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)
A software company is analyzing a process that detects software vulnerabilities at the earliest stage possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. Which of the following would BEST assist the company with this objective?

A. Use fuzzing testing
B. Use a web vulnerability scanner
C. Use static code analysis
D. Use a penetration-testing OS

Answer: C

Explanation:
Using static code analysis would be the best approach to scan the source code looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. This method involves analyzing the source code without actually running the software, which can identify security vulnerabilities that may not be detected by other testing methods. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6: Risk Management, pp. 292-295

NEW QUESTION 2
- (Exam Topic 1)
A company Is planning to install a guest wireless network so visitors will be able to access the Internet. The stakeholders want the network to be easy to connect to so time is not wasted during meetings. The WAPs are configured so that power levels and antennas cover only the conference rooms where visitors will attend meetings. Which of the following would BEST protect the company's Internal wireless network against visitors accessing company resources?

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

Answer: A

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

NEW QUESTION 3
- (Exam Topic 1)
A store receives reports that shoppers’ credit card information is being stolen. Upon further analysis, those same shoppers also withdrew money from an ATM in that store.
The attackers are using the targeted shoppers’ credit card information to make online purchases. Which of the following attacks is the MOST probable cause?

A. Identity theft
B. RFID cloning
C. Shoulder surfing
D. Card skimming

Answer: D

Explanation:
The attackers are using card skimming to steal shoppers' credit card information, which they use to make online purchases. References:
CompTIA Security+ Study Guide Exam SY0-601, Chapter 5

NEW QUESTION 4
- (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 5
- (Exam Topic 1)
A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?

A. Disable Telnet and force SSH.
B. Establish a continuous ping.
C. Utilize an agentless monitor
D. Enable SNMPv3 With passwords.

Answer: C

Explanation:
An agentless monitor is the best method to monitor network operations because it does not require any software or agents to be installed on the devices being monitored, making it less intrusive and less likely to disrupt network operations. This method can monitor various aspects of network operations, such as traffic, performance, and security.
CompTIA Security+ Study Guide, Sixth Edition (SY0-601), Chapter 4: Attacks, Threats, and Vulnerabilities, Monitoring and Detection Techniques, pg. 167-170.

NEW QUESTION 6
- (Exam Topic 1)
The Chief information Security Officer has directed the security and networking team to retire the use of shared passwords on routers and switches. Which of the following choices BEST meets the requirements?

A. SAML
B. TACACS+
C. Password vaults
D. OAuth

Answer: B

Explanation:
TACACS+ is a protocol used for remote authentication, authorization, and accounting (AAA) that can be used to replace shared passwords on routers and switches. It provides a more secure method of authentication that allows for centralized management of access control policies. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6

NEW QUESTION 7
- (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 8
- (Exam Topic 1)
A Chief Information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?

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

Answer: A

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

NEW QUESTION 9
- (Exam Topic 1)
A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The company would like to use MDM, but employees are concerned about the loss of personal data. Which of the following should the IT department implement to BEST protect the company against company data loss while still addressing the employees' concerns?

A. Enable the remote-wiping option in the MDM software in case the phone is stolen.
B. Configure the MDM software to enforce the use of PINs to access the phone.
C. Configure MDM for FDE without enabling the lock screen.
D. Perform a factory reset on the phone before installing the company's applications.

Answer: C

Explanation:
MDM software is a type of remote asset-management software that runs from a central server. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets. It can monitor and regulate both corporate-owned and personally owned devices to the organization's policies.
FDE stands for full disk encryption, which is a method of encrypting all data on a device's storage. FDE can protect data from unauthorized access in case the device is lost or stolen.
If a company decides to allow its employees to use their personally owned devices for work tasks, it should configure MDM software to enforce FDE on those

devices. This way, the company can protect its data from being exposed if the device falls into the wrong hands.
However, employees may be concerned about the loss of personal data if the company also enables the remote-wiping option in the MDM software. Remote wiping is a feature that allows the company to erase all data on a device remotely in case of theft or loss. Remote wiping can also affect personal data on the device, which may not be acceptable to employees.
Therefore, a possible compromise is to configure MDM for FDE without enabling the lock screen. This means that the device will be encrypted, but it will not require a password or PIN to unlock it. This way, employees can access their personal data easily, while the company can still protect its data with encryption.
The other options are not correct because:
- A. Enable the remote-wiping option in the MDM software in case the phone is stolen. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. Remote wiping can erase both work and personal data on the device, which may not be desirable for employees.
- B. Configure the MDM software to enforce the use of PINs to access the phone. This option may enhance the security of the device, but it may not address the company's concern about data loss. PINs can be guessed or bypassed by attackers, and they do not protect data if the device is physically accessed.
- D. Perform a factory reset on the phone before installing the company's applications. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. A factory reset will erase all data on the device, including personal data, which may not be acceptable to employees.

According to CompTIA Security+ SY0-601 Exam Objectives 2.4 Given a scenario, implement secure systems design:
"MDM software is a type of remote asset-management software that runs from a central server1. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets2."
"FDE stands for full disk encryption, which is a method of encrypting all data on a device's storage3." References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.makeuseof.com/what-is-mobile-device-management-mdm-software/

NEW QUESTION 10
- (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 10
- (Exam Topic 1)
A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO).

A. HIDS
B. NIPS
C. HSM
D. WAF
E. NAC
F. NIDS
G. Stateless firewall

Answer: DF

Explanation:
A WAF (Web Application Firewall) and NIDS (Network Intrusion Detection System) are both examples of Layer 7 security controls. A WAF can block attacks at the application layer (Layer 7) of the OSI model by filtering traffic to and from a web server. NIDS can also detect attacks at Layer 7 by monitoring network traffic for suspicious patterns and behaviors. References: CompTIA Security+ Study Guide, pages 94-95, 116-118

NEW QUESTION 13
- (Exam Topic 1)
A security administrator has discovered that workstations on the LAN are becoming infected with malware.
The cause of the infections appears to be users receiving phishing emails that are bypassing the current
email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?

