

CS0-002 Dumps

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

<https://www.certleader.com/CS0-002-dumps.html>



NEW QUESTION 1

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 2

After receiving reports latency, a security analyst performs an Nmap scan and observes the following output:

```
Port      State  Service  Version
80/tcp    open   http     Apache httpd 2.2.14
111/udp   open   rpcbind
443/tcp   filtered https    Apache httpd 2.2.14
2222/tcp  open   ssh      OpenSSH 5.3p1 Debian
3306/tcp  open   mysql    5.5.40-0ubuntu0.14.1
```

Which of the following suggests the system that produced output was compromised?

- A. Secure shell is operating of compromise on this system.
- B. There are no indicators of compromise on this system.
- C. MySQL services is identified on a standard PostgreSQL port.
- D. Standard HTP is open on the system and should be closed.

Answer: B

NEW QUESTION 3

A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentiality protection. Which of the following is the BEST technical security control to mitigate this risk?

- A. Switch to RADIUS technology
- B. Switch to TACACS+ technology.
- C. Switch to 802.1X technology
- D. Switch to the WPA2 protocol.

Answer: B

NEW QUESTION 4

Which of the following is the MOST important objective of a post-incident review?

- A. Capture lessons learned and improve incident response processes
- B. Develop a process for containment and continue improvement efforts
- C. Identify new technologies and strategies to remediate
- D. Identify a new management strategy

Answer: A

NEW QUESTION 5

A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?

- A. `alert udp any any -> root any -> 21`
- B. `alert tcp any any -> any 21 (content:"root")`
- C. `alert tcp any any -> any root 21`
- D. `alert tcp any any -> any root (content:"ftp")`

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 6

Which of the following BEST describes the process by which code is developed, tested, and deployed in small batches?

- A. Agile
- B. Waterfall
- C. SDLC
- D. Dynamic code analysis

Answer: A

NEW QUESTION 7

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 8

A security manager has asked an analyst to provide feedback on the results of a penetration test. After reviewing the results the manager requests information regarding the possible exploitation of vulnerabilities Much of the following information data points would be MOST useful for the analyst to provide to the security manager who would then communicate the risk factors to senior management? (Select TWO)

- A. Probability
- B. Adversary capability
- C. Attack vector
- D. Impact
- E. Classification
- F. Indicators of compromise

Answer: AD

NEW QUESTION 9

Which of the following is the BEST way to share incident-related artifacts to provide non-repudiation?

- A. Secure email
- B. Encrypted USB drives
- C. Cloud containers
- D. Network folders

Answer: B

NEW QUESTION 10

A web developer wants to create a new web part within the company website that aggregates sales from individual team sites. A cybersecurity analyst wants to ensure security measurements are implemented during this process. Which of the following remediation actions should the analyst take to implement a vulnerability management process?

- A. Personnel training
- B. Vulnerability scan
- C. Change management
- D. Sandboxing

Answer: C

NEW QUESTION 10

Which of the following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

- A. It automatically performs remedial configuration changes to enterprise security services
- B. It enables standard checklist and vulnerability analysis expressions for automation
- C. It establishes a continuous integration environment for software development operations
- D. It provides validation of suspected system vulnerabilities through workflow orchestration

Answer: B

NEW QUESTION 11

Which of the following software assessment methods would be BEST for gathering data related to an application's availability during peak times?

- A. Security regression testing
- B. Stress testing
- C. Static analysis testing
- D. Dynamic analysis testing
- E. User acceptance testing

Answer: B

NEW QUESTION 12

An organization developed a comprehensive incident 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 involving 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 14

Which of the following MOST accurately describes an HSM?

- A. An HSM is a low-cost solution for encryption.
- B. An HSM can be networked based or a removable USB
- C. An HSM is slower at encrypting than software
- D. An HSM is explicitly used for MFA

Answer: A

NEW QUESTION 15

A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT. Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?

- A. Attack vectors
- B. Adversary capability
- C. Diamond Model of Intrusion Analysis
- D. Kill chain
- E. Total attack surface

Answer: B

NEW QUESTION 20

It is important to parameterize queries to prevent:

- A. the execution of unauthorized actions against a database.
- B. a memory overflow that executes code with elevated privileges.
- C. the establishment of a web shell that would allow unauthorized access.
- D. the queries from using an outdated library with security vulnerabilities.

