter 7

NEW QUESTION 47
- (Exam Topic 1)
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Answer: DE

Explanation:
The most likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases are included third-party libraries and vendors/supply chain. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 8: Application, Data, and Host Security, Supply Chain and Software Development Life Cycle

NEW QUESTION 48
- (Exam Topic 1)
Which of the following is required in order for 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:
an IDS (Intrusion Detection System) and a WAF (Web Application Firewall) are both used to monitor and protect web applications from common attacks such as cross-site scripting and SQL injection12. However, these attacks can also be hidden in encrypted HTTPS traffic, which uses the TLS (Transport Layer Security) protocol to provide cryptography and authentication between two communicating applications34. Therefore, in order for an IDS and a WAF to be effective on HTTPS traffic, they need to be able to decrypt and inspect the data that flows in the TLS tunnel. This is achieved by using a feature called TLS inspectio3n45, which creates two dedicated TLS connections: one with the web server and another with the client. The firewall then uses a customer-provided CA (Certificate Authority) certificate to generate an on-the-fly certificate that replaces the web server certificate and shares it with the client. This way, the firewall can see the

content of the HTTPS traffic and apply the IDS and WAF rules accordingly34.

NEW QUESTION 52
- (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 57
- (Exam Topic 1)
During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the nsk of lateral spread and the risk that the adversary would notice any changes?

A. Physically move the PC to a separate Internet point of presence.
B. Create and apply microsegmentation rules,
C. Emulate the malware in a heavily monitored DMZ segment
D. Apply network blacklisting rules for the adversary domain

Answer: C

Explanation:
Emulating the malware in a heavily monitored DMZ segment is the best option for observing network-based transactions between a callback domain and the malware running on an enterprise PC. This approach provides an isolated environment for the malware to run, reducing the risk of lateral spread and detection by the adversary. Additionally, the DMZ can be monitored closely to gather intelligence on the adversary's tactics and techniques. References: CompTIA Security+ Study Guide, page 129

NEW QUESTION 62
- (Exam Topic 1)
Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?

A. RTO
B. MTBF
C. MTTR
D. RPO

Answer: C

Explanation:
Mean Time To Repair (MTTR) is a maintenance metric that measures the average time required to troubleshoot and restore failed equipment. References: CompTIA Security+ Certification Exam Objectives 4.6 Explain the importance of secure coding practices. Study Guide: Chapter 7, page 323.

NEW QUESTION 65
- (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 69
- (Exam Topic 1)
A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?

A. Implement input validations
B. Deploy MFA
C. Utilize a WAF
D. Configure HIPS

Answer: A

Explanation:
Implementing input validations will prevent code injection attacks by verifying the type and format of user input. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 8

NEW QUESTION 74
- (Exam Topic 1)
Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

A. Whaling
B. Spam
C. Invoice scam
D. Pharming

Answer: A

Explanation:
A social engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested is known as whaling. Whaling is a type of phishing attack that targets high-profile individuals, such as executives, to steal sensitive information or gain access to their accounts.

NEW QUESTION 78
- (Exam Topic 1)
A business is looking for a cloud service provider that offers a la carte services, including cloud backups, VM elasticity, and secure networking. Which of the following cloud service provider types should business engage?

A. A laaS
B. PaaS
C. XaaS
D. SaaS

Answer: A

Explanation:
Infrastructure as a Service (IaaS) providers offer a la carte services, including cloud backups, VM elasticity, and secure networking. With IaaS, businesses can rent infrastructure components such as virtual machines, storage, and networking from a cloud service provider. References: CompTIA Security+ Study Guide, pages 233-234

NEW QUESTION 79
- (Exam Topic 1)
A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned tf servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

A. 135
B. 139
C. 143
D. 161
E. 443
F. 445

Answer: BF

Explanation:
To protect the servers in the company’s DMZ from external attack due to the new vulnerability in the SMB
protocol on the Windows systems, the security administrator should block TCP ports 139 and 445 for all external inbound connections to the DMZ.
SMB uses TCP port 139 and 445. Blocking these ports will prevent external attackers from exploiting the vulnerability in SMB protocol on Windows systems.
Blocking TCP ports 139 and 445 for all external inbound connections to the DMZ can help protect the servers, as these ports are used by SMB protocol. Port 135 is also associated with SMB, but it is not commonly used. Ports 143 and 161 are associated with other protocols and services. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 1.4 Compare and contrast network architecture and technologies.

NEW QUESTION 83
- (Exam Topic 1)
The Chief Information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside company. Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from a home office. Which of the following should the CISO choose?

A. CASB
B. Next-generation SWG
C. NGFW
D. Web-application firewall

Answer: B

Explanation:

The solution that the CISO should choose is Next-generation Secure Web Gateway (SWG), which provides URL filtering and categorization to prevent users from accessing malicious sites, even when they are away from the office. NGFWs are typically cloud-based and offer multiple security layers, including malware detection, intrusion prevention, and data loss prevention. References:
- CompTIA Security+ Study Guide Exam SY0-601, Chapter 4

NEW QUESTION 85
- (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 88
- (Exam Topic 1)
The compliance team requires an annual recertification of privileged and non-privileged user access. However, multiple users who left the company six months ago still have access. Which of the following would have prevented this compliance violation?

A. Account audits
B. AUP
C. Password reuse
D. SSO

Answer: A

Explanation:
Account audits are periodic reviews of user accounts to ensure that they are being used appropriately and that access is being granted and revoked in accordance with the organization's policies and procedures. If the compliance team had been conducting regular account audits, they would have identified the users who left the company six months ago and ensured that their access was revoked in a timely manner. This would have prevented the compliance violation caused by these users still having access to the company's systems.
To prevent this compliance violation, the company should implement account audits. An account audit is a regular review of all user accounts to ensure that they are being used properly and that they are in compliance with the company's security policies. By conducting regular account audits, the company can identify inactive or unused accounts and remove access for those users. This will help to prevent compliance violations and ensure that only authorized users have access to the company's systems and data.

NEW QUESTION 89
- (Exam Topic 1)
A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords Which of the following should the network analyst enable to meet the requirement?

A. MAC address filtering
B. 802.1X
C. Captive portal
D. WPS

Answer: D

Explanation:
The network analyst should enable Wi-Fi Protected Setup (WPS) to allow users to connect to the wireless access point securely without having to remember passwords. WPS allows users to connect to a wireless network by pressing a button or entering a PIN instead of entering a password.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 4: Identity and Access Management

NEW QUESTION 93
- (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 98
- (Exam Topic 1)
A security administrator is working on a solution to protect passwords stored in a database against rainbow table attacks Which of the following should the administrator consider?

A. Hashing
B. Salting
C. Lightweight cryptography
D. Steganography

Answer: B

Explanation:
Salting is a technique that adds random data to a password before hashing it. This makes the hash output more unique and unpredictable, and prevents attackers from using precomputed tables (such as rainbow tables) to crack the password hash. Salting also reduces the risk of collisions, which occur when different passwords produce the same hash.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

NEW QUESTION 102
- (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 105
- (Exam Topic 2)
Multiple beaconing activities to a malicious domain have been observed. The malicious domain is hosting malware from various endpoints on the network. Which of the following technologies would be best to correlate the activities between the different endpoints?

A. Firewall
B. SIEM
C. IPS
D. Protocol analyzer

Answer: B

Explanation:
SIEM stands for Security Information and Event Management, which is a technology that collects, analyzes, and correlates data from multiple sources, such as firewall logs, IDS/IPS alerts, network devices, applications, and endpoints. SIEM provides real-time monitoring and alerting of security events, as well as historical analysis and reporting for compliance and forensic purposes.
A SIEM technology would be best to correlate the activities between the different endpoints that are beaconing to a malicious domain. A SIEM can detect the malicious domain by comparing it with threat intelligence feeds or known indicators of compromise (IOCs). A SIEM can also identify the endpoints that are communicating with the malicious domain by analyzing the firewall logs and other network traffic data. A SIEM can alert the security team of the potential compromise and provide them with relevant information for investigation and remediation.