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

Answer: C

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

NEW QUESTION 18
- (Exam Topic 1)
Which of the following BEST describes a technique that compensates researchers for finding vulnerabilities?

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

Answer: D

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

NEW QUESTION 20
- (Exam Topic 1)
Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?

A. Pulverizing
B. Shredding
C. Incinerating
D. Degaussing

Answer: B

Explanation:
Shredding may be the most secure and cost-effective way to destroy electronic data in any media that contain hard drives or solid-state drives and have reached their end-of-life1. Shredding reduces electronic devices to pieces no larger than 2 millimeters2. Therefore, shredding is the most secure but least expensive data destruction method for data that is stored on hard drives.

NEW QUESTION 23
- (Exam Topic 1)
As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

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

Answer: A

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

NEW QUESTION 27
- (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 28
- (Exam Topic 1)
The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on

physical location and proximity. Which of the following Is the BEST solution for the pilot?

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

Answer: A

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

NEW QUESTION 31
- (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 33
- (Exam Topic 1)
A security analyst is running a vulnerability scan to check for missing patches during a suspected security rodent During which of the following phases of the response process is this activity MOST likely occurring?

A. Containment
B. Identification
C. Recovery
D. Preparation

Answer: B

Explanation:
Vulnerability scanning is a proactive security measure used to identify vulnerabilities in the network and systems. References: CompTIA Security+ Study Guide 601, Chapter 4

NEW QUESTION 37
- (Exam Topic 1)
A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promoting to production?

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

Answer: C

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

NEW QUESTION 38
- (Exam Topic 1)
A security engineer needs to build @ solution to satisfy regulatory requirements that stale certain critical servers must be accessed using MFA However, the critical servers are older and are unable to support the addition of MFA, Which of te following will the engineer MOST likely use to achieve this objective?

A. A forward proxy
B. A stateful firewall
C. A jump server
D. A port tap

Answer: C

Explanation:
A jump server is a secure host that allows users to access other servers within a network. The jump server acts as an intermediary, and users can access other servers via the jump server after authenticating with MFA.

NEW QUESTION 43
- (Exam Topic 1)
After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?

A. The unexpected traffic correlated against multiple rules, generating multiple alerts.
B. Multiple alerts were generated due to an attack occurring at the same time.
C. An error in the correlation rules triggered multiple alerts.
D. The SIEM was unable to correlate the rules, triggering the alert

Answer: A

Explanation:
Multiple alerts were generated on the SIEM during the emergency maintenance activity due to unexpected traffic correlated against multiple rules. The SIEM generates alerts when it detects an event that matches a rule in its rulebase. If the event matches multiple rules, the SIEM will generate multiple alerts.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION 45
- (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 46
- (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 49
- (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 51
- (Exam Topic 1)
A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time

while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?

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

Answer: B

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

NEW QUESTION 55
- (Exam Topic 1)
A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

A. The Diamond Model of Intrusion Analysis
B. The Cyber Kill Chain
C. The MITRE CVE database
D. The incident response process

Answer: A

Explanation:
The Diamond Model is a framework for analyzing cyber threats that focuses on four key elements: adversary, capability, infrastructure, and victim. By analyzing these elements, security researchers can gain a better understanding of the threat landscape and develop more effective security strategies.

NEW QUESTION 60
- (Exam Topic 1)
Which of the following incident response steps occurs before containment?

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

Answer: D

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

NEW QUESTION 64
- (Exam Topic 1)
Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities. After further investigation, a security analyst notices the following:
• All users share workstations throughout the day.
• Endpoint protection was disabled on several workstations throughout the network.
• Travel times on logins from the affected users are impossible.
• Sensitive data is being uploaded to external sites.
• All user account passwords were forced to be reset and the issue continued. Which of the following attacks is being used to compromise the user accounts?

A. Brute-force
B. Keylogger
C. Dictionary
D. Rainbow

Answer: B

Explanation:
The symptoms suggest a keylogger is being used to compromise the user accounts, allowing the attackers to obtain the users' passwords and other sensitive information. References:
> CompTIA Security+ Study Guide Exam SY0-601, Chapter 6

NEW QUESTION 65
- (Exam Topic 1)
A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:

```
IPv4 Address ..... 10.0.0.87
Subnet Mask  ..... 255.255.255.0
Default Gateway ..... 10.0.0.1


 Internet Address      Physical Address
 10.10.255.255         ff-ff-ff-ff-ff-ff
 10.0.0.1              aa-aa-aa-aa-aa-aa
 10.0.0.254            aa-aa-aa-aa-aa-aa
 224.0.0.2             01-00-5e-00-00-02
```

Based on the IoCS, which of the following was the MOST likely attack used to compromise the network communication?

A. Denial of service
B. ARP poisoning
C. Command injection
D. MAC flooding

Answer: B

Explanation:
ARP poisoning (also known as ARP spoofing) is a type of attack where an attacker sends falsified ARP messages over a local area network to link the attacker's MAC address with the IP address of another host on the network. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 6, page 271.

NEW QUESTION 67
- (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 69
- (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 72
- (Exam Topic 1)
A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technical implementation to prevent this from happening again?

A. Configure DLP solutions
B. Disable peer-to-peer sharing
C. Enable role-based
D. Mandate job rotation

E. Implement content filters

Answer: A

Explanation:
Data loss prevention (DLP) solutions can prevent the accidental or intentional loss of sensitive data. DLP tools can identify and protect sensitive data by classifying and categorizing it, encrypting it, or blocking it from being transferred outside the organization's network.