Answer: A

NEW QUESTION 25

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 26

A development team uses open-source software and follows an Agile methodology with two-week sprints. Last month, the security team filed a bug for an insecure version of a common library. The DevOps team updated the library on the server, and then the security team rescanned the server to verify it was no longer vulnerable. This month, the security team found the same vulnerability on the server. Which of the following should be done to correct the cause of the vulnerability?

- A. Deploy a WAF in front of the application.
- B. Implement a software repository management tool.
- C. Install a HIPS on the server.
- D. Instruct the developers to use input validation in the code.

Answer: B

NEW QUESTION 30

An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:

Src IP	Src DNS	Dst IP	Dst DNS	Port	Application
10.50.50.121	83hht23.org-int.org	8.8.8.8	google...dns-a.google.com	53	DNS
10.50.50.121	83hht23.org-int.org	77.88.55.66	yandex.ru	443	HTTPS
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	53	DNS
10.100.10.45	appserver.org-int.org	69.134.21.90	repo.its.utk.edu	21	FTP
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS
172.16.52.100	sftp.org-dmz.org	62.30.221.56	ftps.bluedmed.net	42991	SSH
172.16.52.20	webserver.org-dmz.org	131.52.88.45	--	10999	HTTPS

Which of the following should be the focus of the investigation?

- A. webserver.org-dmz.org
- B. sftp.org-dmz.org
- C. 83hht23.org-int.org
- D. ftps.bluedmed.net

Answer: A

NEW QUESTION 33

A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server. Which of the following is the FIRST step the analyst should take?

- A. Create a full disk image of the server's hard drive to look for the file containing the malware.
- B. Run a manual antivirus scan on the machine to look for known malicious software.
- C. Take a memory snapshot of the machine to capture volatile information stored in memory.
- D. Start packet capturing to look for traffic that could be indicative of command and control from the miner.

Answer: D

NEW QUESTION 35

A compliance officer of a large organization has reviewed the firm's vendor management program but has discovered there are no controls defined to evaluate third-party risk or hardware source authenticity. The compliance officer wants to gain some level of assurance on a recurring basis regarding the implementation of controls by third parties.

Which of the following would BEST satisfy the objectives defined by the compliance officer? (Choose two.)

- A. Executing vendor compliance assessments against the organization's security controls
- B. Executing NDAs prior to sharing critical data with third parties
- C. Soliciting third-party audit reports on an annual basis
- D. Maintaining and reviewing the organizational risk assessment on a quarterly basis
- E. Completing a business impact assessment for all critical service providers
- F. Utilizing DLP capabilities at both the endpoint and perimeter levels

Answer: AC

NEW QUESTION 37

A security analyst is attempting to utilize the blowing threat intelligence for developing detection capabilities:

APT X's approach to a target would be sending a phishing email to the target after conducting active and passive reconnaissance. Upon successful compromise, APT X conducts internal reconnaissance and attempts to move laterally by utilizing existing resources. When APT X finds data that aligns to its objectives, it stages and then exfiltrates data sets in sizes that can range from 1GB to 1GB. APT X also establishes several backdoors to maintain a CI presence in the environment.

In which of the following phases is this APT MOST likely to leave discoverable artifacts?

- A. Data collection/exfiltration
- B. Defensive evasion
- C. Lateral movement
- D. Reconnaissance

Answer: A

NEW QUESTION 40

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 41

A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database. Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)

- A. Patch the required hosts with the correct updates and hot fixes, and rescan them for vulnerabilities.
- B. Remove the servers reported to have high and medium vulnerabilities.
- C. Tag the computers with critical findings as a business risk acceptance.
- D. Manually patch the computers on the network, as recommended on the CVE website.
- E. Harden the hosts on the network, as recommended by the NIST framework.
- F. Resolve the monthly job issues and test them before applying them to the production network.

Answer: CE

NEW QUESTION 46

Ransomware is identified on a company's network that affects both Windows and MAC hosts. The command and control channel for encryption for this variant uses TCP ports from 11000 to 65000. The channel goes to good1. iholdbadkeys.com, which resolves to IP address 72.172.16.2. Which of the following is the MOST effective way to prevent any newly infected systems from actually encrypting the data on connected network drives while causing the least disruption to normal Internet traffic?

