CompTIA

Exam Questions SY0-701

CompTIA Security+ Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

   All examinations will be up to date.

* 24/7 Quality Support

   We will provide service round the clock.

* 100% Pass Rate

   Our guarantee that you will pass the exam.

* Unique Gurantee

   If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 1)
If a current private key is compromised, which of the following would ensure it cannot be used to decrypt ail historical data?

A. Perfect forward secrecy
B. Elliptic-curve cryptography
C. Key stretching
D. Homomorphic encryption

Answer: A

Explanation:
Perfect forward secrecy would ensure that it cannot be used to decrypt all historical data. Perfect forward secrecy (PFS) is a security protocol that generates a unique session key for each session between two parties. This ensures that even if one session key is compromised, it cannot be used to decrypt other sessions.

NEW QUESTION 2
- (Exam Topic 1)
Which of the following would produce the closet experience of responding to an actual incident response scenario?

A. Lessons learned
B. Simulation
C. Walk-through
D. Tabletop

Answer: B

Explanation:
A simulation exercise is designed to create an experience that is as close as possible to a real-world incident response scenario. It involves simulating an attack or other security incident and then having security personnel respond to the situation as they would in a real incident. References: CompTIA Security+ SY0-601 Exam Objectives: 1.1 Explain the importance of implementing security concepts, methodologies, and practices.

NEW QUESTION 3
- (Exam Topic 1)
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 a software development practice where developers merge their code into a shared repository several times a day, and the code is tested automatically. This ensures that code changes are tested and integrated continuously, reducing the risk of errors and conflicts.

NEW QUESTION 4
- (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 5
- (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. IaC
B. MSSP
C. Containers
D. SaaS

Answer: A

Explanation:
IaaS (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 6
- (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 7
- (Exam Topic 1)
A security assessment found that several embedded systems are running unsecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business Which of the following constraints BEST describes the reason the findings cannot be remediated?

A. inability to authenticate
B. Implied trust
C. Lack of computing power
D. Unavailable patch

Answer: D

Explanation:
If the systems are running unsecure protocols and the company that developed them is no longer in business, it is likely that there are no patches available to remediate the issue. References:
> CompTIA Security+ Study Guide, Sixth Edition, pages 35-36

NEW QUESTION 8
- (Exam Topic 1)
Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?

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

Answer: A

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

NEW QUESTION 9
- (Exam Topic 1)
An organization discovered a disgruntled employee exfiltrated a large amount of PII data by uploading files Which of the following controls should the organization consider to mitigate this risk?

A. EDR
B. Firewall
C. HIPS
D. DLP

Answer: D

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, print, email, upload, or download sensitive data 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.forcepoint.com/cyber-edu/data-loss-prevention-dlp

NEW QUESTION 10
- (Exam Topic 1)

A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

A. Vishing
B. Phishing
C. Spear phishing
D. Whaling

Answer: A

Explanation:
Vishing is a social engineering attack that uses phone calls or voicemail messages to trick people into divulging sensitive information, such as financial information or login credentials.

NEW QUESTION 10
- (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 13
- (Exam Topic 1)
An enterprise needs to keep cryptographic keys in a safe manner. Which of the following network appliances can achieve this goal?

A. HSM
B. CASB
C. TPM
D. DLP

Answer: A

Explanation:
Hardware Security Module (HSM) is a network appliance designed to securely store cryptographic keys and perform cryptographic operations. HSMs provide a secure environment for key management and can be used to keep cryptographic keys safe from theft, loss, or unauthorized access. Therefore, an enterprise can achieve the goal of keeping cryptographic keys in a safe manner by using an HSM appliance. References: CompTIA Security+ Certification Exam Objectives, Exam Domain 2.0: Technologies and Tools, 2.4 Given a scenario, use appropriate tools and techniques to troubleshoot security issues, p. 21

NEW QUESTION 16
- (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 17
- (Exam Topic 1)
An information security manager for an organization is completing a PCI DSS self-assessment for the first time. which of the is following MOST likely reason for this type of assessment?

A. An international expansion project is currently underway.
B. Outside consultants utilize this tool to measure security maturity.
C. The organization is expecting to process credit card information.
D. A government regulator has requested this audit to be completed

Answer: C

Explanation:
PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Any organization that accepts credit card payments is required to comply with PCI DSS.

NEW QUESTION 22
- (Exam Topic 1)
During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:

```
crackmapexec smb 192.168.10.232 -u localadmin -H 0A3CE8D07A46E5C51070F03593E0A5E6
```

Which of the following attacks occurred?

A. Buffer overflow
B. Pass the hash
C. SQL injection
D. Replay attack

Answer: B

Explanation:
Pass the hash is an attack technique that allows an attacker to authenticate to a remote server or service by using the hashed version of a user's password, rather than requiring the plaintext password

NEW QUESTION 27
- (Exam Topic 1)
A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

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

Answer: B

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

NEW QUESTION 31
- (Exam Topic 1)
Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations.
Which of the following documents did Ann receive?

A. An annual privacy notice
B. A non-disclosure agreement
C. A privileged-user agreement
D. A memorandum of understanding

Answer: A

Explanation:
Ann received an annual privacy notice from her mortgage company. An annual privacy notice is a statement from a financial institution or creditor that outlines the institution's privacy policy and explains how the institution collects, uses, and shares customers' personal information. It informs the customer about their rights under the Gramm-Leach-Bliley Act (GLBA) and the institution's practices for protecting their personal information. References:
➢ CompTIA Security+ Certification Exam Objectives - Exam SY0-601

NEW QUESTION 32
- (Exam Topic 1)
Which of the following isa risk that is specifically associated with hesting applications iin the public cloud?

A. Unsecured root accounts
B. Zero day
C. Shared tenancy
D. Insider threat

Answer: C

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

NEW QUESTION 35
- (Exam Topic 1)
A security engineer is hardening existing solutions to reduce application vulnerabilities. Which of the following solutions should the engineer implement FIRST? (Select TWO)

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

Answer: AF

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

NEW QUESTION 38
- (Exam Topic 1)
A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral

Answer: B

Explanation:
Symmetric encryption allows data to be encrypted and decrypted using the same key. This is useful when the data needs to be accessed and manipulated while still encrypted. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 6

NEW QUESTION 43
- (Exam Topic 1)
Which of the technologies is used to actively monitor for specific file types being transmitted on the network?

A. File integrity monitoring
B. Honeynets
C. Tcpreplay
D. Data loss prevention

Answer: D

Explanation:
Data loss prevention (DLP) is a technology used to actively monitor for specific file types being transmitted on the network. DLP solutions can prevent the unauthorized transfer of sensitive information, such as credit card numbers and social security numbers, by monitoring data in motion.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 99-102.

