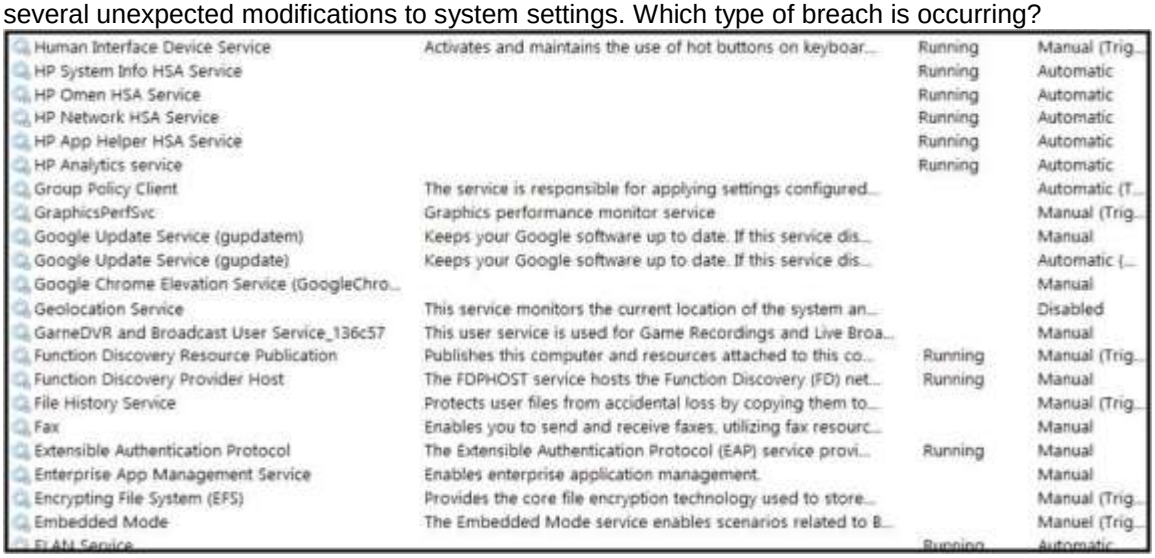
**QUESTION 106**
An analyst wants to upload an infected file containing sensitive information to a hybrid-analysis sandbox. According to the NIST.SP 800-150 guide to cyber threat information sharing, what is the analyst required to do before uploading the file to safeguard privacy?

A. Verify hash integrity.
B. Remove all personally identifiable information.
C. Ensure the online sandbox is GDPR compliant.
D. Lock the file to prevent unauthorized access.

**Answer:** B

**QUESTION 107**
Refer to the exhibit. An engineer received multiple reports from employees unable to log into systems with the error: The Group Policy Client service failed to logon ?Access is denied. Through further analysis, the engineer discovered several unexpected modifications to system settings. Which type of breach is occurring?



| | | | |
|---|---|---|---|
| Human Interface Device Service | Activates and maintains the use of hot buttons on keyboar... | Running | Manual (Trig... |
| HP System Info HSA Service | | Running | Automatic |
| HP Omen HSA Service | | Running | Automatic |
| HP Network HSA Service | | Running | Automatic |
| HP App Helper HSA Service | | Running | Automatic |
| HP Analytics service | | Running | Automatic |
| Group Policy Client | The service is responsible for applying settings configured... | | Automatic (T... |
| GraphicsPerfSvc | Graphics performance monitor service | | Manual (Trig... |
| Google Update Service (gupdatem) | Keeps your Google software up to date. If this service dis... | | Manual |
| Google Update Service (gupdate) | Keeps your Google software up to date. If this service dis... | | Automatic (... |
| Google Chrome Elevation Service (GoogleChro... | | | Manual |
| Geolocation Service | This service monitors the current location of the system an... | | Disabled |
| GarneDVR and Broadcast User Service_136c57 | This user service is used for Game Recordings and Live Broa... | | Manual |
| Function Discovery Resource Publication | Publishes this computer and resources attached to this co... | Running | Manual (Trig... |
| Function Discovery Provider Host | The FDPHOST service hosts the Function Discovery (FD) net... | Running | Manual |
| File History Service | Protects user files from accidental loss by copying them to... | | Manual (Trig... |
| Fax | Enables you to send and receive faxes, utilizing fax resourc... | | Manual |
| Extensible Authentication Protocol | The Extensible Authentication Protocol (EAP) service provi... | Running | Manual |
| Enterprise App Management Service | Enables enterprise application management. | | Manual |
| Encrypting File System (EFS) | Provides the core file encryption technology used to store... | | Manual (Trig... |
| Embedded Mode | The Embedded Mode service enables scenarios related to E... | | Manual (Trig... |
| ELAN Service | | Running | Automatic |