- A. Block all outbound traffic to web host good1 iholdbadkeys.com at the border gateway.
- B. Block all outbound TCP connections to IP host address 172.172.16.2 at the border gateway.
- C. Block all outbound traffic on TCP ports 11000 to 65000 at the border gateway.
- D. Block all outbound traffic on TCP ports 11000 to 65000 to IP host address 172.172.16.2 at the border gateway.

Answer: A

NEW QUESTION 48

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 52

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 55

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 59

A security analyst on the threat-hunting team has developed a list of unneeded, benign services that are currently running as part of the standard OS deployment for workstations. The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization.

Which of the following BEST describes the security analyst's goal?

- A. To create a system baseline
- B. To reduce the attack surface
- C. To optimize system performance
- D. To improve malware detection

Answer: B

NEW QUESTION 64

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 69

Ann, a user, reports to the security team that her browser began redirecting her to random sites while using her Windows laptop. Ann further reports that the OS shows the C: drive is out of space despite having plenty of space recently. Ann claims she not downloaded anything. The security team obtains the laptop and begins to investigate, noting the following:

- > File access auditing is turned off.
- > When clearing up disk space to make the laptop functional, files that appear to be cached web pages are immediately created in a temporary directory, filling up the available drive space.
- > All processes running appear to be legitimate processes for this user and machine.
- > Network traffic spikes when the space is cleared on the laptop.
- > No browser is open.

Which of the following initial actions and tools would provide the BEST approach to determining what is happening?

- A. Delete the temporary files, run an Nmap scan, and utilize Burp Suite.
- B. Disable the network connection, check Sysinternals Process Explorer, and review netstat output.
- C. Perform a hard power down of the laptop, take a dd image, and analyze with FTK.
- D. Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.

Answer: B

NEW QUESTION 73

A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in1marketingpartners.com Below is the exiting SPP word:

```
v=spf1 a mx -all
```

Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?

- A)

```
v=spf1 a mx redirect:mail.marketingpartners.com ?all
```
- B)

```
v=spf1 a mx include:mail.marketingpartners.com -all
```
- C)

```
v=spf1 a mx +all
```
- D)

```
v=spf1 a mx include:mail.marketingpartners.com ~all
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

NEW QUESTION 75

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 80

A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic. Which of the following would BEST accomplish this goal?

- A. Continuous integration and deployment
- B. Automation and orchestration
- C. Static and dynamic analysis
- D. Information sharing and analysis

Answer: B

NEW QUESTION 85

A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication. Which of the following will remediate this software vulnerability?

- A. Enforce unique session IDs for the application.
- B. Deploy a WAF in front of the web application.
- C. Check for and enforce the proper domain for the redirect.
- D. Use a parameterized query to check the credentials.
- E. Implement email filtering with anti-phishing protection.

Answer: D

NEW QUESTION 86

A security analyst discovers accounts in sensitive SaaS-based systems are not being removed in a timely manner when an employee leaves the organization. To BEST resolve the issue, the organization should implement

- A. federated authentication
- B. role-based access control.
- C. manual account reviews
- D. multifactor authentication.

Answer: A

NEW QUESTION 90

An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a more proactive stance for security investigations. Which of the following would BEST meet that goal?

- A. Root-cause analysis
- B. Active response
- C. Advanced antivirus
- D. Information-sharing community
- E. Threat hunting

Answer: E

NEW QUESTION 95

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 100

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 102

A development team is testing a new application release. The team needs to import existing client PHI data records from the production environment to the test environment to test accuracy and functionality.

Which of the following would BEST protect the sensitivity of this data while still allowing the team to perform the testing?

- A. Deidentification
- B. Encoding
- C. Encryption
- D. Watermarking

Answer: A

NEW QUESTION 103

Because some clients have reported unauthorized activity on their accounts, a security analyst is reviewing network packet captures from the company's API server. A portion of a capture file is shown below:

```
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.s/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-instance"></s:Body></s:Envelope> 192.168.1.22 - -
api.somesite.com 200 0 1006 1001 0 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap
<<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/><a:Username>somebody@companyname.com 192.168.5.66 - - api.somesite.com 200 0 11558
1712 2024 192.168.4.89
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation></s:Body>< 192.168.1.22 - - api.somesite.com 200 0 1003 1011
307 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><IsLoggedIn+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="
http://www.w3.org/2001/XMLSchema-instance"><a:Authentication>
<a:ApiToken>kmL4krG2CwwWBan5BReGv5Djb7syxXTNKcWfuSjd</a:ApiToken><a:ImpersonateUserId>0
<a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authe 192.168.5.66 - - api.somesite.com 200 0 1378 1209
48 192.168.4.89
```

Which of the following MOST likely explains how the clients' accounts were compromised?

- A. The clients' authentication tokens were impersonated and replayed.
- B. The clients' usernames and passwords were transmitted in cleartext.
- C. An XSS scripting attack was carried out on the server.
- D. A SQL injection attack was carried out on the server.

Answer: A

NEW QUESTION 106

While preparing of an audit of information security controls in the environment an analyst outlines a framework control that has the following requirements:

- All sensitive data must be classified
- All sensitive data must be purged on a quarterly basis
- Certificates of disposal must remain on file for at least three years

This framework control is MOST likely classified as:

- A. prescriptive
- B. risk-based
- C. preventive
- D. corrective

Answer: A

NEW QUESTION 111

A team of security analysis has been alerted to potential malware activity. The initial examination indicates one of the affected workstations on 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 critically 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 Identify potentially affected systems by creating a correlation
- D. Identify potentially affected system by creating a correlation search in the SIEM based on the network traffic.

Answer: D

NEW QUESTION 113

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

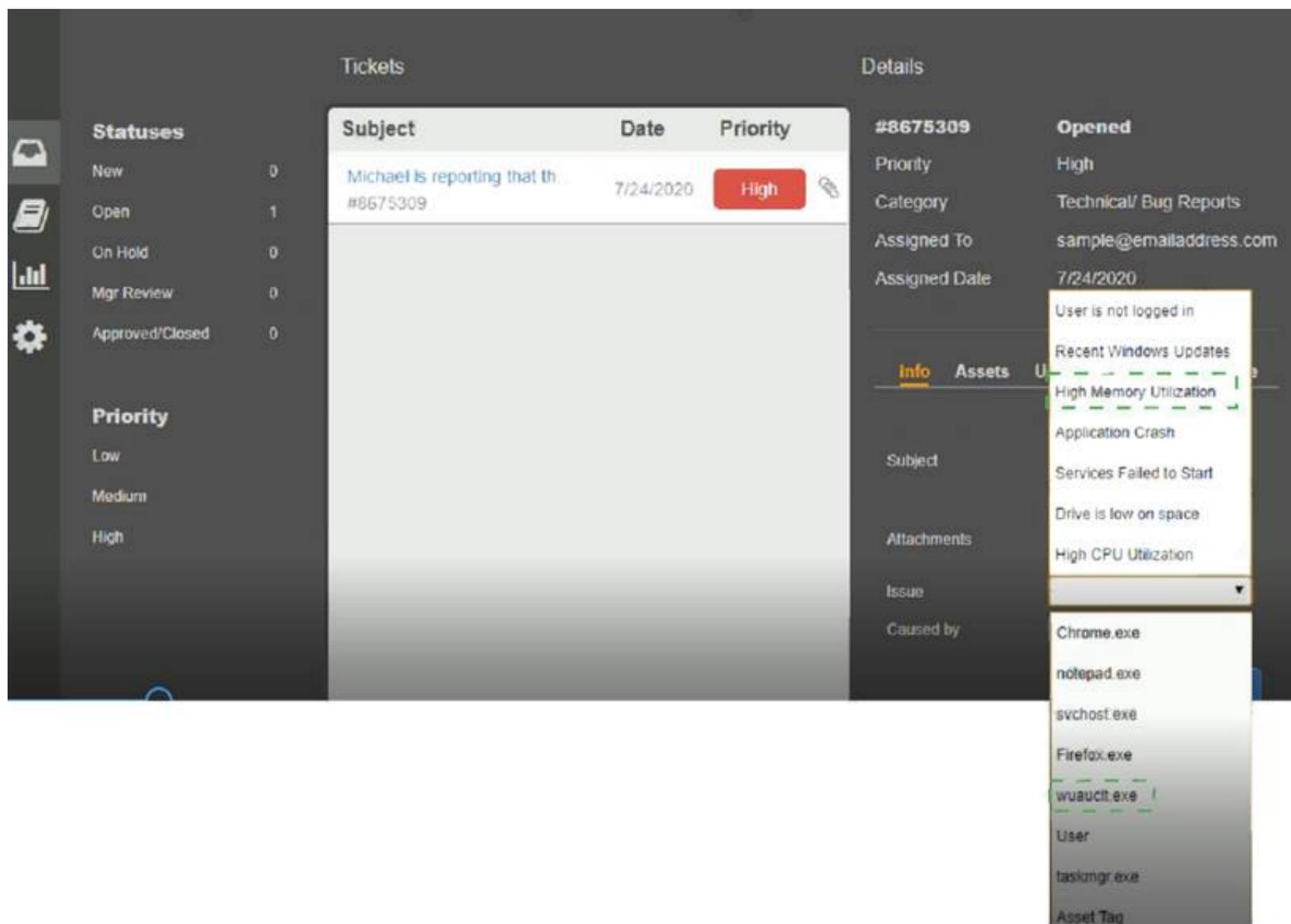