NEW QUESTION 77
- (Exam Topic 1)
An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

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

Answer: CE

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

NEW QUESTION 78
- (Exam Topic 1)
A third party asked a user to share a public key for secure communication. Which of the following file formats should the user choose to share the key?

A. .pfx
B. .csr
C. .pvk
D. .cer

Answer: D

Explanation:
A user should choose the .cer file format to share a public key for secure communication. A .cer file is a public key certificate that can be shared with third parties to enable secure communication.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6: Cryptography, pp. 301-302.
A public key is a cryptographic key that can be used to encrypt or verify data. A public key file is a file that contains one or more public keys in a specific format. There are different formats for public key files, depending on the application and the algorithm used. Some of the common formats are:
- .pfx: This is a file format that stores a certificate and its private and public keys. It is also known as PKCS#12 or Personal Information Exchange. It is used by some applications such as Microsoft Internet Explorer and Outlook to import and export certificates and keys.1
- .csr: This is a file format that stores a Certificate Signing Request, which is a message sent to a Certificate Authority (CA) to request a digital certificate. It contains the public key and some information about the identity of the requester. It is also known as PKCS#10 or Certification Request Syntax.2
- .pvk: This is a file format that stores a private key for Microsoft Authenticode code signing. It is used with a .spc file that contains the certificate and public key.3
- .cer: This is a file format that stores a certificate, which is a document that binds a public key to an identity. It is also known as DER or Distinguished Encoding Rules. It is used by some applications such as OpenSSL and Java to read and write certificates.4

NEW QUESTION 81
- (Exam Topic 1)
Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).

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

Answer: CD

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

NEW QUESTION 86
- (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 90
- (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:
One of the risks of using legacy software is the lack of vendor support. This means that the vendor may no longer provide security patches, software updates, or technical support for the software. This leaves the software vulnerable to new security threats and vulnerabilities that could be exploited by attackers.

NEW QUESTION 95
- (Exam Topic 1)
Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

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

Answer: A

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

NEW QUESTION 97
- (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 100
- (Exam Topic 1)
A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned tf servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

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

Answer: BF

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

Certification Exam Objectives, Exam SY0-601, 1.4 Compare and contrast network architecture and technologies.

NEW QUESTION 101
- (Exam Topic 1)
A Chief information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares Which of the following should the company implement?

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

Answer: A

Explanation:
Detailed
Data Loss Prevention (DLP) can help prevent employees from stealing data by monitoring and controlling access to sensitive data. DLP can also detect and block attempts to transfer sensitive data outside of the organization, such as via email, file transfer, or cloud storage.
References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 10: Managing Identity and Access, p. 465

NEW QUESTION 104
- (Exam Topic 1)
Which of the following involves the inclusion of code in the main codebase as soon as it is written?

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

Answer: D

Explanation:
Detailed
Continuous Integration (CI) is a practice where developers integrate code into a shared repository frequently, preferably several times a day. Each integration is verified by an automated build and automated tests. CI allows for the detection of errors early in the development cycle, thereby reducing overall development costs.

NEW QUESTION 105
- (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)
Employees at a company are receiving unsolicited text messages on their corporate cell phones. The unsolicited text messages contain a password reset Link.
Which of the attacks is being used to target the company?

A. Phishing
B. Vishing
C. Smishing
D. Spam

Answer: C

Explanation:
Smishing is a type of phishing attack which begins with an attacker sending a text message to an individual. The message contains social engineering tactics to convince the person to click on a malicious link or send sensitive information to the attacker. Criminals use smishing attacks for purposes like:
Learn login credentials to accounts via credential phishing Discover private data like social security numbers
Send money to the attacker Install malware on a phone
Establish trust before using other forms of contact like phone calls or emails
Attackers may pose as trusted sources like a government organization, a person you know, or your bank. And messages often come with manufactured urgency and time-sensitive threats. This can make it more difficult for a victim to notice a scam.
Phone numbers are easy to spoof with VoIP texting, where users can create a virtual number to send and receive texts. If a certain phone number is flagged for spam, criminals can simply recycle it and use a new one.

NEW QUESTION 111
- (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 112
- (Exam Topic 1)
A company is concerned about individuals dnvmg a car into the building to gam 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:
A bollard would work best to prevent individuals from driving a car into the building. A bollard is a short,
vertical post that can be used to block vehicles from entering a designated area. It is specifically designed to stop cars from crashing into buildings or other structures.

NEW QUESTION 116
- (Exam Topic 1)
A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:

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

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

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

Answer: C

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

NEW QUESTION 119
- (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 124
- (Exam Topic 1)
An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

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

Answer: A

Explanation:
The Service Level Agreement (SLA) is a contract between the cloud service provider and the organization that stipulates the exact requirements for the cloud provider. It outlines the level of service that the provider must deliver, including the minimum uptime percentage, support response times, and the remedies and penalties for failing to meet the agreed-upon service levels.

NEW QUESTION 129
- (Exam Topic 1)
one of the attendees starts to notice delays in the connection. and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

A. Birthday collision on the certificate key
B. DNS hacking to reroute traffic
C. Brute force to the access point
D. A SSL/TLS downgrade

Answer: D

Explanation:
The scenario describes a Man-in-the-Middle (MitM) attack where the attacker intercepts traffic and downgrades the secure SSL/TLS connection to an insecure HTTP connection. This type of attack is commonly known as SSL/TLS downgrade attack or a stripping attack. The attacker is able to see and modify the communication between the client and server.

NEW QUESTION 133
- (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 138
- (Exam Topic 1)
A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords Which of the following should the network analyst enable to meet the requirement?