A. malware break
B. data theft
C. elevation of privileges
D. denial-of-service

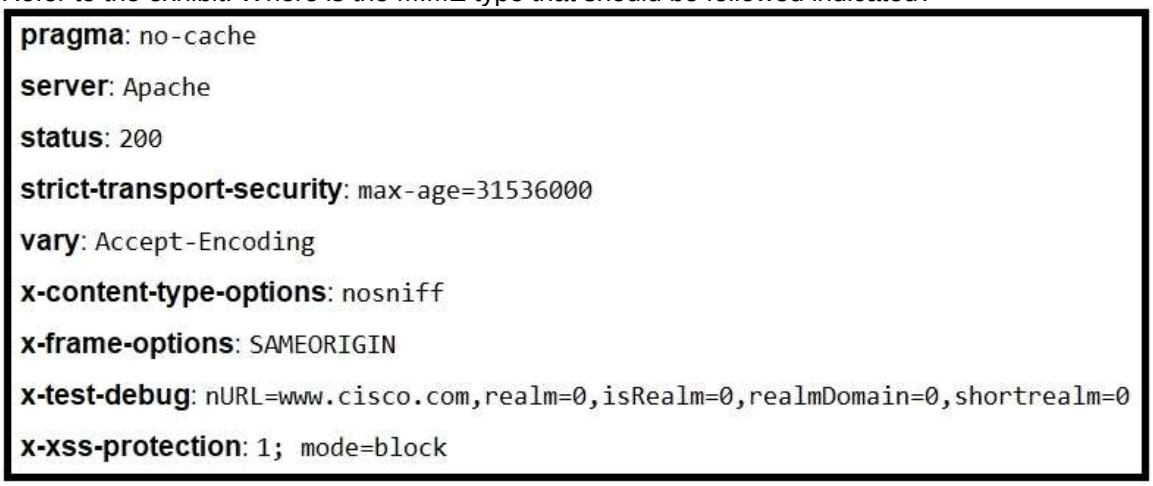
**Answer:** C

**QUESTION 108**
What is needed to assess risk mitigation effectiveness in an organization?

A. analysis of key performance indicators
B. compliance with security standards
C. cost-effectiveness of control measures
D. updated list of vulnerable systems

**Answer:** C

**QUESTION 109**
Refer to the exhibit. Where is the MIME type that should be followed indicated?




A. x-test-debug
B. strict-transport-security
C. x-xss-protection
D. x-content-type-options

**Answer:** A

**QUESTION 110**
Refer to the exhibit. Based on the detected vulnerabilities, what is the next recommended mitigation step?

| Severity | Name | Family | Count | CVSS |
|---|---|---|---|---|
| Critical | Bash Incomplete Fix Remote Code Execution Vulnerability | Gain a shell remotely | 3 | 10 |
| Critical | Bash Remote Code Execution (Shellshock) | Gain a shell remotely | 1 | 10 |
| Critical | CentOS 5 / 6 : samba (CESA-2012:0465) | CentOS Local Security Checks | 1 | 7.4 |
| Critical | Rexecd Service Detection | Service detection | 1 | 5.9 |
| High | Mozilla Foundation Unsupported Application | MacOS X Local Security Checks | 2 | 10 |
| High | SMB Signing Disabled | Misc | 1 | 7 |
| Medium | SSL Certificate Cannot Be Trusted | General | 1 | 6.5 |

A. Evaluate service disruption and associated risk before prioritizing patches.
B. Perform root cause analysis for all detected vulnerabilities.
C. Remediate all vulnerabilities with descending CVSS score order.
D. Temporarily shut down unnecessary services until patch deployment ends.