NEW QUESTION 109
- (Exam Topic 2)
A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multicioud provider environment. The security architect is looking for a solution with reduced latency to allow the incorporation of the organization's existing keys and to maintain consistent, centralized control and management regardless of the data location. Which of the following would best meet the architect's objectives?

A. Trusted Platform Module
B. laaS
C. HSMaas
D. PaaS

Answer: C

Explanation:
HSMaas stands for Hardware Security Module as a Service, which is a cloud-based service that provides secure and scalable key management and cryptographic operations for data encryption and decryption. HSMaas allows the organization to use its own keys or generate new ones, and to control and manage them

centrally regardless of where the data is stored or processed. HSMaas also reduces the latency and complexity of managing multiple encryption keys across different cloud providers, as well as the cost and maintenance of deploying physical HSM devices.
* A. Trusted Platform Module. This is not the correct answer, because a Trusted Platform Module (TPM) is a hardware chip that provides secure storage and generation of cryptographic keys on a device, such as a laptop or a server. A TPM does not offer a cloud-based solution for key management and encryption across multiple cloud providers.
* B. laaS. This is not the correct answer, because laaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources, such as servers, storage, and networks, over the internet. laaS does not provide a specific solution for key management and encryption across multiple cloud providers.
* C. HSMaas. This is the correct answer, because HSMaas stands for Hardware Security Module as a Service, which is a cloud-based service that provides secure and scalable key management and cryptographic operations for data encryption and decryption across multiple cloud providers.
* D. PaaS. This is not the correct answer, because PaaS stands for Platform as a Service, which is a cloud computing model that provides a platform for developing and deploying applications over the internet. PaaS does not provide a specific solution for key management and encryption across multiple cloud providers.
Reference: HSM as a Service (HSMaaS) | Encryption Consulting, What Is Hardware Security Module (HSM
| Thales.

NEW QUESTION 110
- (Exam Topic 2)
The application development teams have been asked to answer the following questions:
- Does this application receive patches from an external source?
- Does this application contain open-source code?
- Is this application accessible by external users?
- Does this application meet the corporate password standard? Which of the following are these questions part of?

A. Risk control self-assessment
B. Risk management strategy
C. Risk acceptance
D. Risk matrix

Answer: A

Explanation:
A risk control self-assessment (RCSA) is a process that allows an organization to identify, evaluate, and mitigate the risks associated with its activities, processes, systems, and products. A RCSA involves asking relevant questions to assess the effectiveness of existing controls and identify any gaps or weaknesses that need improvement. A RCSA also helps to align the risk appetite and tolerance of the organization with its strategic objectives and performance.
The application development teams have been asked to answer questions related to their applications' security posture, such as whether they receive patches from an external source, contain open-source code, are accessible by external users, or meet the corporate password standard. These questions are part of a RCSA process that aims to evaluate the potential risks and vulnerabilities associated with each application and determine how well they are managed and mitigated.

NEW QUESTION 112
- (Exam Topic 2)
An analyst is working on an email security incident in which the target opened an attachment containing a worm. The analyst wants to Implement mitigation techniques to prevent further spread. Which of the
following is the best course of action for the analyst to take?

A. Apply a DLP solution.
B. Implement network segmentation.
C. Utilize email content filtering.
D. Isolate the infected attachment.

Answer: D

Explanation:
Isolating the infected attachment is the best course of action for the analyst to take to prevent further spread of the worm. A worm is a type of malware that can self-replicate and infect other devices without human interaction. By isolating the infected attachment, the analyst can prevent the worm from spreading to other devices or networks via email, file-sharing, or other means. Isolating the infected attachment can also help the analyst to analyze the worm and determine its source, behavior, and impact. References:
- https://www.security.org/antivirus/computer-worm/
- https://sec.cloudapps.cisco.com/security/center/resources/worm_mitigation_whitepaper.html

NEW QUESTION 116
- (Exam Topic 2)
A security administrator performs weekly vulnerability scans on all cloud assets and provides a detailed report. Which of the following describes the administrator's activities?

A. Continuous deployment
B. Continuous integration
C. Continuous validation
D. Continuous monitoring

Answer: C

Explanation:
Continuous validation is a process that involves performing regular and automated tests to verify the security and functionality of a system or an application. Continuous validation can help identify and remediate vulnerabilities, bugs, or misconfigurations before they cause any damage or disruption. The security administrator's activities of performing weekly vulnerability scans on all cloud assets and providing a detailed report are examples of continuous validation.

NEW QUESTION 120
- (Exam Topic 2)
A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the follow r 3 best describes these systems?

A. DNS sinkholes
B. Honey pots
C. Virtual machines
D. Neural networks

Answer: B

Explanation:
Honey pots are decoy systems or resources that are designed to attract and deceive threat actors and to learn more about their motives, techniques, etc. They can be deployed alongside production systems to create an illusion of a vulnerable target and divert attacks away from the real systems. They can also collect valuable information and evidence about the attackers and their activities for further analysis or prosecution.

NEW QUESTION 121
- (Exam Topic 2)
Which of the following would be used to find the most common web-applicalion vulnerabilities?

A. OWASP
B. MITRE ATT&CK
C. Cyber Kill Chain
D. SDLC

Answer: A

Explanation:
OWASP (Open Web Application Security Project) is a non-profit organization that provides resources and guidance for improving the security of web applications. It publishes a list of the most common web application vulnerabilities, such as injection, broken authentication, cross-site scripting, etc., and provides recommendations and best practices for preventing and mitigating them

NEW QUESTION 123
- (Exam Topic 2)
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: AC

Explanation:
MAC filtering is a method of allowing or denying access to a network based on the MAC address of the device attempting to connect. By creating a list of approved MAC addresses, the organization can prevent unauthorized devices from connecting to the network.
Network Access Control (NAC) is a security solution that allows organizations to restrict access to their networks based on the device's identity, configuration, and security posture. This can be used to ensure that only legitimate devices are allowed to connect to the network, and any unauthorized devices are blocked.

NEW QUESTION 125
- (Exam Topic 2)
An organization wants to quickly assess how effectively the IT team hardened new laptops Which of the following would be the best solution to perform this assessment?

A. Install a SIEM tool and properly configure it to read the OS configuration files.
B. Load current baselines into the existing vulnerability scanner.
C. Maintain a risk register with each security control marked as compliant or non-compliant.
D. Manually review the secure configuration guide checklists.

Answer: B

Explanation:
A vulnerability scanner is a tool that can scan devices and systems for known vulnerabilities, misconfigurations, and compliance issues. By loading the current baselines into the scanner, the organization can compare the actual state of the new laptops with the desired state and identify any deviations or weaknesses. This is a quick and automated way to assess the hardening of the new laptops.

NEW QUESTION 126
- (Exam Topic 2)
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 128
- (Exam Topic 2)
A security analyst is investigating network issues between a workstation and a company server. The workstation and server occasionally experience service disruptions, and employees are forced to
reconnect to the server. In addition, some reports indicate sensitive information is being leaked from the server to the public.
The workstation IP address is 192.168.1.103, and the server IP address is 192.168.1.101. The analyst runs arp -a On a separate workstation and obtains the following results:

```
Internet address  Physical address  Type
192.168.1.101     27-4b-17-00-38-08 dynamic
192.168.1.102     8e-45-49-ac-67-b6 dynamic
192.168.1.103     27-4b-17-00-38-08 dynamic
192.168.1.105     1f-35-91-55-0f-39 dynamic
192.168.1.157     27-4b-17-00-38-08 dynamic
192.168.1.190     12-d6-cf-91-f6-3f dynamic
```

Which of the following is most likely occurring?