The screenshot shows a ticket management interface. On the left, there is a sidebar with 'Statuses' (New: 0, Open: 1, On Hold: 0, Mgr Review: 0, Approved/Closed: 0) and 'Priority' (Low, Medium, High). The main area is divided into 'Tickets' and 'Details'. The 'Tickets' section shows a table with one entry: 'Michael is reporting that th...' with ID '#8675309', date '7/24/2020', and priority 'High'. The 'Details' section shows ticket information: ID '#8675309', Priority 'High', Category 'Technical/ Bug Reports', Assigned To 'sample@emailaddress.com', and Assigned Date '7/24/2020'. Below this, there are tabs for 'Info', 'Assets', 'Users', and 'Approved Software'. The 'Info' tab is active, showing the subject 'Michael is reporting that the internet kiosk machine is intermittently freezing and has lagged performance.', Attachments 'none', Issue 'Drive is low on space', and Caused by 'taskmgr.exe'. A 'Close Ticket' button is at the bottom right.

This screenshot is identical to the one above, but with a dropdown menu open over the 'Issue' field. The dropdown menu lists several options: 'User is not logged in', 'Recent Windows Updates', 'High Memory Utilization', 'Application Crash', 'Services Failed to Start', 'Drive is low on space', 'High CPU Utilization', 'Chrome.exe', 'notepad.exe', 'svchost.exe', 'Firefox.exe', 'wuauclt.exe', 'User', 'taskmgr.exe', and 'Asset Tag'. The 'Issue' field in the background is currently set to 'Drive is low on space'.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 118

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 121

A security analyst wants to identify which vulnerabilities a potential attacker might initially exploit if the network is compromised. Which of the following would provide the BEST results?

- A. Baseline configuration assessment
- B. Uncredentialed scan
- C. Network ping sweep
- D. External penetration test

Answer: D

NEW QUESTION 124

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 126

A security analyst gathered forensics from a recent intrusion in preparation for legal proceedings. The analyst used EnCase to gather the digital forensics, cloned the hard drive, and took the hard drive home for further analysis. Which of the following of the security analyst violate?

- A. Cloning procedures
- B. Chain of custody
- C. Hashing procedures
- D. Virtualization

Answer: B

NEW QUESTION 127

A user receives a potentially malicious email that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review.

Which of the following commands would MOST likely indicate if the email is malicious?

- A. sha256sum ~/Desktop/file.pdf
- B. file ~/Desktop/file.pdf
- C. strings ~/Desktop/file.pdf | grep "<script"
- D. cat < ~/Desktop/file.pdf | grep -i .exe

Answer: A

NEW QUESTION 130

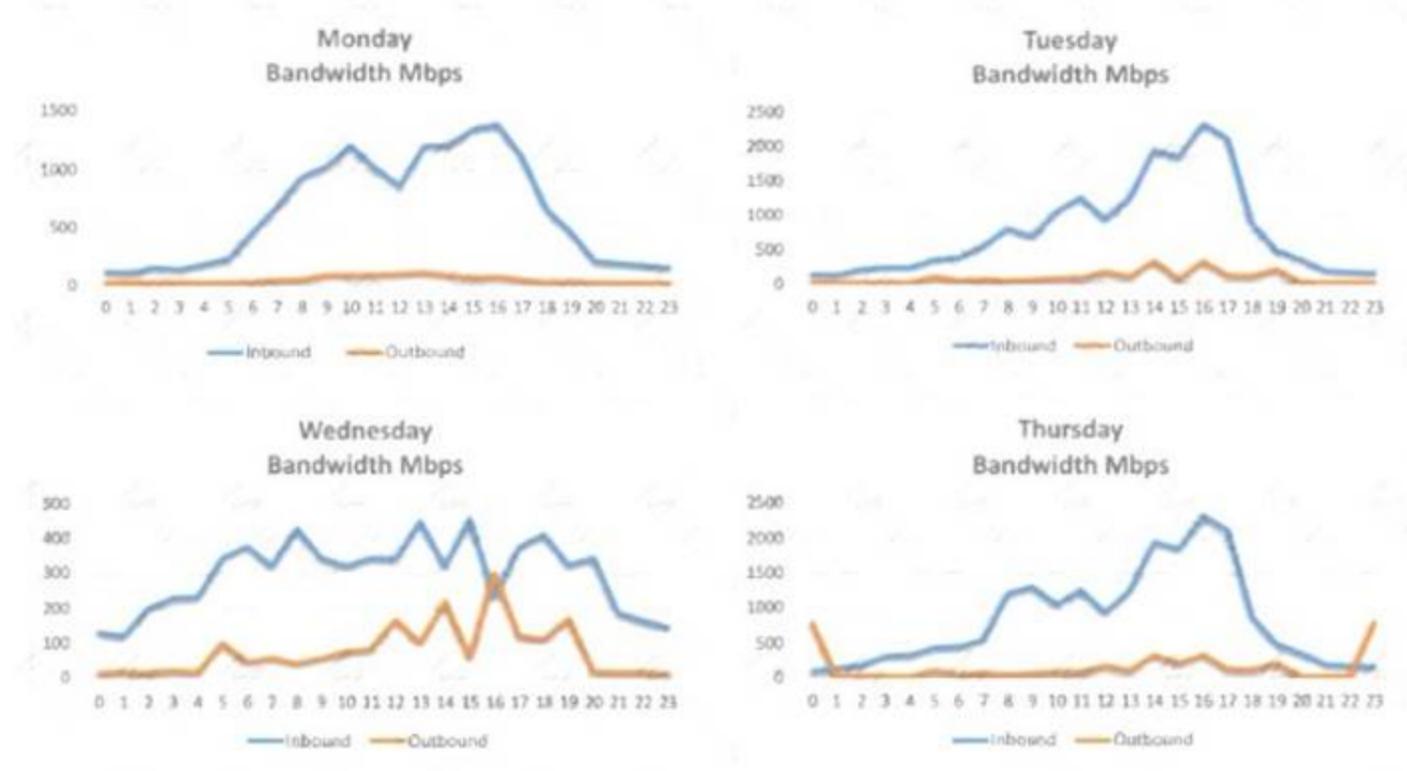