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

Answer: D

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

NEW QUESTION 142
- (Exam Topic 1)
Remote workers in an organization use company-provided laptops with locally installed applications and locally stored data Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public Which of the following security solutions would mitigate the risk of future data disclosures?

A. FDE
B. TPM
C. HIDS
D. VPN

Answer: A

Explanation:
Based on these definitions, the best security solution to mitigate the risk of future data disclosures from a laptop would be FDE123. FDE would prevent unauthorized access to the data stored on the laptop even if it is stolen or lost. FDE can also use TPM to store the encryption key and ensure that only trusted software can decrypt the data3. HIDS and VPN are not directly related to data encryption, but they can provide additional security benefits by detecting intrusions and protecting network traffic respectively.

NEW QUESTION 144
- (Exam Topic 1)
A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

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

Answer: A

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

NEW QUESTION 147
- (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 148
- (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 151
- (Exam Topic 2)
A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

A. Insider threat
B. Hacktivist
C. Nation-state
D. Organized crime

Answer: D

Explanation:
Organized crime is a term that describes groups of criminals who operate in a coordinated and systematic manner to pursue illicit activities for profit. Organized crime groups often use sophisticated tools and techniques to evade law enforcement and exploit vulnerabilities in various sectors, such as finance, transportation, or healthcare. Organized crime groups may also collaborate with other criminal groups or actors to share resources, information, or expertise.
Ransomware as a service (RaaS) is an example of a business model used by organized crime groups to conduct ransomware and extortion attacks. RaaS is an arrangement between an operator, who develops and maintains the tools to power extortion operations, and an affiliate, who deploys the ransomware payload. When the affiliate conducts a successful ransomware and extortion attack, both parties profit. The RaaS model lowers the barrier to entry for attackers who may not have the skill or technical wherewithal to develop their own tools but can manage ready-made penetration testing and sysadmin tools to perform attacks12.
Insider threat is a term that describes individuals who have legitimate access to an organization's systems or data and use it for malicious purposes, such as theft, sabotage, or espionage. Insider threats may be motivated by various factors, such as greed, revenge, ideology, or coercion. Insider threats may also be unintentional, such as when an employee falls victim to phishing or social engineering.
Hacktivist is a term that describes individuals or groups who use hacking or cyberattacks to promote a political or social cause. Hacktivists may target governments, corporations, or other entities that they perceive as oppressive, corrupt, or unethical. Hacktivists may also use cyberattacks to expose information, disrupt services, or deface websites.
Nation-state is a term that describes a sovereign state that has a centralized government and a defined territory. Nation-state actors are individuals or groups who conduct cyberattacks on behalf of or with the support of a nation-state. Nation-state actors may target other states, organizations, or individuals for various reasons, such as espionage, sabotage, influence, or retaliation.

NEW QUESTION 154
- (Exam Topic 2)
Which of the following can reduce vulnerabilities by avoiding code reuse?

A. Memory management
B. Stored procedures
C. Normalization
D. Code obfuscation

Answer: A

Explanation:
Memory management is a technique that can allocate and deallocate memory for applications and processes. Memory management can reduce vulnerabilities by avoiding code reuse, which is a technique that exploits a memory corruption vulnerability to execute malicious code that already exists in memory. Memory management can prevent code reuse by implementing features such as address space layout randomization (ASLR), data execution prevention (DEP), or stack canaries.

NEW QUESTION 155
- (Exam Topic 2)
An analyst is working on an email security incident in which the target opened an attachment containing a worm. The analyst wants to Implement mitigation techniques to prevent further spread. Which of the
following is the best course of action for the analyst to take?

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

Answer: D

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

NEW QUESTION 156
- (Exam Topic 2)
A company recently experienced a significant data loss when proprietary information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the best mitigation strategy to prevent this from happening in the future?

A. User training
B. CAsB
C. MDM
D. EDR

Answer: C

Explanation:
MDM stands for mobile device management, which is a solution that allows organizations to manage and secure mobile devices used by employees. MDM can help prevent data loss and leakage by enforcing policies and restrictions on the devices, such as encryption, password, app installation, remote wipe, and so on. MDM can also monitor and audit the device activity and compliance status. MDM can be the best mitigation strategy to prevent data leakage from an employee's COPE tablet via cloud storage, as it can block or limit the access to cloud services, or apply data protection measures such as containerization or encryption.
References:
- https://www.blackberry.com/us/en/solutions/corporate-owned-personally-enabled
- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/mobile-device-management/

NEW QUESTION 158
- (Exam Topic 2)
Sales team members have been receiving threatening voicemail messages and have reported these incidents to the IT security team. Which of the following would be MOST appropriate for the IT security team to analyze?

A. Access control
B. Syslog
C. Session Initiation Protocol traffic logs
D. Application logs

Answer: B

Explanation:
Syslogs are log files that are generated by devices on the network and contain information about network
activity, including user logins, device connections, and other events. By analyzing these logs, the IT security team can identify the source of the threatening voicemail messages and take the necessary steps to address the issue

NEW QUESTION 162
- (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 166
- (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 170
- (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 173
- (Exam Topic 2)
A security analyst receives an alert that indicates a user's device is displaying anomalous behavior The analyst suspects the device might be compromised Which of the following should the analyst to first?

A. Reboot the device
B. Set the host-based firewall to deny an incoming connection
C. Update the antivirus definitions on the device
D. Isolate the device

Answer: D

Explanation:
Isolating the device is the first thing that a security analyst should do if they suspect that a user’s device might be compromised. Isolating the device means disconnecting it from the network or placing it in a separate network segment to prevent further communication with potential attackers or malicious hosts. Isolating the device can help contain the incident, limit the damage or data loss, preserve the evidence, and facilitate the investigation and remediation.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://resources.infosecinstitute.com/topic/incident-response-process/

NEW QUESTION 178
- (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 182
- (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 184
- (Exam Topic 2)
Which Of the following is a primary security concern for a setting up a BYOD program?