NEW QUESTION 48
- (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 49
- (Exam Topic 1)
An employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm employee's identity before sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing
B. Whaling
C. Phishing
D. Vishing

Answer: C

Explanation:
Phishing is a type of social engineering attack that uses fraudulent emails or other forms of communication to trick users into revealing sensitive information, such as passwords, credit card numbers, or personal details. Phishing emails often impersonate legitimate entities, such as banks, online services, or lottery organizations, and entice users to click on malicious links or attachments that lead to fake websites or malware downloads. Phishing emails usually target a large number of users indiscriminately, hoping that some of them will fall for the scam.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.kaspersky.com/resource-center/definitions/what-is-phishing

NEW QUESTION 51
- (Exam Topic 1)
A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which f the following configuration should an analysis enable
To improve security? (Select TWO.)

A. RADIUS
B. PEAP
C. WPS
D. WEP-EKIP
E. SSL
F. WPA2-PSK

Answer: AF

Explanation:
To improve the security of the WiFi network and prevent unauthorized devices from accessing the network, the configuration options of RADIUS and WPA2-PSK should be enabled. RADIUS (Remote Authentication Dial-In User Service) is an authentication protocol that can be used to control access to the WiFi network. It can provide stronger authentication and authorization than WEP and WPA. WPA2-PSK (WiFi Protected Access 2 with Pre-Shared Key) is a security protocol that uses stronger encryption than WEP and WPA. It requires a pre-shared key (PSK) to be entered on each device that wants to access the network. This helps prevent unauthorized devices from accessing the network.

NEW QUESTION 52
- (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 54
- (Exam Topic 1)
A security analyst reviews a company's authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?

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

Answer: C

Explanation:
Detailed
Password spraying is an attack where an attacker tries a small number of commonly used passwords against a large number of usernames. The goal of password spraying is to avoid detection by avoiding too many failed login attempts for any one user account. The fact that different usernames are being attacked from the same IP address is a strong indication that a password spraying attack is underway.

NEW QUESTION 56
- (Exam Topic 1)
A junior security analyst is reviewing web server logs and identifies the following pattern in the log file:

```
http://comptia.org/../../../etc/passwd
```

Which ol the following types of attacks is being attempted and how can it be mitigated?

A. XS
B. mplement a SIEM
C. CSR
D. implement an IPS
E. Directory traversal implement a WAF
F. SQL infection, mplement an IDS

Answer: C

Explanation:
Detailed
The attack being attempted is directory traversal, which is a web application attack that allows an attacker to access files and directories outside of the web root directory. A WAF can help mitigate this attack by detecting and blocking attempts to access files outside of the web root directory.
References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 4: Securing Application Development and Deployment, p. 191

NEW QUESTION 60
- (Exam Topic 1)
An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

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

Answer: E

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

NEW QUESTION 64
- (Exam Topic 1)
A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasional disappears.
The task list shows the following results

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

Which of the following is MOST likely the issue?

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

Answer: C

Explanation:
Spyware is malicious software that can cause a computer to slow down or freeze. It can also cause the mouse pointer to disappear. The task list shows an application named "spyware.exe" running, indicating that spyware is likely the issue. References:
➢ CompTIA Security+ Certification Exam Objectives 6.0: Given a scenario, analyze indicators of compromise and determine the type of malware.
➢ CompTIA Security+ Study Guide, Sixth Edition, pages 125-126

NEW QUESTION 66
- (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 69
- (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 72
- (Exam Topic 1)
A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls. Which of (he following should the manager request to complete the assessment?

A. A service-level agreement
B. A business partnership agreement
C. A SOC 2 Type 2 report
D. A memorandum of understanding

Answer: C

Explanation:
SOC 2 (Service Organization Control 2) is a type of audit report that evaluates the controls of service providers to verify their compliance with industry standards for security, availability, processing integrity, confidentiality, and privacy. A Type 2 report is based on an audit that tests the effectiveness of the controls over a period of time, unlike a Type 1 report which only evaluates the design of the controls at a specific point in time.
A SOC 2 Type 2 report would provide evidence of the vendor's security controls and how effective they are over time, which can help the security manager assess the vendor's security posture despite the vendor not allowing for a direct audit.
The security manager should request a SOC 2 Type 2 report to assess the security posture of the vendor. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 5

NEW QUESTION 74
- (Exam Topic 1)
During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

A. 1s
B. chflags
C. chmod
D. lsof
E. setuid

Answer: C

Explanation:
The chmod command is used to change the permissions of a file or directory. The analyst can use chmod to reduce the permissions for existing users and groups and remove the set-user-ID bit from the file. References:
➢ CompTIA Security+ Study Guide Exam SY0-601, Chapter 6

NEW QUESTION 76
- (Exam Topic 1)
As part of the lessons-learned phase, the SOC is tasked with building methods to detect if a previous incident is happening again. Which of the following would allow the security analyst to alert the SOC if an event is reoccurring?

A. Creating a playbook within the SOAR
B. Implementing rules in the NGFW
C. Updating the DLP hash database
D. Publishing a new CRL with revoked certificates

Answer: A

Explanation:
Creating a playbook within the Security Orchestration, Automation and Response (SOAR) tool would allow the security analyst to detect if an event is reoccurring by triggering automated actions based on the previous incident's characteristics. This can help the SOC to respond quickly and effectively to the incident. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7: Incident Response, pp. 352-354

NEW QUESTION 80
- (Exam Topic 1)
A backdoor was detected on the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry. Which of the following is the BEST solution to prevent this type of incident from occurring again?

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

Answer: A

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

NEW QUESTION 83
- (Exam Topic 1)
A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

A. Default system configuration
B. Unsecure protocols
C. Lack of vendor support
D. Weak encryption

Answer: C

Explanation:
Using legacy software to support a critical service poses a risk due to lack of vendor support. Legacy software is often outdated and unsupported, which means that security patches and upgrades are no longer available. This can leave the system vulnerable to exploitation by attackers who may exploit known vulnerabilities in the software to gain unauthorized access to the system.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 1: Attacks, Threats, and Vulnerabilities

NEW QUESTION 88
- (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 93
- (Exam Topic 1)
An organization wants seamless authentication to its applications. Which of the following should the organization employ to meet this requirement?

A. SOAP
B. SAML
C. SSO
D. Kerberos

Answer: C

Explanation:
Single Sign-On (SSO) is a mechanism that allows users to access multiple applications with a single set of login credentials. References: CompTIA Security+ Study Guide 601, Chapter 6

NEW QUESTION 96
- (Exam Topic 1)
A company's public-facing website, https://www.organization.com, has an IP address of 166.18.75.6. However, over the past hour the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows hitps://;www.organization.com is pointing to 151.191.122.115. Which of the following is occurring?