A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should 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 133

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 135

A developer wrote a script to make names and other PII data unidentifiable before loading a database export into the testing system Which of the following describes the type of control that is being used?

- A. Data encoding
- B. Data masking
- C. Data loss prevention
- D. Data classification

Answer: C

NEW QUESTION 138

A security analyst has discovered that developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?

- A. Create a security rule that blocks Internet access in the development VPC
- B. Place a jumpbox in between the developers' workstations and the development VPC
- C. Remove the administrator profile from the developer user group in identity and access management
- D. Create an alert that is triggered when a developer installs an application on a server

Answer: A

NEW QUESTION 141

A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability. Company policy prohibits using portable media or mobile storage. The security analyst is trying to determine which user caused the malware to get onto the system. Which of the following registry keys would MOST likely have this information?

- A)
`HKEY_USERS\\Software\Microsoft\Windows\CurrentVersion\Run`
- B)
`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
- C)
`HKEY_USERS\\Software\Microsoft\Windows\explorer\MountPoints2`
- D)
`HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub`

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 145

Which of the following policies would state an employee should not disable security safeguards, such as host firewalls and antivirus on company systems?

- A. Code of conduct policy
- B. Account management policy
- C. Password policy
- D. Acceptable use policy

Answer: D

NEW QUESTION 150

A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:

Antivirus is installed on the remote host:

Installation path: C:\Program Files\AVProduct\Win32\ Product Engine: 14.12.101

Engine Version: 3.5.71

Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported.

The engine version is out of date. The oldest supported version from the vendor is 4.2.11. The analyst uses the vendor's website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?

- A. This is a false positive, and the scanning plugin needs to be updated by the vendor.
- B. This is a true negative, and the new computers have the correct version of the software.
- C. This is a true positive, and the new computers were imaged with an old version of the software.