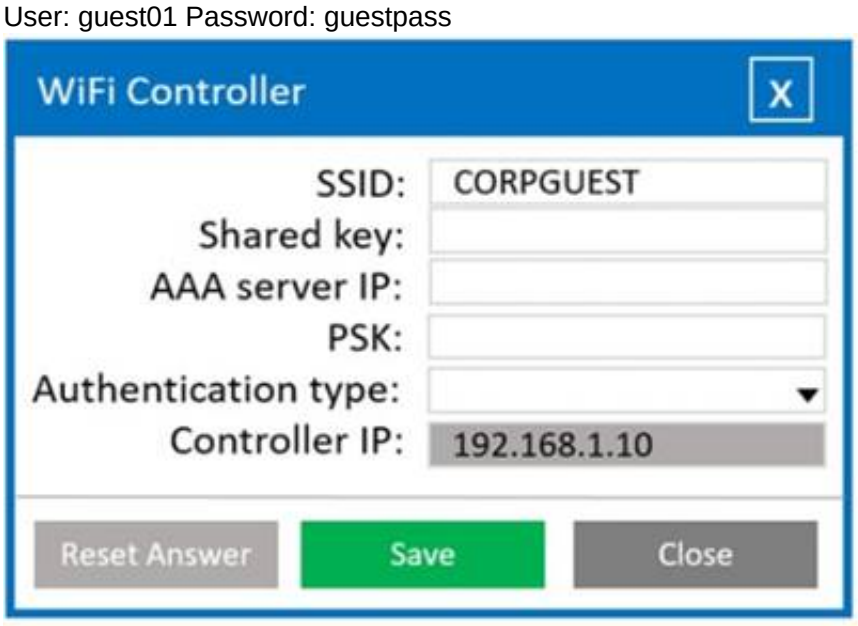
A. End of life
B. Buffer overflow
C. VM escape
D. Jailbreaking

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 189
- (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 191
- (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 192
- (Exam Topic 2)
A security team discovered a large number of company-issued devices with non-work-related software installed. Which of the following policies would most likely contain language that would prohibit this activity?

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

Answer: C

Explanation:
AUP stands for acceptable use policy, which is a document that defines the rules and guidelines for using an organization’s network, systems, devices, and

resources. An AUP typically covers topics such as authorized and unauthorized activities, security requirements, data protection, user responsibilities, and consequences for violations. An AUP can help prevent non-work-related software installation on company-issued devices by clearly stating what types of software are allowed or prohibited, and what actions will be taken if users do not comply with the policy.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.techopedia.com/definition/2471/acceptable-use-policy-aup

NEW QUESTION 194
- (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 195
- (Exam Topic 2)
During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the ‘company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

A. Federation
B. Identity proofing
C. Password complexity
D. Default password changes
E. Password manager
F. Open authentication

Answer: AF

Explanation:
Federation is an access management concept that allows users to authenticate once and access multiple applications or services that trust the same identity provider. Open authentication is a standard protocol that enables federation by allowing users to use their existing credentials from one service to access another service. The company is most likely using federation and open authentication to safeguard intranet accounts and grant access to multiple sites based on a user’s intranet account. For example, the company could use an identity provider such as Azure AD or Keycloak to manage the user identities and credentials for the intranet account, and then use open authentication to allow the users to access other company-owned websites without having to log in again. References:
- https://www.keycloak.org/
- https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/whatis-fed

NEW QUESTION 196
- (Exam Topic 2)
A small, local company experienced a ransomware attack. The company has one web-facing server and a few workstations. Everything is behind an ISP firewall. A single web-facing server is set up on the router to forward all ports so that the server is viewable from the internet. The company uses an older version of third-party software to manage the website. The assets were never patched. Which of the following should be done to prevent an attack like this from happening again? (Select three).

A. Install DLP software to prevent data loss.
B. Use the latest version of software.
C. Install a SIEM device.
D. Implement MDM.
E. Implement a screened subnet for the web server.
F. Install an endpoint security solution.
G. Update the website certificate and revoke the existing ones.
H. Deploy additional network sensors.

Answer: BEF

NEW QUESTION 198
- (Exam Topic 2)
Which Of the following vulnerabilities is exploited an attacker Overwrite a reg-ister with a malicious address that changes the execution path?

A. VM escape
B. SQL injection
C. Buffer overflow
D. Race condition

Answer: C

Explanation:
A buffer overflow is a type of vulnerability that occurs when an attacker sends more data than a buffer can hold, causing the excess data to overwrite adjacent memory locations such as registers. It can allow an attacker to overwrite a register with a malicious address that changes the execution path and executes arbitrary code on the target system

NEW QUESTION 203
- (Exam Topic 2)
An analyst is working on an investigation with multiple alerts for multiple hosts. The hosts are showing signs of being compromised by a fast-spreading worm. Which of the following should be the next step in order to stop the spread?

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

Answer: D

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

NEW QUESTION 206
- (Exam Topic 2)
Security engineers are working on digital certificate management with the top priority of making administration easier. Which of the following certificates is the best option?

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

Answer: B

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

NEW QUESTION 210
- (Exam Topic 2)
A security team will be outsourcing several key functions to a third party and will require that:
• Several of the functions will carry an audit burden.
• Attestations will be performed several times a year.
• Reports will be generated on a monthly basis.
Which of the following BEST describes the document that is used to define these requirements and stipulate how and when they are performed by the third party?