A. DoS attack
B. ARP poisoning
C. DNS spoofing
D. NXDOMAIN attack

Answer: C

Explanation:
The issue is DNS spoofing, where the DNS resolution has been compromised and is pointing to a malicious IP address. References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 7

NEW QUESTION 100
- (Exam Topic 1)
After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?

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

Answer: D

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

NEW QUESTION 101
- (Exam Topic 1)
Which of the following conditions impacts data sovereignty?

A. Rights management
B. Criminal investigations
C. Healthcare data
D. International operations

Answer: D

Explanation:
Data sovereignty refers to the legal concept that data is subject to the laws and regulations of the country in which it is located. International operations can impact data sovereignty as companies operating in multiple countries may need to comply with different laws and regulations. References:
➢ CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 5

NEW QUESTION 106
- (Exam Topic 1)
A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

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

Answer: B

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

NEW QUESTION 109
- (Exam Topic 1)
Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

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

Answer: B

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

NEW QUESTION 113
- (Exam Topic 1)
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

A. An incident response plan

B. A communications plan
C. A business continuity plan
D. A disaster recovery plan

Answer: B

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

NEW QUESTION 114
- (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 117
- (Exam Topic 1)
A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

A. Add a deny-all rule to that host in the network ACL
B. Implement a network-wide scan for other instances of the malware.
C. Quarantine the host from other parts of the network
D. Revoke the client's network access certificates

Answer: C

Explanation:
When malware is discovered on a host, the best course of action is to quarantine the host from other parts of the network. This prevents the malware from spreading and potentially infecting other hosts. Adding a
deny-all rule to the host in the network ACL may prevent legitimate traffic from being processed, implementing a network-wide scan is time-consuming and may not be necessary, and revoking the client's network access certificates is an extreme measure that may not be warranted. References: CompTIA Security+ Study Guide, pages 113-114

NEW QUESTION 118
- (Exam Topic 1)
During an investigation, the incident response team discovers that multiple administrator accounts were suspected of being compromised. The host audit logs indicate a repeated brute-force attack on a single administrator account followed by suspicious logins from unfamiliar geographic locations. Which of the following data sources would be BEST to use to assess the accounts impacted by this attack?

A. User behavior analytics
B. Dump files
C. Bandwidth monitors
D. Protocol analyzer output

Answer: A

Explanation:
User behavior analytics (UBA) would be the best data source to assess the accounts impacted by the attack, as it can identify abnormal activity, such as repeated brute-force attacks and logins from unfamiliar geographic locations, and provide insights into the behavior of the impacted accounts. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7: Incident Response, pp. 338-341

NEW QUESTION 121
- (Exam Topic 1)
Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid. Which of the following is impacted the MOST?

A. Identify theft
B. Data loss
C. Data exfiltration
D. Reputation

Answer: D

Explanation:
The best option that describes what is impacted the most by the hackers' attack and threat would be D. Reputation. Reputation is the perception or opinion that others have about a person or an organization. Reputation can affect the trust, credibility, and success of a person or an organization. In this scenario, if the hackers send the unfavorable pictures to the press, it can damage the reputation of the Chief Executive Officer and the company, and cause negative consequences such as loss of customers, partners, investors, or employees.

NEW QUESTION 126
- (Exam Topic 1)
A company recently experienced an attack during which 5 main website was directed to the atack-er's web server, allowing the attacker to harvest credentials from unsuspecting customers. Which of the following should the company Implement to prevent this type of attack from occurring in the future?

A. IPSec
B. SSL/TLS
C. DNSSEC
D. S/MIME

Answer: C

Explanation:
The attack described in the question is known as a DNS hijacking attack. In this type of attack, an attacker modifies the DNS records of a domain name to redirect traffic to their own server. This allows them to intercept traffic and steal sensitive information such as user credentials.
To prevent this type of attack from occurring in the future, the company should implement C. DNSSEC.
DNSSEC (Domain Name System Security Extensions) is a security protocol that adds digital signatures to DNS records. This ensures that DNS records are not modified during transit and prevents DNS hijacking attacks.

NEW QUESTION 129
- (Exam Topic 1)
A security engineer needs to create a network segment that can be used for servers thal require connections from untrusted networks. Which of the following should the engineer implement?

A. An air gap
B. A hot site
C. A VUAN
D. A screened subnet

Answer: D

Explanation:
A screened subnet is a network segment that can be used for servers that require connections from untrusted networks. It is placed between two firewalls, with one firewall facing the untrusted network and the other facing the trusted network. This setup provides an additional layer of security by screening the traffic that flows between the two networks. References: CompTIA Security+ Certification Guide, Exam SY0-501

NEW QUESTION 134
- (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 137
- (Exam Topic 1)
An employee's company account was used in a data breach Interviews with the employee revealed:
• The employee was able to avoid changing passwords by using a previous password again.
• The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.
Which of the following can be implemented to prevent these issues from reoccuring? (Select TWO)

A. Geographic dispersal
B. Password complexity
C. Password history
D. Geotagging
E. Password lockout
F. Geofencing

Answer: CF

Explanation:
two possible solutions that can be implemented to prevent these issues from reoccurring are password history and geofenc1in2g. Password history is a feature that prevents users from reusing their previous passwords1. This can enhance password security by forcing users to create new and unique passwords periodically1. Password history can be configured by setting a policy that specifies how many previous passwords are remembered and how often users must change their passwords1.
Geofencing is a feature that restricts access to a system or network based on the geographic location of the user or device2. This can enhance security by preventing unauthorized access from hostile or foreign region2s. Geofencing can be implemented by using GPS, IP address, or other methods to determine the location of the user or device and compare it with a predefined set of boundaries2.

NEW QUESTION 141
- (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 142
- (Exam Topic 1)
As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

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

Answer: A

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

NEW QUESTION 147
- (Exam Topic 1)
Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

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

Answer: D

Explanation:
A development environment is the environment that is used to develop and test software. It is typically installed locally on a system that allows code to be assessed directly and modified easily with each build. In this environment, dummy data is often utilized to test the software's functionality.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION 150
- (Exam Topic 1)
An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days. A security analyst notices the following:
•Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.
•Internal users in question were changing their passwords frequently during that time period.
•A jump box that several domain administrator users use to connect to remote devices was recently compromised.
•The authentication method used in the environment is NTLM.
Which of the following types of attacks is MOST likely being used to gain unauthorized access?