A. Evil twin attack
B. Domain hijacking attack
C. On-path attack
D. MAC flooding attack

Answer: C

Explanation:
An on-path attack is a type of attack where an attacker places themselves between two devices (such as a workstation and a server) and intercepts or modifies the communications between them. An on-path attacker can collect sensitive information, impersonate either device, or disrupt the service. In this scenario, the attacker is likely using an on-path attack to capture and alter the network traffic between the workstation and the server, causing service disruptions and data leakage.

NEW QUESTION 130
- (Exam Topic 2)
A security team is conducting a security review of a hosted data provider. The management team has asked the hosted data provider to share proof that customer data is being appropriately protected.
Which of the following would provide the best proof that customer data is being protected?

A. SOC2
B. CSA
C. CSF
D. 1SO 31000

Answer: A

Explanation:
SOC2 is a type of audit report that provides assurance on the security, availability, processing integrity, confidentiality, and privacy of a service organization's systems. It is based on the Trust Services Criteria developed by the American Institute of Certified Public Accountants (AICPA). A SOC2 report can provide proof that customer data is being appropriately protected by the hosted data provider1
https://www.csagroup.org/store/product/50072454/ 3: https://www.csagroup.org/store/product/50072454os/ 1: https://cloudsecurityalliance.org/blog/2021/08/20/star-testimonial-csa-star-soc2-from-readiness-to-attestation/

NEW QUESTION 132
- (Exam Topic 2)
An organization routes all of its traffic through a VPN Most users are remote and connect into a corporate data center that houses confidential information There is a firewall at the internet border, followed by a DLP appliance, the VPN server and the data center itself Which of the following is the weakest design element?

A. The DLP appliance should be integrated into a NGFW.
B. Split-tunnel connections can negatively impact the DLP appliance's performance.
C. Encrypted VPN traffic will not be inspected when entering or leaving the network.
D. Adding two hops in the VPN tunnel may slow down remote connections

Answer: C

Explanation:
VPN (Virtual Private Network) traffic is encrypted to protect its confidentiality and integrity over the internet. However, this also means that it cannot be inspected by security devices or tools when entering or leaving the network, unless it is decrypted first. This can create a blind spot or a vulnerability for the network security posture, as malicious traffic or data could bypass detection or prevention mechanisms by using VPN encryption

NEW QUESTION 137
- (Exam Topic 2)
A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

A. A worm is propagating across the network.
B. Data is being exfiltrated.
C. A logic bomb is deleting data.
D. Ransomware is encrypting files.

Answer: B

Explanation:
Data is being exfiltrated when an internal system is sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Data exfiltration is the unauthorized transfer of data from a system or network to an external destination or actor. Data exfiltration can be performed by malicious insiders or external attackers who have compromised the system or network. DNS queries are requests for resolving domain names to IP addresses. DNS queries can be used as a covert channel for data exfiltration by encoding data in the domain names or subdomains and sending them to a malicious DNS server that can decode and collect the data. References:
https://www.comptia.org/blog/what-is-data-exfiltration
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 142
- (Exam Topic 2)
A security team is providing input on the design of a secondary data center that has Which of the following should the security team recommend? (Select two).

A. Coniguring replication of the web servers at the primary site to offline storage
B. Constructing the secondary site in a geographically disperse location
C. Deploying load balancers at the primary site
D. Installing generators
E. Using differential backups at the secondary site
F. Implementing hot and cold aisles at the secondary site

Answer: BD

Explanation:
* B. Constructing the secondary site in a geographically disperse location would ensure that a natural disaster at the primary site would not affect the secondary site. It would also allow for failover during traffic surge situations by distributing the load across different regions. D. Installing generators would provide protection against power surges and outages by providing backup power sources in case of a failure. Generators are part of the physical security requirements for data centers as they ensure availability and resilience. References: 1
CompTIA Security+ Certification Exam Objectives, page 8, Domain 2.0: Architecture and Design, Objective 2.1 : Explain the importance of secure staging deployment concepts 2
CompTIA Security+ Certification Exam
Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application
development, deployment, and automation concepts 3
CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls

NEW QUESTION 145
- (Exam Topic 2)
An analyst is working on an investigation with multiple alerts for multiple hosts. The hosts are showing signs of being compromised by a fast-spreading worm. Which of the following should be the next step in order to stop the spread?

A. Disconnect every host from the network.
B. Run an AV scan on the entire
C. Scan the hosts that show signs of
D. Place all known-infected hosts on an isolated network

Answer: D

Explanation:
Placing all known-infected hosts on an isolated network is the best way to stop the spread of a worm infection. This will prevent the worm from reaching other hosts on the network and allow the infected hosts to be cleaned and restored. Disconnecting every host from the network is not practical and may disrupt business operations. Running an AV scan on the entire network or scanning the hosts that show signs of infection may not be effective or fast enough to stop a fast-spreading worm.

NEW QUESTION 146
- (Exam Topic 2)
The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be best to mitigate the CEO's concerns? (Select two).

A. Geolocation
B. Time-of-day restrictions

C. Certificates
D. Tokens
E. Geotagging
F. Role-based access controls

Answer: AB

Explanation:
Geolocation and time-of-day restrictions would be best to mitigate the CEO's concerns about staff members working from high-risk countries while on holiday or outsourcing work to a third-party organization in another country. Geolocation is a technique that involves determining the physical location of a device or user based on its IP address, GPS coordinates, Wi-Fi signals, or other indicators. Time-of-day restrictions are policies that limit the access or usage of resources based on the time of day or week. Geolocation and time-of-day restrictions can help to enforce access control rules, prevent unauthorized access, detect anomalous behavior, and comply with regulations. References: https://www.comptia.org/blog/what-is-geolocation https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 148
- (Exam Topic 2)
A security analyst is creating baselines for the server team to follow when hardening new devices for deployment. Which of the following best describes what the analyst is creating?

A. Change management procedure
B. Information security policy
C. Cybersecurity framework
D. Secure configuration guide

Answer: D

Explanation:
A secure configuration guide is a document that provides an overview of the security features and best practices for a specific product, system, or application. A secure configuration guide helps to reduce unnecessary cyber vulnerabilities and enhance overall security by applying consistent and standardized settings and policies. A security analyst can create baselines for the server team to follow when hardening new devices for deployment based on a secure configuration guide.
* A. Change management procedure. This is not the correct answer, because a change management procedure is a document that describes the steps and processes for implementing, reviewing, and approving changes to an IT system or environment. A change management procedure helps to minimize the risks and impacts of changes on the system performance, availability, and security.
* B. Information security policy. This is not the correct answer, because an information security policy is a document that defines the rules and principles for protecting the confidentiality, integrity, and availability of information assets within an organization. An information security policy helps to establish the roles and responsibilities of employees, managers, and stakeholders regarding information security.
* C. Cybersecurity framework. This is not the correct answer, because a cybersecurity framework is a document that provides a set of standards, guidelines, and best practices for managing cybersecurity risks and improving resilience. A cybersecurity framework helps to align the business objectives and priorities with the security requirements and capabilities.
* D. Secure configuration guide. This is the correct answer, because a secure configuration guide is a document that provides an overview of the security features and best practices for a specific product, system, or application. A secure configuration guide helps to reduce unnecessary cyber vulnerabilities and enhance overall security by applying consistent and standardized settings and policies.
Reference: Secure Configuration Guide, Security Technical Implementation Guide - Wikipedia.