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

Answer: C

Explanation:
A service level agreement (SLA) is a contract between a service provider and a customer that outlines the services that are to be provided and the expected levels of performance. It is used to define the requirements for the service, including any attestations and reports that must be generated, and the timescales in which these must be completed. It also outlines any penalties for failing to meet these requirements. SLAs are essential for ensuring that third-party services are meeting the agreed upon performance levels.
Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968
CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide by Darril Gibson https://www.amazon.com/CompTIA-Security-Certified-Ahead-SY0-601/dp/1260117558
Note: SLA is the best document that is used to define these requirements and stipulate how and when they are performed by the third party.

NEW QUESTION 215
- (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 219
- (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 220
- (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 224
- (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 229
- (Exam Topic 2)
A company is moving to new location. The systems administrator has provided the following server room requirements to the facilities staff:
- Consistent power levels in case of brownouts or voltage spikes
- A minimum of 30 minutes runtime following a power outage
- Ability to trigger graceful shutdowns of critical systems

Which of the following would BEST meet the requirements?

A. Maintaining a standby, gas-powered generator
B. Using large surge suppressors on computer equipment
C. Configuring managed PDUs to monitor power levels
D. Deploying an appropriately sized, network-connected UPS device

Answer: D

Explanation:
A UPS (uninterruptible power supply) device is a battery backup system that can provide consistent power levels in case of brownouts or voltage spikes. It can also provide a minimum of 30 minutes runtime following a power outage, depending on the size and load of the device. A network-connected UPS device can also communicate with critical systems and trigger graceful shutdowns if the battery level is low or the power is not restored.

NEW QUESTION 230
- (Exam Topic 2)
A security operations center wants to implement a solution that can execute files to test for malicious activity. The solution should provide a report of the files' activity against known threats.
Which of the following should the security operations center implement?

A. theHarvester
B. Nessus
C. Cuckoo
D. Sn1per

Answer: C

Explanation:
Cuckoo is a sandbox that is specifically written to run programs inside and identify any malware. A sandbox is a virtualized environment that isolates the program from the rest of the system and monitors its behavior. Cuckoo can analyze files of various types, such as executables, documents, URLs, and more. Cuckoo can provide a report of the files' activity against known threats, such as network traffic, file operations, registry changes, API calls, and so on.
A security operations center can implement Cuckoo to execute files to test for malicious activity and generate a report of the analysis. Cuckoo can help the security operations center to detect and prevent malware infections, investigate incidents, and perform threat intelligence.

NEW QUESTION 233
- (Exam Topic 2)
A security administrator examines the ARP table of an access switch and sees the following output:

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

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

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

Answer: C

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

NEW QUESTION 238
- (Exam Topic 2)
Users report access to an application from an internal workstation is still unavailable to a specific server, even after a recent firewall rule implementation that was requested for this access. ICMP traffic is successful between the two devices. Which of the following tools should the security analyst use to help identify if the traffic is being blocked?

A. nmap
B. tracert
C. ping
D. ssh

Answer: A

Explanation:
Tracert is a command-line tool that shows the route that packets take to reach a destination on a network1. It also displays the time it takes for each hop along the way1. By using tracert, you can see if there is a router or firewall that is blocking or slowing down the traffic between the internal workstation and the specific server1.

NEW QUESTION 242
- (Exam Topic 2)
Security analysts have noticed the network becomes flooded with malicious packets at specific times of the day. Which of the following should the analysts use to investigate this issue?

A. Web metadata
B. Bandwidth monitors
C. System files
D. Correlation dashboards

Answer: D

Explanation:
Correlation dashboards are tools that allow security analysts to monitor and analyze multiple sources of data and events in real time. They can help identify patterns, trends, anomalies, and threats by correlating different types of data and events, such as network traffic, logs, alerts, and incidents. Correlation dashboards can help investigate network flooding by showing the source, destination, volume, and type of malicious packets and their impact on the network performance and availability. References:
https://www.comptia.org/blog/what-is-a-correlation-dashboard

NEW QUESTION 245
- (Exam Topic 2)
An audit identified Pll being utilized in the development environment of a crit-ical application. The Chief Privacy Officer (CPO) is adamant that this data must be removed: however, the developers are concerned that without real data they cannot perform functionality tests and search for specific data. Which of the following should a security professional implement to best satisfy both the CPOs and the development team's requirements?

A. Data purge
B. Data encryption
C. Data masking
D. Data tokenization

Answer: D

Explanation:
Data tokenization is a technique of replacing sensitive data with non-sensitive substitutes called tokens that have no intrinsic value or meaning. It can satisfy both the CPO’s and the development team’s requirements by removing personally identifiable information (PII) from the development environment of a critical application while preserving the functionality and format of the data for testing purposes.

NEW QUESTION 247
- (Exam Topic 2)
Which of the following secure application development concepts aims to block verbose error messages from being shown in a user’s interface?

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

Answer: D

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

NEW QUESTION 250
- (Exam Topic 2)
Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP

B. CSR
C. CA
D. CRC

Answer: A

Explanation:
Online Certificate Status Protocol (OCSP) is used to validate a certificate when it is presented to a user. OCSP is a protocol that allows a client or browser to query the status of a certificate from an OCSP responder, which is a server that maintains and provides the revocation status of certificates issued by a certificate authority (CA). OCSP can help to verify the authenticity and validity of a certificate and prevent the use of revoked or expired certificates. References:
https://www.comptia.org/blog/what-is-ocsp
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 251
- (Exam Topic 2)
A company recently completed the transition from data centers to the cloud. Which of the following solutions will best enable the company to detect security threats in applications that run in isolated environments within the cloud environment?