- D. This is a false negative, and the new computers need to be updated by the desktop team.

Answer: C

NEW QUESTION 151

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 155

A cybersecurity analyst is supporting 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: A

NEW QUESTION 159

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 160

During an investigation, an incident responder intends to recover multiple pieces of digital media. Before removing the media, the responder should initiate:

- A. malware scans.
- B. secure communications.
- C. chain of custody forms.
- D. decryption tools.

Answer: C

NEW QUESTION 163

A new on-premises application server was recently installed on the network. Remote access to the server was enabled for vendor support on required ports, but recent security reports show large amounts of data are being sent to various unauthorized networks through those ports. Which of the following configuration changes must be implemented to resolve this security issue while still allowing remote vendor access?

- A. Apply a firewall application server rule.
- B. Whitelist the application server.
- C. Sandbox the application server.
- D. Enable port security.
- E. Block the unauthorized networks.

Answer: B

NEW QUESTION 165

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 167

A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:

CVE ID	CVSS Base	Name
CVE-1999-0524	None	ICMP timestamp request remote date disclosure
CVE-1999-0497	5.0	Anonymous FTP enabled
None	7.5	Unsupported web server detection
CVE-2005-2150	5.0	Windows SMB service enumeration via \srvsvc

Which of the following is MOST likely a false positive?

- A. ICMP timestamp request remote date disclosure
- B. Windows SMB service enumeration via \srvsvc
- C. Anonymous FTP enabled
- D. Unsupported web server detection

Answer: B

NEW QUESTION 170

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 173

An information security analyst is compiling data from a recent penetration test and reviews the following output:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-01 16:06 UTC
Nmap scan report for 10.79.95.173.rdns.datacenters.com (10.79.95.173)
Host is up (0.026s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
22/tcp    open  ssh      SilverShield sshd (protocol 2.0)
80/tcp    open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp   open  https?
691/tcp   open  resvc?
5060/tcp  open  sip      Barracuda NG Firewall (Status: 200 OK)
Nmap done: 1 IP address (1 host up) scanned in 158.22 seconds
```