NEW QUESTION 152
- (Exam Topic 2)
A company wants to deploy PKI on its internet-facing website The applications that are currently deployed are
• www company.com (mam website)
• contact us company com (for locating a nearby location)
• quotes company.com (for requesting a price quote)
The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store company com Which of the following certificate types would best meet the requirements?

A. SAN
B. Wildcard
C. Extended validation
D. Self-signed

Answer: B

Explanation:
A wildcard certificate is a type of SSL certificate that can secure multiple subdomains under one domain name by using an asterisk (*) as a placeholder for any subdomain name. For example, *.company.com can secure www.company.com, contactus.company.com, quotes.company.com, etc. It can work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com.

NEW QUESTION 155
- (Exam Topic 2)
Security analysts notice a server login from a user who has been on vacation for two weeks, The an-alysts confirm that the user did not log in to the system while on vacation After reviewing packet capture the analysts notice the following:
Which of the following occurred?

A. A buffer overflow was exploited to gain unauthorized access.
B. The user's account was con-promised, and an attacker changed the login credentials.
C. An attacker used a pass-the-hash attack to gain access.
D. An insider threat with username logged in to the account.

Answer: C

Explanation:
A pass-the-hash attack is a type of replay attack that captures and uses the hash of a password. The attacker then attempts to log on as the user with the stolen hash. This type of attack is possible be-cause some authentication protocols send hashes over the network instead of plain text passwords. The packet capture shows that the attacker used NTLM authentication, which is vulnerable to pass-the-hash attacks

NEW QUESTION 156
- (Exam Topic 2)
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing	Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPSDatabase server Worm Change the default application passwordExecutive KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification
A screenshot of a computer program Description automatically generated with low confidence

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

NEW QUESTION 157
- (Exam Topic 2)
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 158
- (Exam Topic 2)
A malicious actor recently penetrated a company's network and moved laterally to the data center Upon investigation a forensics firm wants to know what was in the memory on the compromised server Which of the following files should be given to the forensics firm?

A. Security
B. Application
C. Dump
D. Syslog

Answer: C

Explanation:
A dump file is a file that contains the contents of memory at a specific point in time. It can be used for debugging or forensic analysis of a system or an application. It can reveal what was in the memory on the compromised server, such as processes, variables, passwords, encryption keys, etc.

NEW QUESTION 161
- (Exam Topic 2)
A company recently suffered a breach in which an attacker was able to access the internal mail servers and directly access several user inboxes. A large number of email messages were later posted online. Which of the following would bast prevent email contents from being released should another breach occur?

A. Implement S/MIME to encrypt the emails at rest.
B. Enable full disk encryption on the mail servers.
C. Use digital certificates when accessing email via the web.
D. Configure web traffic to only use TLS-enabled channels.

Answer: A

Explanation:

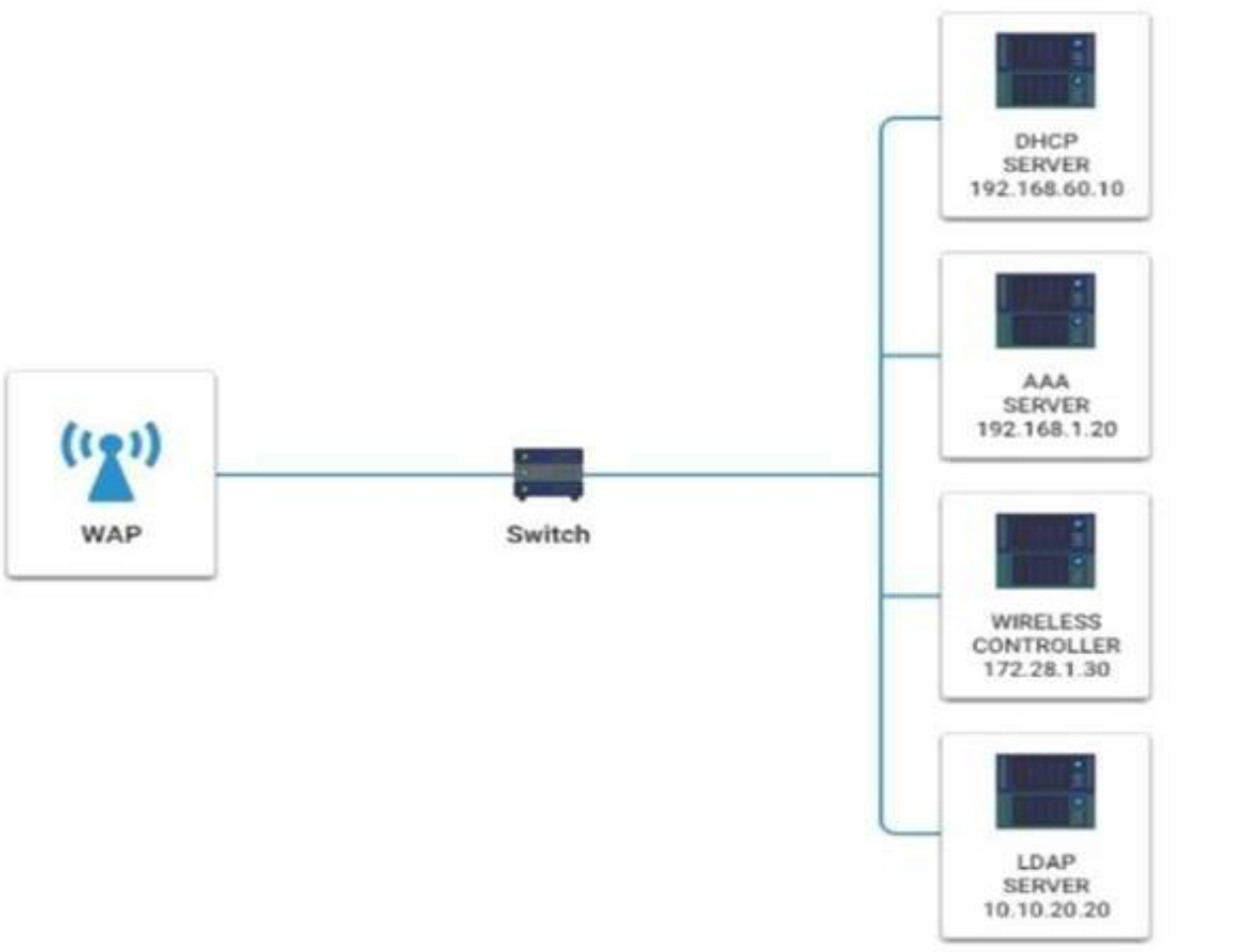
S/MIME stands for Secure/Multipurpose Internet Mail Extensions, which is a standard for encrypting and digitally signing email messages. S/MIME can provide confidentiality, integrity, authentication and
non-repudiation for email communications. S/MIME can encrypt the emails at rest, which means that the
email contents are protected even if they are stored on the mail servers or the user inboxes. S/MIME can prevent email contents from being released should another breach occur, as the attacker would not be able to decrypt or read the encrypted emails without the proper keys or certificates. Verified References:

- Cryptography Concepts – SY0-601 CompTIA Security+ : 2.8 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/cryptography-concepts-2/ (See
S/MIME)
- Mail Encryption - CompTIA Security+ All-in-One Exam Guide (Exam SY0-301) https://www.oreilly.com/library/view/comptia-security-all-in-one/9780071771474/sec5_chap14.html (See S/MIME)
- Symmetric and Asymmetric Encryption – CompTIA Security+ SY0-501 – 6.1 https://www.professormesser.com/security-plus/sy0-501/symmetric-and-asymmetric-encryption/ (See S/MIME)

NEW QUESTION 164
- (Exam Topic 2)
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 167
- (Exam Topic 2)
Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

A. A full inventory of all hardware and software
B. Documentation of system classifications
C. A list of system owners and their departments
D. Third-party risk assessment documentation

Answer: A

Explanation:
A full inventory of all hardware and software would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed, as it would allow the analyst to identify which systems and applications are affected by the vulnerability and prioritize the remediation efforts accordingly. A full inventory would also help the analyst to determine the impact and likelihood of a successful exploit, as well as the potential loss of confidentiality, integrity and availability of the data and services. References:
- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/risk-analysis/
- https://www.comptia.org/landing/securityplus/index.html
- https://www.comptia.org/blog/complete-guide-to-risk-management

NEW QUESTION 171
- (Exam Topic 2)
Developers are writing code and merging it into shared repositories several times a day. where it is tested automatically. Which of the following concepts does this best represent?

