



# CompTIA

## Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

#### NEW QUESTION 1

- (Exam Topic 3)

A security analyst is researching ways to improve the security of a company's email system to mitigate emails that are impersonating company executives. Which of the following would be BEST for the analyst to configure to achieve this objective?

- A. A TXT record on the name server for SPF
- B. DNSSEC keys to secure replication
- C. Domain Keys identified Mail
- D. A sandbox to check incoming mail

**Answer: B**

#### NEW QUESTION 2

- (Exam Topic 3)

An organization has specific technical risk mitigation configurations that must be implemented before a new server can be approved for production. Several critical servers were recently deployed with the antivirus missing, unnecessary ports disabled, and insufficient password complexity. Which of the following should the analyst recommend to prevent a recurrence of this risk exposure?

- A. Perform password-cracking attempts on all devices going into production
- B. Perform an Nmap scan on all devices before they are released to production
- C. Perform antivirus scans on all devices before they are approved for production
- D. Perform automated security controls testing of expected configurations prior to production

**Answer: D**

#### NEW QUESTION 3

- (Exam Topic 3)

A security technician configured a NIDS to monitor network traffic. Which of the following is a condition in which harmless traffic is classified as a potential network attack?

- A. True positive
- B. True negative
- C. False positive
- D. False negative

**Answer: D**

#### NEW QUESTION 4

- (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 5

- (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 6

- (Exam Topic 3)

While reviewing incident reports from the previous night, a security analyst notices the corporate websites were defaced with political 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 7

- (Exam Topic 3)

An organization prohibits users from logging in to the administrator account. If a user requires elevated permissions, the user's account should be part of an administrator group, and the user should escalate permission only as needed and on a temporary basis. The organization has the following reporting priorities when reviewing system activity:

- Successful administrator login reporting priority - high
- Failed administrator login reporting priority - medium
- Failed temporary elevated permissions - low
- Successful temporary elevated permissions - non-reportable

A security analyst is reviewing server syslogs and sees the following: Which of the following events is the HIGHEST reporting priority?

- A. `<100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success`
- B. `<100>2 2020-01-10T21:19:34.002Z adminserver sudo 201 32001 - BOM 'sudo more /etc/passwords' success`
- C. `<100>2 2020-01-10T19:33:48.002Z webserver su 201 32001 - BOM 'su' success`
- D. `<100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe`

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

**Answer:** A

### NEW QUESTION 8

- (Exam Topic 3)

An organization has the following policies:

\*Services must run on standard ports.

\*Unneeded services must be disabled.

The organization has the following servers:

\*192.168.10.1 - web server

\*192.168.10.2 - database server

A security analyst runs a scan on the servers and sees the following output:

```
Host 192.168.10.1
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
443/tcp   open   https
1027/tcp   open   IIS
```

```
Host 192.168.10.2
PORT      STATE  SERVICE
22/tcp    open   ssh
53/tcp    open   dns
1434/tcp  open   mssql
```

Which of the following actions should the analyst take?

- A. Disable HTTPS on 192.168.10.1.  
B. Disable IIS on 192.168.10.1.  
C. Disable DNS on 192.168.10.2.  
D. Disable MSSQL on 192.168.10.2.  
E. Disable SSH on both servers.

**Answer:** C

### NEW QUESTION 9

- (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 10

- (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 10

- (Exam Topic 3)

A vulnerability assessment solution is hosted in the cloud This solution will be used as an accurate inventory data source for both the configuration management database and the governance nsk and compliance tool An analyst has been asked to automate the data acquisition Which of the following would be the BEST way to acqutre the data'

- A. CSV export
- B. SOAR
- C. API
- D. Machine learning

**Answer:** C

#### Explanation:

An example of API is google weather app, using the weather channel's API to collect accurate weather data and broadcast it on goggle weather app, so google doesn't have to do it their selves

#### NEW QUESTION 11

- (Exam Topic 3)