A. Pass-the-hash
B. Brute-force
C. Directory traversal
D. Replay

Answer: A

Explanation:
The suspicious activity reported by the application owner, combined with the recent compromise of the jump box and the use of NTLM authentication, suggests

that an attacker is likely using a pass-the-hash attack to gain unauthorized access to the financial application. This type of attack involves stealing hashed passwords from memory and then using them to authenticate as the compromised user without needing to know the user's plaintext password. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 5

NEW QUESTION 154
- (Exam Topic 1)
A security analyst needs an overview of vulnerabilities for a host on the network. Which of the following is the BEST type of scan for the analyst to run to discover which vulnerable services are running?

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

Answer: C

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

NEW QUESTION 155
- (Exam Topic 2)
A financial institution recently joined a bug bounty program to identify security issues in the institution's new public platform. Which of the following best describes who the institution is working with to identify security issues?

A. Script kiddie
B. Insider threats
C. Malicious actor
D. Authorized hacker

Answer: D

Explanation:
An authorized hacker, also known as an ethical hacker or a white hat hacker, is someone who uses their skills and knowledge to find and report security issues in a system or application with the permission of the owner. An authorized hacker follows the rules and guidelines of the bug bounty program and does not cause any harm or damage to the system or its users.

NEW QUESTION 156
- (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 161
- (Exam Topic 2)
A company recently upgraded its authentication infrastructure and now has more computing power. Which of the following should the company consider using to ensure user credentials are
being transmitted and stored more securely?

A. Blockchain
B. Salting
C. Quantum
D. Digital signature

Answer: B

Explanation:
Salting is a technique that adds random data to user credentials before hashing them. This makes the hashed credentials more secure and resistant to brute-force attacks or rainbow table attacks. Salting also ensures that two users with the same password will have different hashed credentials.
A company that has more computing power can consider using salting to ensure user credentials are being transmitted and stored more securely. Salting can increase the complexity and entropy of the hashed credentials, making them harder to crack or reverse.

NEW QUESTION 162
- (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. IaaS
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. IaaS. This is not the correct answer, because IaaS 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. IaaS 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 167
- (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 171
- (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 172
- (Exam Topic 2)
A security investigation revealed mat malicious software was installed on a server using a server administrator credentials. During the investigation the server administrator explained that Telnet was regularly used to log in. Which of the blowing most likely occurred?

A. A spraying attack was used to determine which credentials to use

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

Answer: B

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

NEW QUESTION 175
- (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 178
- (Exam Topic 2)
A network manager is concerned that business may be negatively impacted if the firewall in its data center goes offline. The manager would like to implement a high availability pair to:

A. decrease the mean time between failures.
B. remove the single point of failure.
C. cut down the mean time to repair
D. reduce the recovery time objective

Answer: B

Explanation:
A single point of failure is a component or element of a system that, if it fails, will cause the entire system to fail or stop functioning. It can pose a high risk and impact for business continuity and availability. A high availability pair is a configuration that involves two identical devices or systems that operate in parallel and provide redundancy and failover capabilities. It can remove the single point of failure by ensuring that if one device or system fails, the other one can take over its functions without interruption or downtime.

NEW QUESTION 182
- (Exam Topic 2)
A cybersecurity analyst at Company A is working to establish a secure communication channel with a counter part at Company B, which is 3,000 miles (4.828 kilometers) away. Which of the following concepts would help the analyst meet this goal m a secure manner?

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

Answer: B

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

NEW QUESTION 183
- (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 184
- (Exam Topic 2)
An organization recently released a software assurance policy that requires developers to run code scans each night on the repository. After the first night, the security team alerted the developers that more than 2,000 findings were reported and need to be addressed. Which of the following is the MOST likely cause for the high number of findings?

A. The vulnerability scanner was not properly configured and generated a high number of false positives
B. Third-party libraries have been loaded into the repository and should be removed from the codebase.
C. The vulnerability scanner found several memory leaks during runtime, causing duplicate reports for the same issue.
D. The vulnerability scanner was not loaded with the correct benchmarks and needs to be updated.

Answer: A

Explanation:
The most likely cause for the high number of findings is that the vulnerability scanner was not properly configured and generated a high number of false positives. False positive results occur when a vulnerability scanner incorrectly identifies a non-vulnerable system or application as being vulnerable. This can happen due to incorrect configuration, over-sensitive rule sets, or outdated scan databases.
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/sy0-601-comptia-security-plus-course/

NEW QUESTION 186
- (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 190
- (Exam Topic 2)
Which Of the following is a primary security concern for a 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 191
- (Exam Topic 2)
An organization has hired a security analyst to perform a penetration test The analyst captures 1Gb worth of inbound network traffic to the server and transfers the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?

A. Nmap
B. CURL
C. Neat
D. Wireshark

Answer: D

Explanation:
Wireshark is a tool that can analyze pcap files, which are files that capture network traffic. Wireshark can display the packets, protocols, and other details of the network traffic in a graphical user interface. Nmap is a tool that can scan networks and hosts for open ports and services. CURL is a tool that can transfer data from or to a server using various protocols. Neat is a tool that can test network performance and quality.

NEW QUESTION 196
- (Exam Topic 2)
A security administrator needs to provide secure access to internal networks for external partners The administrator has given the PSK and other parameters to

the third-party security administrator. Which of the following is being used to establish this connection?

A. Kerberos
B. SSL/TLS
C. IPSec
D. SSH

Answer: C

Explanation:
IPSec is a protocol suite that provides secure communication over IP networks. It uses encryption,
authentication, and integrity mechanisms to protect data from unauthorized access or modification. IPSec can operate in two modes: transport mode and tunnel mode. In tunnel mode, IPSec can create a virtual private network (VPN) between two endpoints, such as external partners and internal networks. To establish a VPN connection, IPSec requires a pre-shared key (PSK) or other parameters to negotiate the security association. References: https://www.comptia.org/content/guides/what-is-vpn