**Answer:** B

**QUESTION 111**
An engineer received an incident ticket of a malware outbreak and used antivirus and malware removal tools to eradicate the threat. The engineer notices that abnormal processes are still occurring in the system and determines that manual intervention is needed to clean the infected host and restore functionality. What is the next step the engineer should take to complete this playbook step?

A. Scan the network to identify unknown assets and the asset owners.
B. Analyze the components of the infected hosts and associated business services.
C. Scan the host with updated signatures and remove temporary containment.
D. Analyze the impact of the malware and contain the artifacts.

**Answer:** B

**QUESTION 112**
The SIEM tool informs a SOC team of a suspicious file. The team initializes the analysis with an automated sandbox tool, sets up a controlled laboratory to examine the malware specimen, and proceeds with behavioral analysis. What is the next step in the malware analysis process?

A. Perform static and dynamic code analysis of the specimen.
B. Unpack the specimen and perform memory forensics.
C. Contain the subnet in which the suspicious file was found.
D. Document findings and clean-up the laboratory.

**Answer:** B

**QUESTION 113**
A logistic company must use an outdated application located in a private VLAN during the migration to new

technologies. The IPS blocked and reported an unencrypted communication. Which tuning option should be applied to IPS?

A. Allow list only authorized hosts to contact the application's IP at a specific port.
B. Allow list HTTP traffic through the corporate VLANS.
C. Allow list traffic to application's IP from the internal network at a specific port.
D. Allow list only authorized hosts to contact the application's VLAN.

**Answer:** D

**QUESTION 114**
A company recently started accepting credit card payments in their local warehouses and is undergoing a PCI audit. Based on business requirements, the company needs to store sensitive authentication data for 45 days. How must data be stored for compliance?

A. post-authorization by non-issuing entities if there is a documented business justification
B. by entities that issue the payment cards or that perform support issuing services
C. post-authorization by non-issuing entities if the data is encrypted and securely stored
D. by issuers and issuer processors if there is a legitimate reason

**Answer:** C

**QUESTION 115**
A security engineer discovers that a spreadsheet containing confidential information for nine of their employees was fraudulently posted on a competitor's website. The spreadsheet contains names, salaries, and social security numbers. What is the next step the engineer should take in this investigation?

A. Determine if there is internal knowledge of this incident.
B. Check incoming and outgoing communications to identify spoofed emails.
C. Disconnect the network from Internet access to stop the phishing threats and regain control.
D. Engage the legal department to explore action against the competitor that posted the spreadsheet.

**Answer:** D

**QUESTION 116**
An engineer notices that every Sunday night, there is a two-hour period with a large load of network activity. Upon further investigation, the engineer finds that the activity is from locations around the globe outside the organization's service are

A. What are the next steps the engineer must take?
B. Assign the issue to the incident handling provider because no suspicious activity has been observed during business hours.
C. Review the SIEM and FirePower logs, block all traffic, and document the results of calling the call center.
D. Define the access points using StealthWatch or SIEM logs, understand services being offered during the hours in Question:, and cross-correlate other source events.
E. Treat it as a false positive, and accept the SIEM issue as valid to avoid alerts from triggering on weekends.

**Answer:** A

**QUESTION 117**
An organization had an incident with the network availability during which devices unexpectedly malfunctioned. An engineer is investigating the incident and found that the memory pool buffer usage reached a peak before the malfunction. Which action should the engineer take to prevent this issue from reoccurring?

A. Disable memory limit.
B. Disable CPU threshold trap toward the SNMP server.
C. Enable memory tracing notifications.
D. Enable memory threshold notifications.