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

```
Request="GET /public/report.html?iewt=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 iniecton
- D. Denial of service

**Answer:** A

#### NEW QUESTION 16

- (Exam Topic 3)

A security analyst needs to determine the best method for securing access to a top-secret datacenter Along with an access card and PIN code, which of the following additional authentication methods would be BEST to enhance the datacenter's security?

- A. Physical key
- B. Retinal scan
- C. Passphrase
- D. Fingerprint

**Answer:** D

#### NEW QUESTION 18

- (Exam Topic 3)

A company's Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support employee morale. Which of the following security recommendations would allow employees to browse non-business-related websites?

- A. Implement a virtual machine alternative.
- B. Develop a new secured browser.
- C. Configure a personal business VLAN.
- D. Install kiosks throughout the building.

**Answer:** C

#### NEW QUESTION 20



- (Exam Topic 3)

An incident response team is responding to a breach of multiple systems that contain PII and PHI Disclosure of the incident to external entities should be based on:

- A. the responder's discretion.
- B. the public relations policy.
- C. the communication plan.
- D. the senior management team's guidance

**Answer: C**

#### NEW QUESTION 21

- (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:

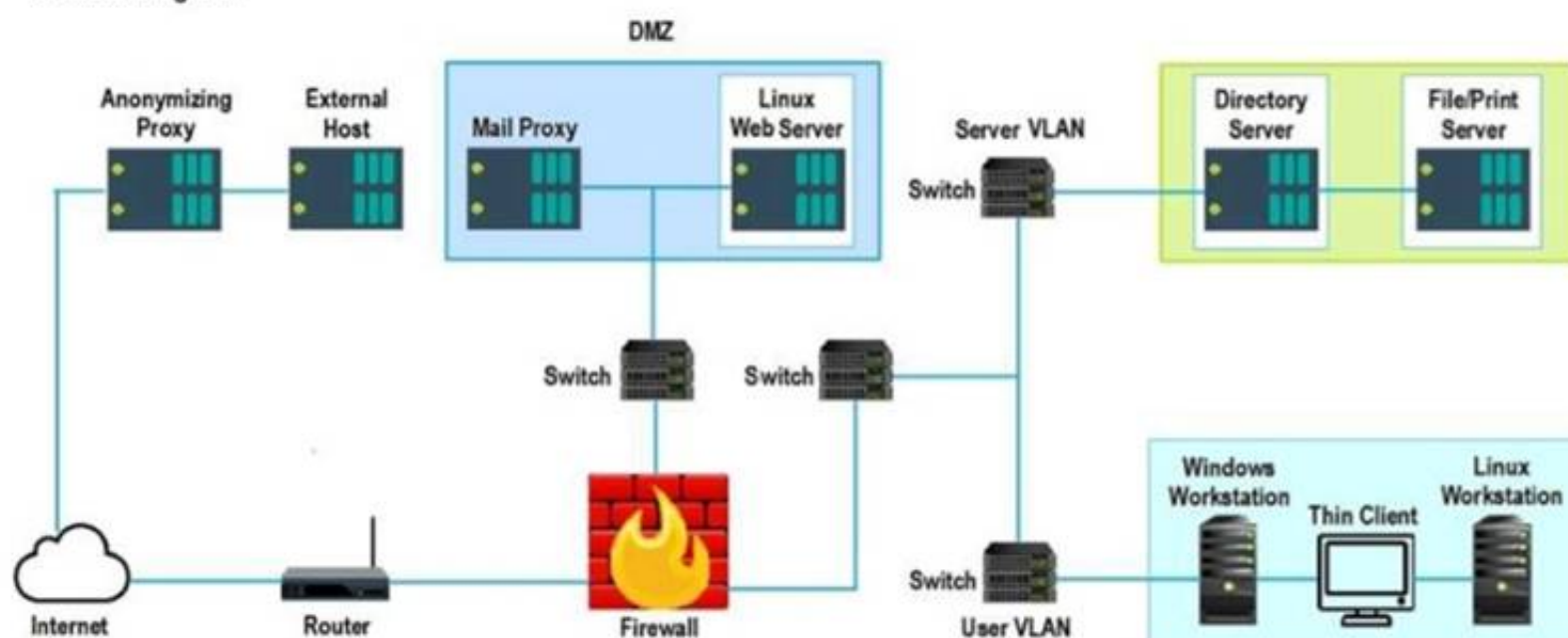
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan. For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. 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:

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

## Hot Area:

Findings Listing 1	Results Generated
<p><b>Fake Positive</b></p> <p>Critical (10.0) 12209 Security Update for Microsoft Windows (835732)</p> <p>Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)</p> <p>Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)</p> <p>Critical (10.0) 58662 Samba 3.x&lt;3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)</p> <p>Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)</p>	<p>Credentialed</p> <p>Non-Credentialed</p> <p>Compliance</p>
<p><b>Fake Positive</b></p> <p>Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)</p> <p>Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)</p> <p>Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)</p> <p>Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)</p> <p>Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)</p>	<p>Credentialed</p> <p>Non-Credentialed</p> <p>Compliance</p>
<p><b>Fake Positive</b></p> <p>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</p> <p>INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled</p> <p>INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled</p> <p>INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled</p> <p>INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves</p>	<p>Credentialed</p> <p>Non-Credentialed</p> <p>Compliance</p>

## NEW QUESTION 22

- (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 m the future.

**Answer: B**

## NEW QUESTION 24

- (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 28

- (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 33

- (Exam Topic 1)

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

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

**Answer: D**

## NEW QUESTION 34

- (Exam Topic 1)

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

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

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

**Answer:** A

#### NEW QUESTION 36

- (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 40

- (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

AppServ1 AppServ2 AppServ3 AppServ4

Compliance Report

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