A. Functional testing
B. Stored procedures
C. Elasticity
D. Continuous Integration

Answer: D

Explanation:
Continuous Integration is the concept that best represents developers writing code and merging it into shared repositories several times a day, where it is tested automatically. Continuous Integration is a software development practice that involves integrating code changes from multiple developers into a shared repository frequently and running automated tests to ensure quality and functionality. Continuous Integration can help to detect and fix errors early, improve collaboration, reduce rework, and accelerate delivery. References: https://www.comptia.org/blog/what-is-devops
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 176
- (Exam Topic 2)
A network engineer receives a call regarding multiple LAN-connected devices that are on the same switch. The devices have suddenly been experiencing speed and latency issues while connecting to network resources. The engineer enters the command show mac address-table and reviews the following output

VLAN	MAC	PORT
1	00-04-18-EB-14-30	Fa0/1
1	88-CD-34-19-E8-98	Fa0/2
1	40-11-08-87-10-13	Fa0/3
1	00-04-18-EB-14-30	Fa0/4
1	88-CD-34-00-15-F3	Fa0/5
1	FA-13-02-04-27-64	Fa0/6

Which of the following best describes the attack that is currently in progress?

A. MAC flooding
B. Evil twin
C. ARP poisoning
D. DHCP spoofing

Answer: C

Explanation:
This is an attempt to redirect traffic to an attacking host by sending an ARP packet that contains the forged address of the next hop router. The attacker tricks the victim into believing that it is the legitimate router by sending a spoofed ARP reply with its own MAC address. This causes the victim to send all its traffic to the attacker instead of the router. The attacker can then intercept, modify, or drop the packets as they please.

NEW QUESTION 181
- (Exam Topic 2)
A user downloaded an extension for a browser, and the user's device later became infected. The analyst who Is Investigating the Incident saw various logs where the attacker was hiding activity by deleting data. The following was observed running:
New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter C| Format-Volume -Driveletter C - FileSystemLabel "New"-FileSystem NTFS - Full -Force -Confirm:$false

Which of the following is the malware using to execute the attack?

A. PowerShell
B. Python
C. Bash
D. Macros

Answer: A

Explanation:
PowerShell is a scripting language and command-line shell that can be used to automate tasks and manage systems. PowerShell can also be used by malware to execute malicious commands and evade detection. The code snippet in the question is a PowerShell command that creates a new partition on disk 2, formats it with NTFS file system, and assigns it a drive letter C. This could be part of an attack that wipes out the original data on the disk or creates a hidden partition for storing malware or stolen data. References:
- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/scripting-and-automation/
- https://learn.microsoft.com/en-us/powershell/module/storage/new-partition?view=windowsserver2022-ps

NEW QUESTION 186
- (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 188
- (Exam Topic 2)
A company is auditing the manner in which its European customers' personal information is handled. Which of the following should the company consult?

A. GDPR
B. ISO
C. NIST
D. PCI DSS

Answer: A

Explanation:
GDPR stands for General Data Protection Regulation, which is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). GDPR also applies to organizations outside the EU that offer goods or services to, or monitor the behavior of, EU data subjects. GDPR aims to protect the privacy and rights of EU citizens and residents regarding their personal data. GDPR defines personal data as any information relating to an identified or identifiable natural person, such as name, identification number, location data, online identifiers, or any factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. A company that is auditing the manner in which its European customers' personal information is handled should consult GDPR to ensure compliance with its rules and obligations. References:
- https://www.gdpreu.org/the-regulation/key-concepts/personal-data/
- https://ico.org.uk/for-organisations-2/guide-to-data-protection/guide-to-the-general-data-protection-regula

NEW QUESTION 190
- (Exam Topic 2)
The application development team is in the final stages of developing a new healthcare application. The team has requested copies of current PHI records to perform the final testing.
Which of the following would be the best way to safeguard this information without impeding the testing process?

A. Implementing a content filter
B. Anonymizing the data
C. Deploying DLP tools
D. Installing a FIM on the application server

Answer: B

Explanation:
Anonymizing the data is the process of removing personally identifiable information (PII) from data sets, so that the people whom the data describe remain anonymous12. Anonymizing the data can safeguard the PHI records without impeding the testing process, because it can protect the privacy of the patients while preserving the data integrity and statistical accuracy for the application development team12. Anonymizing the data can be done by using techniques such as data masking, pseudonymization, generalization, data swapping, or data perturbation12.
Implementing a content filter is not the best way to safeguard the information, because it is a technique that blocks or allows access to certain types of content based on predefined rules or policies3. A content filter does not remove or encrypt PII from data sets, and it may not prevent unauthorized access or leakage of PHI records.
Deploying DLP tools is not the best way to safeguard the information, because it is a technique that monitors and prevents data exfiltration or transfer to

unauthorized destinations or users. DLP tools do not remove or encrypt PII from data sets, and they may not be sufficient to protect PHI records from internal misuse or negligence.
Installing a FIM on the application server is not the best way to safeguard the information, because it is a technique that detects and alerts changes to files or directories on a system. FIM does not remove or encrypt PII from data sets, and it may not prevent unauthorized access or modification of PHI records.

NEW QUESTION 194
- (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 197
- (Exam Topic 2)
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 201
- (Exam Topic 2)
A security engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses. Which of the following will the engineer most likely recommended?

A. A content filter
B. AWAF
C. A next-generation firewall
D. An IDS

Answer: C

Explanation:
A next-generation firewall (NGFW) is a solution that can defend against malicious actors misusing protocols and being allowed through network defenses. A NGFW is a type of firewall that can perform deep packet inspection, application-level filtering, intrusion prevention, malware detection, and identity-based access control. A NGFW can also use threat intelligence and behavioral analysis to identify and block malicious traffic based on protocols, signatures, or anomalies.
References:
https://www.comptia.org/blog/what-is-a-next-generation-firewall
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 206
- (Exam Topic 2)
An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained Which of the following roles would MOST likely include these responsibilities?

A. Data protection officer
B. Data owner
C. Backup administrator
D. Data custodian
E. Internal auditor

Answer: C

Explanation:
The role that would most likely include the responsibilities of implementing technical controls to protect data and ensuring backups are properly maintained would be a Backup Administrator. A Backup Administrator is responsible for maintaining and managing an organization's backup systems and procedures, which includes ensuring that backups are properly configured, tested and securely stored. They are also responsible for the recovery of data in case of a disaster or data loss.

NEW QUESTION 210
- (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 212
- (Exam Topic 2)
A network engineer is troubleshooting wireless network connectivity issues that were reported by users The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return to their desks after using their devices in other areas of the building There have also been reports of users being required to enter their credentials on web pages in order to gain access to them Which of the following is the most likely cause of this issue?