NEW QUESTION 197
- (Exam Topic 2)
A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802. IX using the most secure encryption and protocol available.
Perform the following steps:
* 1. Configure the RADIUS server.
* 2. Configure the WiFi controller.
* 3. Preconfigure the client for an incoming guest. The guest AD credentials are:
User: guest01 Password: guestpass
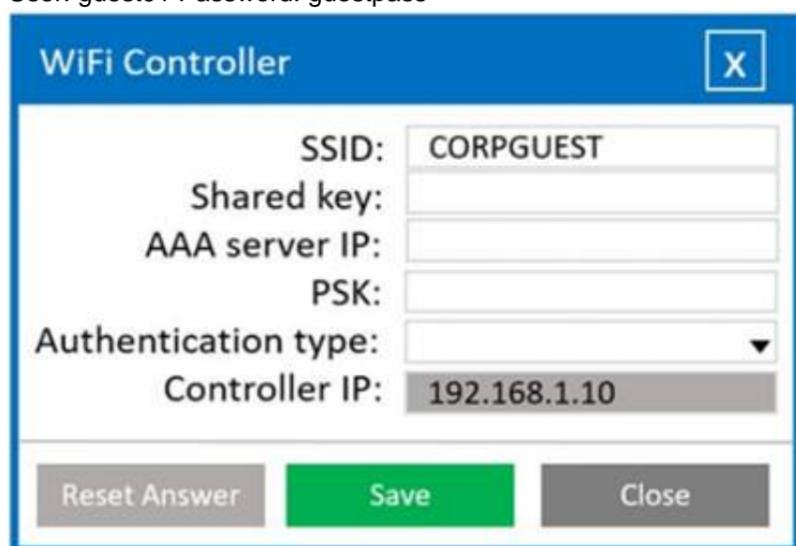
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Wifi Controller SSID: CORPGUEST
SHARED KEY: Secret
AAA server IP: 192.168.1.20
PSK: Blank
Authentication type: WPA2-EAP-PEAP-MSCHAPv2 Controller IP: 192.168.1.10
Radius Server Shared Key: Secret
Client IP: 192.168.1.10
Authentication Type: Active Directory Server IP: 192.168.1.20
Wireless Client SSID: CORPGUEST
Username: guest01 Userpassword: guestpass PSK: Blank
Authentication type: WPA2-Enterprise

NEW QUESTION 202
- (Exam Topic 2)
An annual information security has revealed that several OS-level configurations are not in compliance due to Outdated hardening standards the company is using Which Of the following would be best to use to update and reconfigure the OS.level security configurations?

A. CIS benchmarks
B. GDPR guidance
C. Regional regulations
D. ISO 27001 standards

Answer: A

Explanation:
CIS benchmarks are best practices and standards for securing various operating systems, applications, cloud environments, etc. They are developed by a community of experts and updated regularly to reflect the latest threats and vulnerabilities. They can be used to update and reconfigure the OS-level security configurations to ensure compliance and reduce risks

NEW QUESTION 204

- (Exam Topic 2)
A company is focused on reducing risks from removable media threats. Due to certain primary applications, removable media cannot be entirely prohibited at this time. Which of the following best describes the company's approach?

A. Compensating controls
B. Directive control
C. Mitigating controls
D. Physical security controls

Answer: C

Explanation:
Mitigating controls are designed to reduce the impact or severity of an event that has occurred or is likely to occur. They do not prevent or detect the event, but rather limit the damage or consequences of it. For example, a backup system is a mitigating control that can help restore data after a loss or corruption.
In this case, the company is focused on reducing risks from removable media threats, which are threats that can compromise data security, introduce malware infections, or cause media failure123. Removable media threats can be used to bypass network defenses and target industrial/OT environments2. The company cannot prohibit removable media entirely because of certain primary applications that require them, so it implements mitigating controls to lessen the potential harm from these threats.
Some examples of mitigating controls for removable media threats are:
- Encrypting data on removable media
- Scanning removable media for malware before use
- Restricting access to removable media ports
- Implementing policies and procedures for removable media usage and disposal
- Educating users on the risks and best practices of removable media

NEW QUESTION 208
- (Exam Topic 2)
An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization most likely consult?

A. The business continuity plan
B. The risk management plan
C. The communication plan
D. The incident response plan

Answer: A

Explanation:
A business continuity plan is a document or a process that outlines how an organization can continue its critical operations and functions in the event of a disruption or disaster. It can include strategies and procedures for recovering or relocating resources, personnel, data, etc., to ensure minimal downtime and impact. The organization will most likely consult the business continuity plan when setting up offices in a temporary work space after its corporate offices were destroyed due to a natural disaster.

NEW QUESTION 211
- (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 214
- (Exam Topic 2)
A data cento has experienced an increase in under-voltage events Mowing electrical grid maintenance outside the facility These events are leading to occasional losses of system availability Which of the following would be the most cost-effective solution for the data center 10 implement''

A. Uninterruptible power supplies with battery backup
B. Managed power distribution units lo track these events
C. A generator to ensure consistent, normalized power delivery
D. Dual power supplies to distribute the load more evenly

Answer: A

Explanation:
Uninterruptible power supplies with battery backup would be the most cost-effective solution for the data center to implement to prevent under-voltage events following electrical grid maintenance outside the facility. An uninterruptible power supply (UPS) is a device that provides emergency power to a load when the main power source fails or drops below an acceptable level. A UPS with battery backup can help prevent under-voltage events by switching to battery power when it detects a voltage drop or outage in the main power source. A UPS with battery backup can also protect the data center equipment from power surges or spikes. References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.apc.com/us/en/faqs/FA158852/

NEW QUESTION 216
- (Exam Topic 2)
A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

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

Answer: A

Explanation:
MFA stands for multi-factor authentication, which is a method of verifying a user's identity using two or more
factors, such as something you know (e.g., password), something you have (e.g., token), or something you are (e.g., biometrics). MFA can prevent someone from using the exfiltrated credentials, as they would need to provide another factor besides the username and password to access the system or application. MFA can also alert the legitimate user of an unauthorized login attempt, allowing them to change their credentials or report the incident. References:
- https://www.comptia.org/certifications/security
- https://www.youtube.com/watch?v=yCJyPPvM-xg
- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/multi-factor-authentication-5/

NEW QUESTION 219
- (Exam Topic 2)
Which of the following is required in order (or an IDS and a WAF to be effective on HTTPS traffic?

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

Answer: C

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

NEW QUESTION 221
- (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 224
- (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 226
- (Exam Topic 2)
A user enters a password to log in to a workstation and is then prompted to enter an authentication code Which of the following MFA factors or attributes are being utilized in the authentication process? {Select two).

A. Something you know
B. Something you have
C. Somewhere you are
D. Someone you know
E. Something you are
F. Something you can do

Answer: AB

Explanation:
MFA (Multi-Factor Authentication) is a method of verifying a user's identity by requiring two or more factors or attributes that belong to different categories. The categories are something you know (such as a password or a PIN), something you have (such as a token or a smart card), something you are (such as a fingerprint or an iris scan), something you do (such as a gesture or a voice command), and somewhere you are (such as a location or an IP address). In this case, the user enters a password (something you know) and then receives an authentication code (something you have) to log in to a workstation.

NEW QUESTION 227
- (Exam Topic 2)
Which Of the following security controls can be used to prevent multiple from using a unique card swipe and being admitted to a entrance?