A. Security groups
B. Container security
C. Virtual networks
D. Segmentation

Answer: B

Explanation:
Container security is a solution that can enable the company to detect security threats in applications that run in isolated environments within the cloud environment. Containers are units of software that package code and dependencies together, allowing applications to run quickly and reliably across different computing environments. Container security involves securing the container images, the container runtime, and the container orchestration platforms. Container security can help prevent unauthorized access, data breaches, malware infections, or denial-of-service attacks on the applications running in containers.
References: 1
CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3 : Summarize secure application development, deployment, and automation concepts 2
CompTIA Security+
Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the
importance of embedded and specialized systems security 3
https://www.comptia.org/blog/what-is-container-security

NEW QUESTION 252
- (Exam Topic 2)
Several users have been violating corporate security policy by accessing inappropriate Sites on
corporate-issued mobile devices while off campus. The senior leadership team wants all mobile devices to be hardened with controls that:
- Limit the sites that can be accessed
- Only allow access to internal resources while physically on campus.
- Restrict employees from downloading images from company email

Whip of the following controls would best address this situation? (Select two).

A. MFA
B. GPS tagging
C. Biometric authentication
D. Content management
E. Geofencing
F. Screen lock and PIN requirements

Answer: DE

Explanation:
Content management is a security control that can limit the sites that can be accessed by corporate-issued mobile devices. It can also restrict employees from downloading images from company email by filtering or blocking certain types of content1. Geofencing is a security control that can only allow access to internal resources while physically on campus. It can use GPS or other location services to define a virtual boundary around a physical area and enforce policies based on the device’s location2.
References:
1:
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardeni
2: https://www.makeuseof.com/how-to-secure-your-content-management-system/

NEW QUESTION 255
- (Exam Topic 2)
Which of the following can be used by an authentication application to validate a user's credentials without the need to store the actual sensitive data?

A. Salt string
B. Private Key
C. Password hash
D. Cipher stream

Answer: C

Explanation:
Password hash is a method of storing a user’s credentials without the need to store the actual sensitive data. A password hash is a one-way function that

transforms the user's password into a fixed-length string of characters that cannot be reversed. The authentication application can then compare the password hash with the stored hash to validate the user's credentials without revealing the original password. References: 1
CompTIA Security+ Certification Exam Objectives, page 15, Domain 3.0: Implementation, Objective 3.5:
Implement secure authentication mechanisms 2
CompTIA Security+ Certification Exam Objectives, page 16,
Domain 3.0: Implementation, Objective 3.6: Implement identity and account management best practices 3
https://www.comptia.org/blog/what-is-password-hashing

NEW QUESTION 258
- (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 263
- (Exam Topic 2)
Which of the following security controls s sed to isolate a section of the network and its externally available resources from the internal corporate network in order to reduce the number of
possible attacks?

A. Faraday cages
B. Air gap
C. Vaulting
D. Proximity readers

Answer: B

Explanation:
An air gap is a security measure that physically isolates a section of the network from any other network or device that could compromise its security. An air gap prevents any unauthorized access, data leakage, or malware infection through network connections, such as Ethernet cables, wireless signals, or Bluetooth devices. An air gap can be used to protect sensitive or critical systems and data from external threats, such as hackers, spies, or cyberattacks.

NEW QUESTION 268
- (Exam Topic 2)
A security administrator is integrating several segments onto a single network. One of the segments, which includes legacy devices, presents a significant amount of risk to the network.
Which of the following would allow users to access to the legacy devices without compromising the security of the entire network?

A. NIDS
B. MAC filtering
C. Jump server
D. IPSec
E. NAT gateway

Answer: C

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

NEW QUESTION 272
- (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 277
- (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 279
- (Exam Topic 2)
An audit report indicates multiple suspicious attempts to access company resources were made. These attempts were not detected by the company. Which of the following would be the best solution to implement on the company's network?

A. Intrusion prevention system
B. Proxy server
C. Jump server
D. Security zones

Answer: A

Explanation:
An intrusion prevention system (IPS) is the best solution to implement on the company's network to detect and prevent suspicious attempts to access company resources. An IPS is a network security technology that continuously monitors network traffic for malicious or anomalous activity and takes automated actions to block or mitigate it. An IPS can also alert the system administrators of any potential threats and provide detailed logs and reports of the incidents. An IPS can help the company to improve its security posture and prevent data breaches, unauthorized access, or denial-of-service attacks. References:
- https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
- https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips

NEW QUESTION 284
- (Exam Topic 2)
A security analyst needs to recommend a solution that will allow current Active Directory accounts and groups to be used for access controls on both network and remote-access devices. Which of the
following should the analyst recommend? (Select two).

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

Answer: BE

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

NEW QUESTION 285
- (Exam Topic 2)
A security engineer updated an application on company workstations. The application was running before the update, but it is no longer launching successfully. Which of the following most likely needs to be updated?

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

Answer: D

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

NEW QUESTION 286
- (Exam Topic 2)
An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the most acceptable?

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

Answer: A

Explanation:
SED stands for Self-Encrypting Drive, which is a type of hard drive that automatically encrypts and decrypts data using a built-in hardware encryption engine1. SEDs do not require any additional software or configuration, and they do not affect the performance or usability of the laptop2. SEDs also have a feature called Instant Secure Erase, which allows the user to quickly and securely wipe the data on the drive by deleting the encryption key1.

NEW QUESTION 291
- (Exam Topic 2)
A security administrator is managing administrative access to sensitive systems with the following requirements:
• Common login accounts must not be used for administrative duties.
• Administrative accounts must be temporal in nature.
• Each administrative account must be assigned to one specific user.
• Accounts must have complex passwords.
" Audit trails and logging must be enabled on all systems.
Which of the following solutions should the administrator deploy to meet these requirements? (Give explanation and References from CompTIA Security+ SY0-601 Official Text Book and Resources)

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

Answer: C

Explanation:
PAM is a solution that enables organizations to securely manage users' accounts and access to sensitive systems. It allows administrators to create unique and complex passwords for each user, as well as assign each account to a single user for administrative duties. PAM also provides audit trails and logging capabilities, allowing administrators to monitor user activity and ensure that all systems are secure. According to the CompTIA Security+ SY0-601 Course Book, “PAM is the most comprehensive way to control and monitor privileged accounts”.