**Answer:** D

**QUESTION 118**
A SOC analyst detected a ransomware outbreak in the organization coming from a malicious email attachment. Affected parties are notified, and the incident response team is assigned to the case. According to the NIST incident response handbook, what is the next step in handling the incident?

A. Create a follow-up report based on the incident documentation.
B. Perform a vulnerability assessment to find existing vulnerabilities.
C. Eradicate malicious software from the infected machines.
D. Collect evidence and maintain a chain-of-custody during further analysis.

**Answer:** D

**QUESTION 119**
A security manager received an email from an anomaly detection service, that one of their contractors has downloaded 50 documents from the company's confidential document management folder using a company- owned asset al039-ice-4ce687TL0500. A security manager reviewed the content of downloaded documents and noticed that the data affected is from different departments. What are the actions a security manager should take?

A. Measure confidentiality level of downloaded documents.
B. Report to the incident response team.
C. Escalate to contractor's manager.
D. Communicate with the contractor to identify the motives.

**Answer:** B

**QUESTION 120**
An engineer detects an intrusion event inside an organization's network and becomes aware that files that contain personal data have been accessed. Which action must be taken to contain this attack?

A. Disconnect the affected server from the network.
B. Analyze the source.
C. Access the affected server to confirm compromised files are encrypted.
D. Determine the attack surface.

**Answer:** C

**QUESTION 121**
The network operations center has identified malware, created a ticket within their ticketing system, and assigned the case to the SOC with high-level information. A SOC analyst was able to stop the malware from spreading and identified the attacking host. What is the next step in the incident response workflow?

A. eradication and recovery
B. post-incident activity
C. containment
D. detection and analysis

**Answer:** A

**QUESTION 122**
A SOC engineer discovers that the organization had three DDOS attacks overnight. Four servers are reported offline, even though the hardware seems to be working as expected. One of the offline servers is affecting the pay system reporting times. Three employees, including executive management, have reported ransomware on their laptops. Which steps help the engineer understand a comprehensive overview of the incident?

A. Run and evaluate a full packet capture on the workloads, review SIEM logs, and define a root cause.
B. Run and evaluate a full packet capture on the workloads, review SIEM logs, and plan mitigation steps.
C. Check SOAR to learn what the security systems are reporting about the overnight events, research the attacks, and plan mitigation step.
D. Check SOAR to know what the security systems are reporting about the overnight events, review the threat vectors, and define a root cause.

**Answer:** D

**QUESTION 123**
Which action should be taken when the HTTP response code 301 is received from a web application?

A. Update the cached header metadata.
B. Confirm the resource's location.
C. Increase the allowed user limit.
D. Modify the session timeout setting.

**Answer:** A

**QUESTION 124**
Employees receive an email from an executive within the organization that summarizes a recent security breach and requests that employees verify their credentials through a provided link. Several employees report the email as suspicious, and a security analyst is investigating the reports. Which two steps should the analyst take to begin this investigation? (Choose two.)

A. Evaluate the intrusion detection system alerts to determine the threat source and attack surface.
B. Communicate with employees to determine who opened the link and isolate the affected assets.
C. Examine the firewall and HIPS configuration to identify the exploited vulnerabilities and apply recommended mitigation.
D. Review the mail server and proxy logs to identify the impact of a potential breach.
E. Check the email header to identify the sender and analyze the link in an isolated environment.

**Answer:** CE

**QUESTION 125**
A SOC team is investigating a recent, targeted social engineering attack on multiple employees. Cross- correlated log analysis revealed that two hours before the attack, multiple assets received requests on TCP port 79. Which action should be taken by the SOC team to mitigate this attack?

A. Disable BIND forwarding from the DNS server to avoid reconnaissance.
B. Disable affected assets and isolate them for further investigation.
C. Configure affected devices to disable NETRJS protocol.
D. Configure affected devices to disable the Finger service.

**Answer:** D