A. Visitor logs
B. Faraday cages
C. Access control vestibules
D. Motion detection sensors

Answer: C

Explanation:
Access control vestibules are physical security controls that consist of two sets of doors or gates that create a small enclosed space between them. Only one door or gate can be opened at a time, and only one person can enter or exit the vestibule at a time. Access control vestibules can prevent multiple people from using a unique card swipe and being admitted to a secure entrance, as they require each person to authenticate individually and prevent tailgating or piggybacking.

NEW QUESTION 228
- (Exam Topic 2)
A security administrator is using UDP port 514 to send a syslog through an unsecure network to the SIEM server. Which of the following is the best way for the administrator to improve the process?

A. Change the protocol to TCP.
B. Add LDAP authentication to the SIEM server.
C. Use a VPN from the internal server to the SIEM and enable DLP.
D. Add SSL/TLS encryption and use a TCP 6514 port to send logs.

Answer: D

Explanation:
SSL/TLS encryption is a method of securing the syslog traffic by using cryptographic protocols to encrypt and authenticate the data. SSL/TLS encryption can prevent eavesdropping, tampering, or spoofing of the syslog messages. TCP 6514 is the standard port for syslog over TLS, as defined by RFC 5425. Using this port can ensure compatibility and interoperability with other syslog implementations that support TLS.

NEW QUESTION 231
- (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 233
- (Exam Topic 2)
An attacker is using a method to hide data inside of benign files in order to exfiltrate confidential data. Which of the following is the attacker most likely using?

A. Base64 encoding
B. Steganography
C. Data encryption
D. Perfect forward secrecy

Answer: B

Explanation:
Steganography is a technique for hiding data inside of benign files such as images, audio, or video. This can be used to exfiltrate confidential data without raising suspicion or detection.
References: How to Hide Files Inside Files [Images, Folder] - Raymond.CC Blog; How to Hide Data in a Secret Text File Compartment - How-To Geek; How to Hide Data Within an Image - Medium

NEW QUESTION 234
- (Exam Topic 2)
A user is trying unsuccessfully to send images via SMS. The user downloaded the images from a corporate email account on a work phone. Which of the following policies is preventing the user from completing this action?

A. Application management
B. Content management
C. Containerization
D. Full disk encryption

Answer: B

Explanation:
Content management is a policy that controls what types of data can be accessed, modified, shared, or transferred by users or applications. Content management can prevent data leakage or exfiltration by blocking or restricting certain actions, such as copying, printing, emailing, or sending data via SMS. If the user downloaded the images from a corporate email account on a work phone, the content management policy may prevent the user from sending the images via SMS to protect the confidentiality and integrity of the data.
References: 1
CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and
Design, Objective 2.4: Explain the importance of embedded and specialized systems security 2
CompTIA
Security+ Certification Exam Objectives, page 12, Domain 3.0: Implementation, Objective 3.1: Implement
secure network architecture concepts 3 https://www.comptia.org/blog/what-is-data-loss-prevention

NEW QUESTION 238
- (Exam Topic 2)
An air traffic controller receives a change in flight plan for an morning aircraft over the phone. The air traffic controller compares the change to what appears on radar and determines the information to be false. As a result, the air traffic controller is able to prevent an incident from occurring. Which of the following is this scenario an example of?

A. Mobile hijacking
B. Vishing
C. Unsecure VoIP protocols
D. SPIM attack

Answer: B

Explanation:
Vishing is a form of phishing that uses voice calls or voice messages to trick victims into revealing personal information, such as credit card numbers, bank details, or passwords. Vishing often uses spoofed phone numbers, voice-altering software, or social engineering techniques to impersonate legitimate organizations or authorities. In this scenario, the caller pretended to be someone who could change the flight plan of an aircraft, which could have caused a serious incident.

NEW QUESTION 242
- (Exam Topic 2)
The management team has requested that the security team implement 802.1X into the existing wireless network setup. The following requirements must be met:
• Minimal interruption to the end user
• Mutual certificate validation
Which of the following authentication protocols would meet these requirements?

A. EAP-FAST
B. PSK
C. EAP-TTLS
D. EAP-TLS

Answer: D

Explanation:
EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses certificates to provide mutual authentication between the client and the authentication server. It also allows for the encryption of user credentials, making EAP-TLS a secure and reliable authentication protocol. According to the CompTIA Security+ SY0-601 Official Text Book, EAP-TLS is well-suited for wireless networks due to its mutual authentication capabilities and its ability to securely store credentials. It is also the preferred authentication protocol for 802.1X wireless networks.

NEW QUESTION 245
- (Exam Topic 2)
To reduce and limit software and infrastructure costs the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have secuity controls to protect sensitive data Which of the following cloud services would best accommodate the request?

A. IaaS
B. PaaS
C. DaaS
D. SaaS

Answer: D

Explanation:
SaaS (Software as a Service) is a cloud model that provides clients with applications and software that are hosted and managed by a cloud provider over the internet. It can move email services to the cloud by allowing clients to access and use email applications without installing or maintaining them on their own devices or servers