NEW QUESTION 294
- (Exam Topic 2)
An employee's laptop was stolen last month. This morning, the was returned by the A cyberrsecurity analyst retrieved laptop and has since cybersecurity incident checklist Four incident handlers are responsible for executing the checklist. Which of the following best describes the process for evidence collection assurance?

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

Answer: B

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

NEW QUESTION 296
- (Exam Topic 2)
A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following
• The manager of the accounts payable department is using the same password across multiple external websites and the corporate account

• One of the websites the manager used recently experienced a data breach.
• The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country.
Which of the following attacks has most likely been used to compromise the manager's corporate account?

A. Remote access Trojan
B. Brute-force
C. Dictionary
D. Credential stuffing
E. Password spraying

Answer: D

Explanation:
Credential stuffing is a type of attack that involves using stolen or leaked usernames and passwords from one website or service to gain unauthorized access to other websites or services that use the same credentials. It can exploit the common practice of reusing passwords across multiple accounts. It is the most likely attack tha has been used to compromise the manager’s corporate account, given that the manager is using the same password across multiple external websites and the corporate account, and one of the websites recently experienced a data breach.

NEW QUESTION 301
- (Exam Topic 2)
A help desk technician receives a phone call from someone claiming to be a part of the organization's cybersecurity incident response team. The caller asks the technician to verify the network's internal firewall IP address. Which of the following is the technician's best course of action?

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

Answer: C

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

NEW QUESTION 305
- (Exam Topic 2)
Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

A. Compensating control
B. Network segmentation
C. Transfer of risk
D. SNMP traps

Answer: A

Explanation:
A compensating control is a type of security control that is implemented in lieu of a recommended security measure that is deemed too difficult or impractical to implement at the present time. A compensating control must provide equivalent or comparable protection for the system or network and meet the intent and rigor of the original security requirement. An example of a compensating control is using a host-based firewall on a legacy Linux system to allow connections from only specific internal IP addresses, as it can provide a similar level of defense as a network firewall that may not be compatible with the system. References:
- https://www.techtarget.com/whatis/definition/compensating-control
- https://reciprocity.com/resources/whats-the-difference-between-compensating-controls-and-mitigating-co

NEW QUESTION 308
- (Exam Topic 2)
Which of the following describes business units that purchase and implement scripting software without approval from an organization's technology Support staff?

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

Answer: A

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

NEW QUESTION 313

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

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

Answer: C

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

NEW QUESTION 315
- (Exam Topic 2)
A company was recently breached Pan of the company's new cybersecurity strategy is to centralize? the togs horn all security devices Which of the following components forwards the logs to a central source?

A. Log enrichment
B. Log queue
C. Log parser
D. Log collector

Answer: D

Explanation:
A log collector is a component that forwards the logs from all security devices to a central source. A log collector can be a software tool or a hardware appliance that collects logs from various sources, such as firewalls, routers, servers, applications, or endpoints. A log collector can also perform functions such as log filtering, parsing, aggregation, normalization, and enrichment. A log collector can help centralize logging by sending the collected logs to a central log server or a security information and event management (SIEM) system for further analysis and correlation.
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://geekflare.com/open-source-centralized-logging/

NEW QUESTION 319
- (Exam Topic 2)
Which of the following would be the best resource for a software developer who is looking to improve secure coding practices for web applications?

A. OWASP
B. Vulnerability scan results
C. NIST CSF
D. Third-party libraries

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 can be the best resource for a software developer who is looking to improve secure coding practices for web applications by offering various tools, frameworks, standards, cheat sheets, testing guides, etc., that cover various aspects of web application security development and testing

NEW QUESTION 321
- (Exam Topic 2)
A security analyst needs to implement security features across smartphones. laptops, and tablets. Which of the following would be the most effective across heterogeneous platforms?

A. Enforcing encryption
B. Deploying GPOs
C. Removing administrative permissions
D. Applying MDM software

Answer: D

Explanation:
MDM stands for Mobile Device Management, which is a software solution that can manage and secure smartphones, laptops, tablets and other mobile devices across heterogeneous platforms. MDM can enforce security features such as encryption, password policies, remote wipe, device tracking, app control and more. MDM can also monitor and update the devices remotely and provide reports and alerts on their status. MDM is the most effective solution to implement security features across heterogeneous platforms, as it can provide centralized and consistent management of various types of devices. Verified References:
- Security+ (Plus) Certification | CompTIA IT Certifications
https://www.comptia.org/certifications/security (See Domain 3: Architecture and Design, Objective 3.4: Given a scenario, implement secure systems design.)
- CompTIA Security+ 601 - Infosec
https://www.infosecinstitute.com/wp-content/uploads/2021/03/CompTIA-Security-eBook.pdf (See Security+: 5 in-demand cybersecurity skills, Implementation)
- Certification Security+ | CompTIA https://www.comptia.org/landing/securityplus/index.html (See Exam Objectives)

NEW QUESTION 325

- (Exam Topic 2)
After installing a patch On a security appliance. an organization realized a massive data exfiltration occurred. Which Of the following describes the incident?

A. Supply chain attack
B. Ransomware attack
C. Cryptographic attack
D. Password attack

Answer: A

Explanation:
A supply chain attack is a type of attack that involves compromising a trusted third-party provider or vendor and using their products or services to deliver malware or gain access to the target organization. The attacker can exploit the trust and dependency that the organization has on the provider or vendor and bypass their security controls. In this case, the attacker may have tampered with the patch for the security appliance and used it to exfiltrate data from the organization.

NEW QUESTION 327
.....

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/