A. An external access point is engaging in an evil-Twin attack
B. The signal on the WAP needs to be increased in that section of the building
C. The certificates have expired on the devices and need to be reinstalled
D. The users in that section of the building are on a VLAN that is being blocked by the firewall

Answer: A

Explanation:
An evil-Twin attack is a type of wireless network attack that involves setting up a rogue access point that mimics a legitimate one. It can trick users into connecting to the rogue access point instead of the real one, and then intercept or modify their traffic, steal their credentials, launch phishing pages, etc. It is the most likely cause of the issue that users are experiencing slow speeds, unable to connect to network drives, and required to enter their credentials on web pages when working in the section of the building that is closest to the parking lot, where an external access point could be placed nearby.

NEW QUESTION 217
- (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 219
- (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 222
- (Exam Topic 2)
A corporate security team needs to secure the wireless perimeter of its physical facilities to ensure only authorized users can access corporate resources. Which of the following should the security team do? (Refer the answer from CompTIA SY0-601 Security+ documents or guide at comptia.org)

A. Identify rogue access points.
B. Check for channel overlaps.
C. Create heat maps.
D. Implement domain hijacking.

Answer: A

Explanation:
Based on CompTIA SY0-601 Security+ guide, the answer to the question is A. Identify rogue access points. To secure the wireless perimeter of its physical facilities, the corporate security team should focus on
identifying rogue access points, which are unauthorized access points that have been set up by employees or outsiders to bypass security controls. By identifying and removing these rogue access points, the team can ensure that only authorized users can access corporate resources through the wireless network.
https://www.comptia.org/training/books/security-sy0-601-study-guide

NEW QUESTION 225
- (Exam Topic 2)
Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's Pll?

A. SCAP
B. NetFlow
C. Antivirus
D. DLP

Answer: D

Explanation:
DLP stands for Data Loss Prevention, which is a technology that can monitor, detect and prevent the unauthorized transmission of sensitive data, such as PII (Personally Identifiable Information). DLP can be implemented on endpoints, networks, servers or cloud services to protect data in motion, in use or at rest. DLP can also block or alert on data transfers that violate predefined policies or rules. DLP is the best tool to assist with detecting an employee who has accidentally emailed a file containing a customer’s PII, as it can scan the email content and attachments for any data that matches the criteria of PII and prevent the email from being sent or notify the administrator of the incident. Verified References:
- Data Loss Prevention Guide to Blocking Leaks - CompTIA https://www.comptia.org/content/guides/data-loss-prevention-a-step-by-step-guide-to-blocking-leaks
- Data Loss Prevention – SY0-601 CompTIA Security+ : 2.1 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-loss-prevention-4/
- Data Loss Prevention – CompTIA Security+ SY0-501 – 2.1 https://www.professormesser.com/security-plus/sy0-501/data-loss-prevention-3/

NEW QUESTION 228
- (Exam Topic 2)
An organization wants to ensure that proprietary information is not inadvertently exposed during facility tours. Which of the following would the organization implement to mitigate this risk?

A. Clean desk policy
B. Background checks
C. Non-disclosure agreements
D. Social media analysis

Answer: A

Explanation:
A clean desk policy is a set of rules that require employees to clear their desks of any documents, papers, or devices that contain sensitive or confidential information when they leave their workstations. This policy helps to prevent unauthorized access, theft, or disclosure of proprietary information during facility tours or other situations where outsiders may visit the premises.
* A. Clean desk policy. This is the correct answer, because a clean desk policy is a simple and effective way to mitigate the risk of exposing proprietary information during facility tours.

NEW QUESTION 230
- (Exam Topic 2)
A help desk technician receives a phone call from someone claiming to be a part of the organization's cybersecurity incident response team. The caller asks the technician to verify the network's internal firewall IP address. Which of the following is the technician's best course of action?

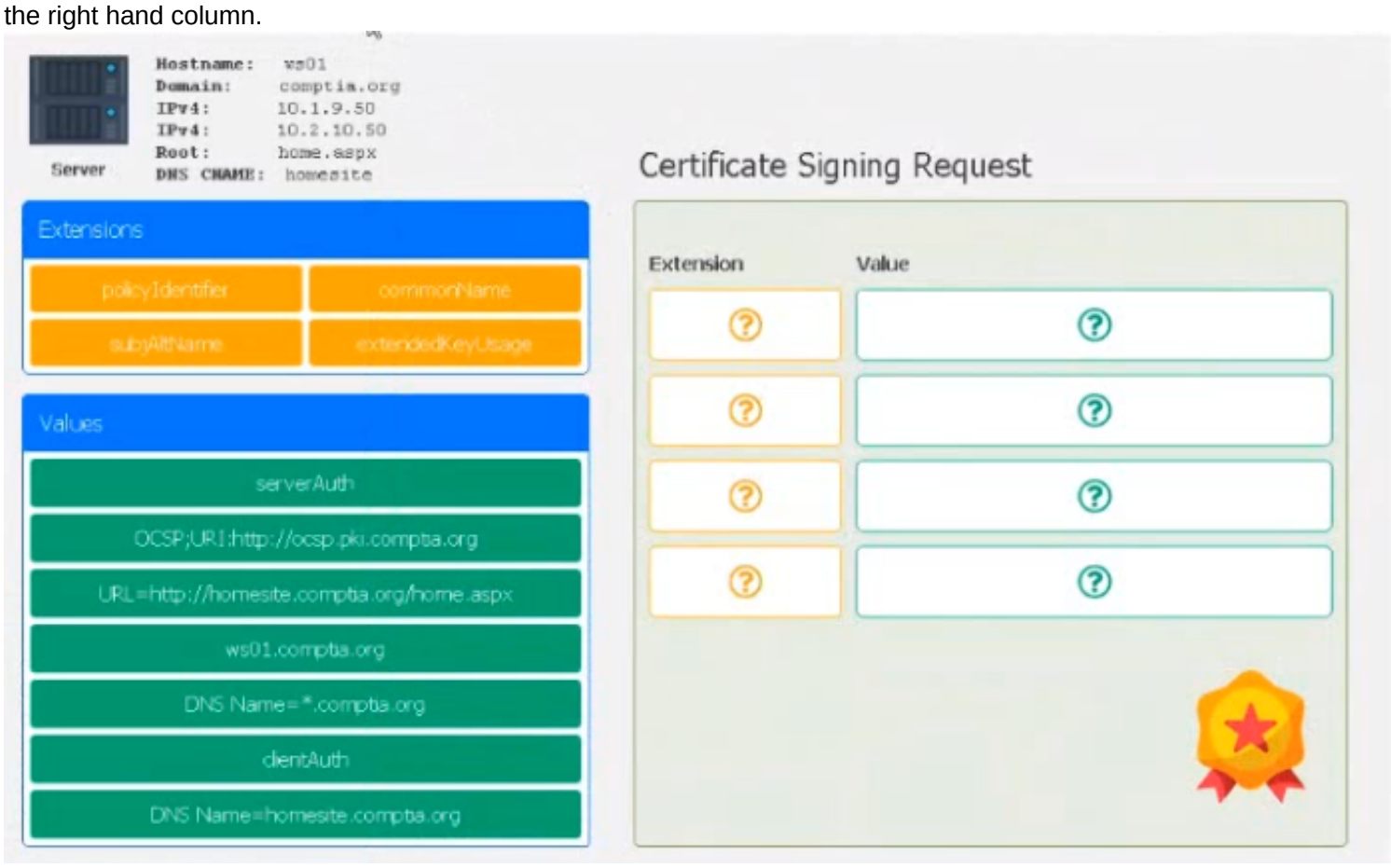
A. Direct the caller to stop by the help desk in person and hang up declining any further requests from the caller.
B. Ask for the caller's name, verify the person's identity in the email directory, and provide the requested information over the phone.
C. Write down the phone number of the caller if possible, the name of the person requesting the information, hang up, and notify the organization's cybersecurity officer.
D. Request the caller send an email for identity verification and provide the requested information via email to the caller.