The analyst wants to obtain more information about the web-based services that are running on the target. Which of the following commands would MOST likely provide the needed information?

- A. ping -t 10.79.95.173.rdns.datacenters.com
- B. telnet 10.79.95.173 443
- C. ftpd 10.79.95.173.rdns.datacenters.com 443
- D. tracer 10.79.95.173

Answer: B

NEW QUESTION 177

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 180

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 183

A cybersecurity analyst is currently checking a newly deployed server that has an access control list applied. When conducting the scan, the analyst received the following code snippet of results:

```
Mail Server1
Trying 192.168.2.2
Connected
Get / HTTP/ 1.0

HTTP:1.0 200 Document follows
Server: server/0.10
Connection: close
Set-Cookie: testing=1; path=/
```

Which of the following describes the output of this scan?

- A. The analyst has discovered a False Positive, and the status code is incorrect providing an OK message.
- B. The analyst has discovered a True Positive, and the status code is correct providing a file not found error message.
- C. The analyst has discovered a True Positive, and the status code is incorrect providing a forbidden message.
- D. The analyst has discovered a False Positive, and the status code is incorrect providing a server error message.

Answer: B

NEW QUESTION 186

An incident responder successfully acquired application binaries off a mobile device for later forensic analysis. Which of the following should the analyst do NEXT?

- A. Decompile each binary to derive the source code.
- B. Perform a factory reset on the affected mobile device.
- C. Compute SHA-256 hashes for each binary.
- D. Encrypt the binaries using an authenticated AES-256 mode of operation.
- E. Inspect the permissions manifests within each application.

Answer: C

NEW QUESTION 188

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 193

During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation. Which of the following would cause the analyst to further review the incident?

- A)

```
BadReputationIp - - [2019-04-12 10:43z] "GET /etc/passwd" 403 1023
```
- B)

```
BadReputationIp - - [2019-04-12 10:43z] "GET /index.html?src=../../ssh/id_rsa" 401 17044
```
- C)

```
BadReputationIp - - [2019-04-12 10:43z] "GET /a.php?src=/etc/passwd" 403 11056
```
- D)

```
BadReputationIp - - [2019-04-12 10:43z] "GET /a.php?src=../../ssh/id_rsa" 200 15036
```
- E)

```
BadReputationIp - - [2019-04-12 10:43z] "GET /favicon.ico?src=../../usr/share/icons" 200 19064
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

Answer: D

NEW QUESTION 196

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 197

A security team is implementing a new vulnerability management program in an environment that has a historically poor security posture. The team is aware of issues with patch management in the environment and expects a large number of findings. Which of the following would be the MOST efficient way to increase the security posture of the organization in the shortest amount of time?

- A. Create an SLA stating that remediation actions must occur within 30 days of discovery for all levels of vulnerabilities.
- B. Incorporate prioritization levels into the remediation process and address critical findings first.
- C. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.
- D. Implement a change control policy that allows the security team to quickly deploy patches in the production environment to reduce the risk of any vulnerabilities.

found.

Answer: B

NEW QUESTION 202

A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs.

Which of the following is the main concern a security analyst should have with this arrangement?

- A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.
- B. Moving the FPGAs between development sites will lessen the time that is available for security testing.
- C. Development phases occurring at multiple sites may produce change management issues.
- D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Answer: B

NEW QUESTION 206

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 208

A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-in-the-middle attack. The security analyst also verified that privileges were not escalated, and the two devices did not gain access to other network devices. Which of the following would BEST mitigate and improve the security posture of the wireless network for this type of attack?

- A. Enable MAC filtering on the wireless router and suggest a stronger encryption for the wireless network.
- B. Change the SSID, strengthen the passcode, and implement MAC filtering on the wireless router.
- C. Enable MAC filtering on the wireless router and create a whitelist that allows devices on the network.
- D. Conduct a wireless survey to determine if the wireless strength needs to be reduced.

Answer: A

NEW QUESTION 209

A large amount of confidential data was leaked during a recent security breach. As part of a forensic investigation, the security team needs to identify the various types of traffic that were captured between two compromised devices.

Which of the following should be used to identify the traffic?

- A. Carving
- B. Disk imaging
- C. Packet analysis
- D. Memory dump
- E. Hashing

Answer: C

NEW QUESTION 214

Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?

- A. Use a UEFI boot password.
- B. Implement a self-encrypted disk.
- C. Configure filesystem encryption
- D. Enable Secure Boot using TPM

Answer: A

NEW QUESTION 219

A security analyst implemented a solution that would analyze the attacks that the organization's firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command.

```
S sudo nc -l -v -c maildemon . py 25 caplog, txt
```

Which of the following solutions did the analyst implement?

- A. Log collector
- B. Crontab mail script
- C. Snikhole
- D. Honeytrap

Answer: A

NEW QUESTION 222

While planning segmentation for an ICS environment, a security engineer determines IT resources will need access to devices within the ICS environment without compromising security.

To provide the MOST secure access model in this scenario, the jumpbox should be.

- A. placed in an isolated network segment, authenticated on the IT side, and forwarded into the ICS network.
- B. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.
- C. bridged between the IT and operational technology networks to allow authenticated access.
- D. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.

Answer: D

NEW QUESTION 223

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 225

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CS0-002 Exam with Our Prep Materials Via below:

<https://www.certleader.com/CS0-002-dumps.html>