NEW QUESTION 248
- (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)
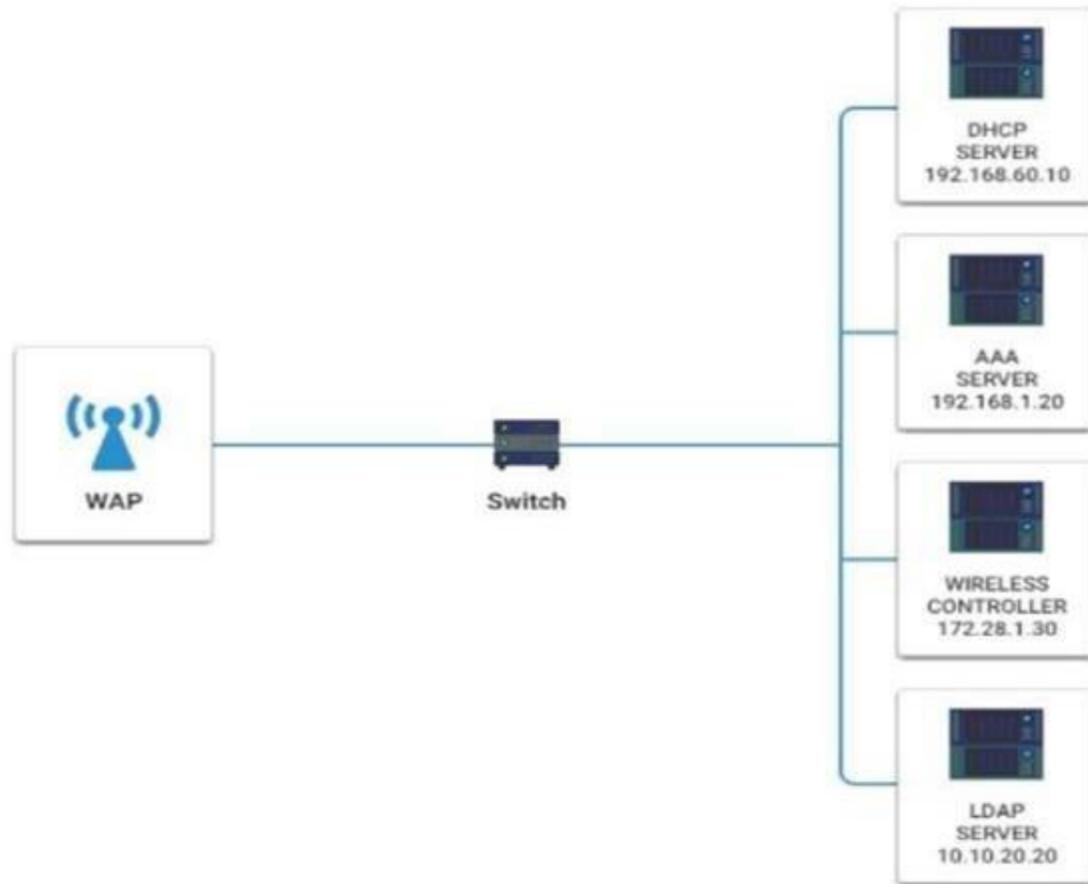
NEW QUESTION 250
- (Exam Topic 2)
A newly purchased corporate WAP needs to be configured in the MOST secure manner possible. INSTRUCTIONS
Please click on the below items on the network diagram and configure them accordingly:
> WAP
> DHCP Server
> AAA Server
> Wireless Controller
> LDAP Server
If at any 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 252
- (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 points are up and running One of the help desk technicians notices the affected users are working in a building near the parking lot. Which of the following is the most likely reason for the outage?

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

Answer: A

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

NEW QUESTION 255
- (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 259
- (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 261
- (Exam Topic 2)
Which of the following is the correct order of evidence from most to least volatile in forensic analysis?

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

Answer: C

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

NEW QUESTION 264
- (Exam Topic 2)
A security administrator recently used an internal CA to issue a certificate to a public application. A user tries to reach the application but receives a message stating, "Your connection is not private." Which of the following is the best way to fix this issue?

A. Ignore the warning and continue to use the application normally.
B. Install the certificate on each endpoint that needs to use the application.
C. Send the new certificate to the users to install on their browsers.
D. Send a CSR to a known CA and install the signed certificate on the application's server.

Answer: D

Explanation:
A certificate issued by an internal CA is not trusted by default by external users or applications. Therefore, when a user tries to reach the application that uses an internal CA certificate, they will receive a warning message that their connection is not private1. The best way to fix this issue is to use a certificate signed by a well-known public CA that is trusted by most browsers and operating systems1. To do this, the security administrator needs to send a certificate signing request (CSR) to a public CA and install the signed certificate on the application's server2. The other options are not recommended or feasible. Ignoring the warning and continuing to use the application normally is insecure and exposes the user to potential man-in-the-middle attacks3. Installing the certificate on each endpoint that needs to use the application is impractical and cumbersome, especially if there are many users or devices involved3. Sending the new certificate to the users to install on their browsers is also inconvenient and may not work for some browsers or devices3.

References: 1: https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-self-signed-certificate 2: https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-certificate-management 3: https://serverfault.com/questions/1106443/should-i-use-a-public-or-a-internal-ca-for-client-certificate-mtls

NEW QUESTION 267
- (Exam Topic 2)
A company is concerned about individuals driving a car into the building to gain access. Which of the following security controls would work BEST to prevent this from happening?

A. Bollard
B. Camera
C. Alarms
D. Signage
E. Access control vestibule

Answer: A

Explanation:
Bollards are posts designed to prevent vehicles from entering an area. They are usually made of steel or concrete and are placed close together to make it difficult for vehicles to pass through. In addition to preventing vehicles from entering an area, bollards can also be used to protect buildings and pedestrians from ramming attacks. They are an effective and cost-efficient way to protect buildings and pedestrians from unauthorized access.

NEW QUESTION 270
- (Exam Topic 2)
While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?

A. Documenting the new policy in a change request and submitting the request to change management
B. Testing the policy in a non-production environment before enabling the policy in the production network
C. Disabling any intrusion prevention signatures on the "deny any" policy prior to enabling the new policy
D. Including an "allow any" policy above the "deny any" policy

Answer: B

Explanation:
Testing the policy in a non-production environment before enabling the policy in the production network would prevent the issue of making several company servers unreachable. A non-production environment is a replica of the production network that is used for testing, development, or training purposes. By testing the policy in a non-production environment, the technician can verify the functionality and impact of the policy without affecting the real network or users. This can help to identify and resolve any errors or conflicts before applying the policy to the production network. Testing the policy in a non-production environment can also help to ensure compliance with security standards and best practices.

NEW QUESTION 275
- (Exam Topic 2)
A security architect is designing the new outbound internet for a small company. The company would like all 50 users to share the same single Internet connection. In addition, users will not be permitted to use social media sites or external email services while at work. Which of the following should be included in this design to satisfy these requirements? (Select TWO).

A. DLP
B. MAC filtering
C. NAT
D. VPN
E. Content filler
F. WAF

Answer: CD

Explanation:
NAT (Network Address Translation) is a technology that allows multiple devices to share a single IP address, allowing them to access the internet while still maintaining security and privacy. VPN (Virtual Private Network) is a technology that creates a secure, encrypted tunnel between two or more devices, allowing users to access the internet and other network resources securely and privately. Additionally, VPNs can also be used to restrict access to certain websites and services, such as social media sites and external email services.

NEW QUESTION 280
- (Exam Topic 2)
An employee's company email is configured with conditional access and requires that MFA is enabled and used. An example of MFA is a phone call and:

A. a push notification
B. a password.
C. an SMS message.
D. an authentication application.

Answer: D

Explanation:
An authentication application can generate one-time passwords or QR codes that are time-based and unique to each user and device. It does not rely on network connectivity or SMS delivery, which can be intercepted or delayed. It also does not require the user to respond to a push notification, which can be accidentally approved or ignored.

NEW QUESTION 284
- (Exam Topic 2)
Which of the following Is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

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

Answer: A

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

NEW QUESTION 289
- (Exam Topic 2)
Which of the following terms should be included in a contract to help a company monitor the ongo-ing security maturity Of a new vendor?