Answer: C

Explanation:

This is the best course of action for the help desk technician because it can help prevent a potential social engineering attack. Social engineering is a technique that involves manipulating or deceiving people into revealing sensitive information or performing actions that compromise security. The caller may be impersonating a member of the organization's cybersecurity incident response team to obtain the network's internal firewall IP address, which could be used for further attacks. The help desk technician should not provide any information over the phone without verifying the caller's identity and authorization. The help desk technician should also report the incident to the organization's cybersecurity officer for investigation and response. References:
https://www.comptia.org/blog/social-engineering-explained
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 235
- (Exam Topic 2)
Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)
• Hostname: ws01
• Domain: comptia.org
• IPv4: 10.1.9.50
• IPV4: 10.2.10.50
• Root: home.aspx
• DNS CNAME:homesite. Instructions:
Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 236
- (Exam Topic 2)
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 238
- (Exam Topic 2)
A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage Which of the following is most likely the cause?

A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage
B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.

C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.

Answer: D

Explanation:
Mimikatz is a tool that can extract plaintext credentials from memory on Windows systems. A malicious flash drive can bypass the GPO blocking the flash drives by using techniques such as autorun.inf or HID spoofing to execute Mimikatz on the target system without user interaction or consent. This can cause AV alerts indicating Mimikatz attempted to run on the remote systems and also reduce the storage capacity of the flash drives to only 512KB by creating hidden partitions or files on them.

NEW QUESTION 240
- (Exam Topic 2)
Which of the following can best protect against an employee inadvertently installing malware on a company system?

A. Host-based firewall
B. System isolation
C. Least privilege
D. Application allow list

Answer: C

Explanation:
Least privilege is a security principle that states that users should only be granted the permissions they need to do their job. This helps to protect against malware infections by preventing users from installing unauthorized software.
A host-based firewall can help to protect against malware infections by blocking malicious traffic from reaching a computer. However, it cannot prevent a user from installing malware if they have the necessary permissions.
System isolation is the practice of isolating systems from each other to prevent malware from spreading. This can be done by using virtual machines or network segmentation. However, system isolation can be complex and expensive to implement.
An application allow list is a list of applications that are allowed to run on a computer. This can help to prevent malware infections by preventing users from running unauthorized applications. However, an application allow list can be difficult to maintain and can block legitimate applications.
Therefore, the best way to protect against an employee inadvertently installing malware on a company system is to use the principle of least privilege. This will help to ensure that users only have the permissions they need to do their job, which will reduce the risk of malware infections. Here are some additional benefits of least privilege:
- It can help to improve security by reducing the attack surface.
- It can help to simplify security management by reducing the number of permissions that need to be managed.
- It can help to improve compliance by reducing the risk of data breaches.

NEW QUESTION 241
- (Exam Topic 2)
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 243
- (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 247
- (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 249
- (Exam Topic 2)
During a recent cybersecurity audit, the auditors pointed out various types of vulnerabilities in the production area. The production area hardware runs applications that are critical to production Which of the following describes what the company should do first to lower the risk to the
Production the hardware.

A. Back up the hardware.
B. Apply patches.
C. Install an antivirus solution.
D. Add a banner page to the hardware.

Answer: B

Explanation:
Applying patches is the first step to lower the risk to the production hardware, as patches are updates that fix vulnerabilities or bugs in the software or firmware. Patches can prevent attackers from exploiting known vulnerabilities and compromising the production hardware. Applying patches should be done regularly and in a timely manner, following a patch management policy and process. 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 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of
embedded and specialized systems security 3 https://www.comptia.org/blog/patch-management-best-practices

NEW QUESTION 253
- (Exam Topic 2)
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 pcints are up and running. One of the help desk technicians notices the affected users are working in a near the parking Jot Which Of the following IS the most likely reason for the outage?

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

Answer: A

Explanation:
Wireless jamming is a way for an attacker to disrupt a wireless network and create a denial of ser-vice situation by decreasing the signal-to-noise ratio at the receiving device. The attacker would need to be relatively close to the wireless network to overwhelm the good signal. The other options are not likely to cause a wireless network outage for users near the parking lot.

NEW QUESTION 255
- (Exam Topic 2)
A security analyst is currently addressing an active cyber incident. The analyst has been able to identify affected devices that are running a malicious application with a unique hash. Which of the following is the next step according to the incident response process?

A. Recovery
B. Lessons learned
C. Containment
D. Preparation

Answer: C

Explanation:
Containment is the next step according to the incident response process after identifying affected devices that are running a malicious application with a unique hash. Containment involves isolating the compromised devices or systems from the rest of the network to prevent the spread of the attack and limit its impact. Containment can be done by disconnecting the devices from the network, blocking network traffic to or from them, or applying firewall rules or access control lists. Containment is a critical step in incident response because it helps to preserve evidence for further analysis and remediation, and reduces the risk of data loss or exfiltration
https://www.fortinet.com/resources/cyberglossary/incident-response https://www.ibm.com/topics/incident-response

NEW QUESTION 257
- (Exam Topic 2)
Which of the following should customers who are involved with Ul developer agreements be concerned with when considering the use of these products on highly

sensitive projects?

A. Weak configurations
B. Integration activities
C. Unsecure user accounts
D. Outsourced code development

Answer: A

Explanation:
Customers who are involved with Ul developer agreements should be concerned with weak configurations when considering the use of these products on highly sensitive projects. Weak configurations can lead to security vulnerabilities, which can be exploited by malicious actors. It is important to ensure that all configurations are secure and up-to-date in order to protect sensitive data. Source: UL

NEW QUESTION 259
- (Exam Topic 2)
As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

A. HTTPS://*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
C. HTTPS://*.app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
D. HTTPS://".comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2023

Answer: C

Explanation:
This certificate property will meet the requirements because it has a wildcard at the secondary subdomain level (.app1.comptia.org), which means it can be used for any subdomain under app1.comptia.org, such as test.app1.comptia.org or dev.app1.comptia.org. It also has a validity period of less than one year, which means it will need to be rotated annually. The other options do not meet the requirements because they either have a wildcard at the primary domain level (.comptia.org), which is not allowed, or they have a validity period of more than one year, which is too long.

NEW QUESTION 262
- (Exam Topic 2)
During a recent security assessment, a vulnerability was found in a common OS. The OS vendor was unaware of the issue and promised to release a patch within the next quarter. Which of the following best describes this type of vulnerability?

A. Legacy operating system
B. Weak configuration
C. Zero day
D. Supply chain

Answer: C

Explanation:
A zero-day vulnerability is a security flaw that is unknown to the vendor and the public, and therefore has no patch or fix available. A zero-day attack is an exploit that takes advantage of a zero-day vulnerability before the vendor or the security community becomes aware of it. A zero-day attack can cause serious damage to a system or network, as there is no defense against it until a patch is released. References:
- https://resources.infosecinstitute.com/certification/security-domain-1-threats-attacks-and-vulnerabilities/
- https://www.professormesser.com/security-plus/sy0-501/zero-day-attacks-4/

NEW QUESTION 264
- (Exam Topic 2)
Which of the following would provide guidelines on how to label new network devices as part of the initial configuration?

A. IP schema
B. Application baseline configuration
C. Standard naming convention policy
D. Wireless LAN and network perimeter diagram

Answer: C

Explanation:
A standard naming convention policy would provide guidelines on how to label new network devices as part of the initial configuration. A standard naming convention policy is a document that defines the rules and formats for naming network devices, such as routers, switches, firewalls, servers, or printers. A standard naming convention policy can help an organization achieve consistency, clarity, and efficiency in network management and administration.
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/td/docs/solutions/Enterprise/Network_Virtualization/PathIsolationDesignGuide/P

NEW QUESTION 267
- (Exam Topic 2)
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: C

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 272
- (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 276
- (Exam Topic 2)
A government organization is developing an advanced Al defense system. Develop-ers are using information collected from third-party providers Analysts are no-ticing inconsistencies in the expected powers Of then learning and attribute the Outcome to a recent attack on one of the suppliers. Which of the following IS the most likely reason for the inaccuracy of the system?

A. Improper algorithms security
B. Tainted training data
C. virus
D. Cryptomalware

Answer: B

Explanation:
Tainted training data is a type of data poisoning attack that involves modifying or injecting malicious data into the training dataset of a machine learning or artificial intelligence system. It can cause the system to learn incorrect or biased patterns and produce inaccurate or malicious outcomes. It is the most likely reason for the inaccuracy of the system that is using information collected from third-party providers that have been compromised by an attacker.

NEW QUESTION 280
- (Exam Topic 2)
Which of the following should be addressed first on security devices before connecting to the network?

A. Open permissions
B. Default settings
C. API integration configuration
D. Weak encryption

Answer: B

Explanation:
Before connecting security devices to the network, it is crucial to address default settings first. Manufacturers often ship devices with default settings that include default usernames, passwords, and configurations. These settings are widely known and can be easily exploited by attackers. Changing default settings helps to secure the device and prevent unauthorized access. Reference: CompTIA Security+ SY0-501 Exam Objectives, Section 3.2: "Given a scenario, implement secure systems design." (https://www.comptia.jp/pdf/Security%2B%20SY0-501%20Exam%20Objectives.pdf)

NEW QUESTION 281
- (Exam Topic 2)
Stakeholders at an organisation must be kept aware of any incidents and receive updates on status changes as they occur Which of the following Plans would fulfill this requirement?

A. Communication plan
B. Disaster recovery plan
C. Business continuity plan
D. Risk plan

Answer: A

Explanation:

A communication plan is a plan that would fulfill the requirement of keeping stakeholders at an organization aware of any incidents and receiving updates on status changes as they occur. A communication plan is a document that outlines the communication objectives, strategies, methods, channels, frequency, and audience for an incident response process. A communication plan can help an organization communicate effectively and efficiently with internal and external stakeholders during an incident and keep them informed of the incident's impact, progress, resolution, and recovery.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.ready.gov/business-continuity-plan

NEW QUESTION 283
- (Exam Topic 2)
Which of the following describes where an attacker can purchase DDoS or ransomware services?

A. Threat intelligence
B. Open-source intelligence
C. Vulnerability database
D. Dark web

Answer: D

Explanation:
The best option to describe where an attacker can purchase DDoS or ransomware services is the dark web. The dark web is an anonymous, untraceable part of the internet where a variety of illicit activities take place, including the purchase of DDoS and ransomware services. According to the CompTIA Security+ SY0-601 Official Text Book, attackers can purchase these services anonymously and without the risk of detection or attribution. Additionally, the text book recommends that organizations monitor the dark web to detect any possible threats or malicious activity.

NEW QUESTION 284
- (Exam Topic 2)
An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls' (Select two).

A. ISO
B. PCI DSS
C. SOC
D. GDPR
E. CSA
F. NIST

Answer: BD

Explanation:
PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards and requirements for organizations that store, process, or transmit payment card data. It aims to protect cardholder data and prevent fraud and data breaches. GDPR (General Data Protection Regulation) is a regulation that governs the collection, processing, and transfer of personal data of individuals in the European Union. It aims to protect the privacy and rights of data subjects and impose obligations and penalties on data controllers and
processors. These are the frameworks that the security officer should map the existing controls to, as they are relevant for a credit card transaction company that has a new office in Europe

NEW QUESTION 289
- (Exam Topic 2)
A company wants to build a new website to sell products online. The website wd I host a storefront application that allow visitors to add products to a shopping cart and pay for products using a credit card. which Of the following protocols •would be most secure to implement?

A. SSL
B. SFTP
C. SNMP
D. TLS

Answer: D

Explanation:
TLS (Transport Layer Security) is a cryptographic protocol that provides secure communication over the internet. It can protect the data transmitted between the website and the visitors from eavesdropping, tampering, etc. It is the most secure protocol to implement for a website that sells products online using a credit card.

NEW QUESTION 291
- (Exam Topic 2)
An organization recently completed a security control assessment The organization determined some controls did not meet the existing security measures. Additional mitigations are needed to lessen the risk of the non-complaint controls. Which of the following best describes these mitigations?

A. Corrective
B. Compensating
C. Deterrent
D. Technical

Answer: B

Explanation:
Compensating controls are additional security measures that are implemented to reduce the risk of
non-compliant controls. They do not fix the underlying issue, but they provide an alternative way of achieving the same security objective. For example, if a system does not have encryption, a compensating control could be to restrict access to the system or use a secure network connection.

NEW QUESTION 292
- (Exam Topic 2)
An organization is repairing the damage after an incident. Which of the following controls is being implemented?

A. Detective
B. Preventive
C. Corrective
D. Compensating

Answer: C

Explanation:
A corrective control is a type of security control that is designed to mitigate the damage caused by a security incident or to restore the normal operations after an incident. A corrective control can include actions such as restoring from backups, applying patches, isolating infected systems, or implementing new policies and procedures. A corrective control is different from a preventive control, which aims to stop an incident from happening, or a detective control, which aims to identify and record an incident. References:
- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/security-controls-3/
- https://www.oreilly.com/library/view/comptia-security-all-in-one/9781260464016/ch31.xhtml
- https://www.professormesser.com/security-plus/sy0-501/security-controls-2/

NEW QUESTION 294
- (Exam Topic 2)
Which of the following best describes configuring devices to log to a centralized, off-site location for possible future reference?

A. Log aggregation
B. DLP
C. Archiving
D. SCAP

Answer: C

Explanation:
Archiving is the process of storing data for long-term preservation. In the context of IT security, archiving logs is the process of collecting and storing log files from devices in a centralized location. This allows organizations to access and analyze log data for troubleshooting, compliance, and security auditing purposes.
Log aggregation is the process of collecting log data from multiple sources and storing it in a single location. This can be done for performance or security reasons. However, log aggregation does not necessarily involve storing the logs in an off-site location.
DLP (Data Loss Prevention) is a set of technologies and processes that are used to protect sensitive data from unauthorized access, use, disclosure, alteration, or destruction. DLP can be used to prevent data from being exfiltrated from an organization's network, but it does not typically involve storing logs in an off-site location.
SCAP (Security Content Automation Protocol) is a set of standards and tools that are used to automate the assessment and remediation of security vulnerabilities. SCAP can be used to collect log data from devices, but it does not typically involve storing the logs in an off-site location.
Therefore, the best answer to the question is archiving.

NEW QUESTION 297
- (Exam Topic 2)
Which of the following is a primary security concern for a company setting up a BYOD program?

A. End of life
B. Buffer overflow
C. VM escape
D. Jailbreaking

Answer: D

Explanation:
Jailbreaking is a process of bypassing or removing the manufacturer-imposed restrictions on a mobile device’s operating system, allowing users to install unauthorized applications, modify settings, etc. It is a primary security concern for setting up a BYOD program because it can expose the device and its data to malware, vulnerabilities, unauthorized access, etc.

NEW QUESTION 301
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SY0-701 Exam with Our Prep Materials Via below:

https://www.certleader.com/SY0-701-dumps.html