A. A right-to-audit clause allowing for annual security audits
B. Requirements for event logs to kept for a minimum of 30 days
C. Integration of threat intelligence in the companys AV
D. A data-breach clause requiring disclosure of significant data loss

Answer: A

Explanation:
A right-to-audit clause is a contractual provision that allows one party to audit the records and activities of
another party to ensure compliance with security policies and standards. It can help a company monitor the ongoing security maturity of a new vendor by conducting annual security audits and identifying any gaps or issues that need to be addressed.

NEW QUESTION 294
- (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 296
- (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 300
- (Exam Topic 2)
Which of the following security design features can an development team to analyze the deletion eoting Of data sets the copy?

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

Answer: C

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

NEW QUESTION 303
- (Exam Topic 2)
A network security manager wants to implement periodic events that will test the security team's preparedness for incidents in a controlled and scripted manner, Which of the following concepts describes this scenario?

A. Red-team exercise
B. Business continuity plan testing
C. Tabletop exercise
D. Functional exercise

Answer: C

Explanation:
A tabletop exercise is a type of security exercise that involves a simulated scenario of a security incident and a discussion of how the security team would respond to it1. A tabletop exercise is a low-impact and
cost-effective way to test the security team's preparedness, identify gaps and areas for improvement, and
enhance communication and coordination among team members2. A tabletop exercise is different from a red-team exercise, which is a simulated attack by an authorized group of ethical hackers to test the security defenses and response capabilities of an organization3. A business continuity plan testing is a process of verifying that an organization can continue its essential functions and operations in the event of a disaster or disruption4. A functional exercise is a type of security exercise that involves a realistic simulation of a security incident and requires the security team to perform their roles and responsibilities as if it were a real event.
References: 1:
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-g
2: https://www.linuxjournal.com/content/security-exercises 3:
https://www.imperva.com/learn/application-security/red-team-blue-team/ 4: https://www.ready.gov/business-continuity-plan : https://www.ready.gov/exercises

NEW QUESTION 306
- (Exam Topic 2)
A security analyst was asked to evaluate a potential attack that occurred on a publicly accessible section of the company's website. The malicious actor posted an entry in an attempt to trick users into clicking the following:

```
https://www.c0mpt1a.com/contact-us/%3Fname%3D%3Cscript%3Ealert(document.cookie)%3C%2Fscript%3E
```

Which of the following was most likely observed?

A. DLL injection
B. Session replay
C. SQLi
D. xss

Answer: D

Explanation:
Cross-site scripting is a type of web application attack that involves injecting malicious code or scripts into a trusted website or application. The malicious code or script can execute in the browser of the victim who visits the website or application, and can perform actions such as stealing cookies, redirecting to malicious sites, displaying fake content, or compromising the system. References:
https://www.comptia.org/blog/what-is-cross-site-scripting
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 311
- (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 314
- (Exam Topic 2)
An organization has expanded its operations by opening a remote office. The new office is fully furnished with office resources to support up to 50 employees working on any given day. Which of the following VPN solutions would best support the new office?

A. Always-on
B. Remote access
C. Site-to-site
D. Full tunnel

Answer: C

Explanation:
Site-to-site VPN is a type of VPN solution that connects two or more networks or sites across the public internet in a secure and encrypted way. Site-to-site VPN can be implemented using VPN appliances, such as firewalls or routers, that can establish and maintain the VPN tunnel between the sites. Site-to-site VPN can support multiple users or devices that need to access resources on the other site without requiring individual VPN clients or software. Site-to-site VPN is the best solution to support the new remote office, as it can provide secure and seamless connectivity between the office network and the main network of the organization.
Verified References:
➤ Virtual Private Networks – SY0-601 CompTIA Security+ : 3.3 https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/virtual-private-networks-sy0-601- (See Site-to-Site VPN)
➤ VPN Technologies – CompTIA Security+ SY0-501 – 3.2 https://www.professormesser.com/security-plus/sy0-501/vpn-technologies/ (See Site-to-Site VPN)
➤ Security+ (Plus) Certification | CompTIA IT Certifications https://www.comptia.org/certifications/security (See Domain 3: Architecture and Design, Objective 3.3: Given a scenario, implement secure network architecture concepts.)

NEW QUESTION 317
- (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 321
- (Exam Topic 2)
A security engineer is setting up passwordless authentication for the first time. INSTRUCTIONS
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.
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:
A screenshot of a computer Description automatically generated with medium confidence

NEW QUESTION 323
- (Exam Topic 2)
An organization wants to secure a LAN/WLAN so users can authenticate and transport data securely. The solution needs to prevent on-path attacks and evil twin attacks. Which of the following will best meet the organization's need?

A. MFA
B. 802.1X
C. WPA2
D. TACACS

Answer: B

Explanation:
* 802.1 X is a standard for network access control that provides authentication and encryption for devices that connect to a LAN/WLAN. 802.1X uses the Extensible Authentication Protocol (EAP) to exchange authentication messages between a supplicant (the device requesting access), an authenticator (the device granting access), and an authentication server (the device verifying credentials). 802.1X can prevent on-path attacks and evil twin attacks by requiring users to provide valid credentials before accessing the network and encrypting the data transmitted over the network.
On-path attacks are attacks that involve intercepting or modifying network traffic between two endpoints. An on-path attacker can eavesdrop on sensitive information, alter or inject malicious data, or redirect traffic to malicious destinations. On-path attacks are frequently perpetrated over WiFi network1s.
Evil twin attacks are attacks that involve setting up a fake WiFi access point that mimics a legitimate one. An evil twin attacker can trick users into connecting to the fake network and then monitor or manipulate their online activity. Evil twin attacks are more common on public WiFi networks that are unsecured and leave personal data vulnerable23.

NEW QUESTION 325
- (Exam Topic 2)
A network administrator has been alerted that web pages are experiencing long load times After determining it is not a routing or DNS issue the administrator logs in to the router, runs a command, and receives the following output:
CPU 0 percent busy, from 300 sec ago 1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
Which of the following is The router experiencing?

A. DDoS attack
B. Memory leak
C. Buffer overflow
D. Resource exhaustion

Answer: D

Explanation:
The router is experiencing a resource exhaustion issue. The output from the command indicates that the CPU is consistently busy, with a 1-second average of 99 percent busy and a 1-minute average of 83 percent busy.
This indicates that the router is struggling to keep up with the demands placed on it, potentially due to a high volume of traffic or other factors. As a result, web pages are experiencing long load times. This is an example of resource exhaustion, where the router's resources are being overwhelmed and are unable to meet the demands placed on them. A DDoS attack, memory leak, or buffer overflow would not typically cause the symptoms described in the scenario.

NEW QUESTION 330
- (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 334
- (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 336
......

Relate Links

100% Pass Your SY0-701 Exam with Exambible Prep Materials

https://www.exambible.com/SY0-701-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/