```
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
```

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



Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

Compliance Report

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

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

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

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

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

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

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

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

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

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

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

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

## Part 1

## Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv3.fictionalorg.com:443

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

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

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

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

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

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

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

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

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

## Compliance Report

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

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



## Part 1

### Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
root@INFOSEC:~# curl --head appsrv4.fictionalorg.com:443

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

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

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

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

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

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

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

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

### Compliance Report

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

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

## Part 2

### Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

### Configuration Change Recommendations



Add recommendation for

AppSrv1  
AppSrv2  
AppSrv3  
AppSrv4

- 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

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

```
AppServ1    AppServ2    AppServ3    AppServ4
```

```
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: "13520-58c007930177d"
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:
|_ TLSv1.1:
|_ TLSv1.2:
|_ TLSv1.3:
```

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

"GET /form.php?id=463225%2b%2575%256e%2569%256f%256e%2b%2573%2574%2b%3133333731,1223,1224&name=%&state=IL"

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

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

- 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.

An analyst is reviewing the following output as part of an incident:

```
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=10 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=10 ABCDEFGHIJ
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=15 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=15 ABCDEFGHIJ|8fd
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=20 ABCDEFGHIJ1234567890
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=20 ABCDEFGHIJ1234567890
```

A. The hosts are part of a reflective denial-of-service attack.  
B. Information is leaking from the memory of host 10.20.30.40.  
C. Sensitive data is being exfiltrated by host 192.168.1.10.  
D. Host 291.168.1.10 is performing firewall port knocking.

visit - <https://www.certshared.com>



#### NEW QUESTION 48

- (Exam Topic 2)

A company recently experienced financial fraud, which included shared passwords being compromised and improper levels of access being granted. The company has asked a security analyst to help improve its controls.

Which of the following will MOST likely help the security analyst develop better controls?

- A. An evidence summarization
- B. An indicator of compromise
- C. An incident response plan
- D. A lessons-learned report

**Answer: C**

#### NEW QUESTION 51

- (Exam Topic 2)

A security analyst receives an alert to expect increased and highly advanced cyberattacks originating from a foreign country that recently had sanctions implemented. Which of the following describes the type of threat actors that should concern the security analyst?

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

**Answer: D**

#### NEW QUESTION 52

- (Exam Topic 2)

An organization recently discovered some inconsistencies in the motherboards it received from a vendor. The organization's security team then provided guidance on how to ensure the authenticity of the motherboards it received from vendors.

Which of the following would be the BEST recommendation for the security analyst to provide'?

- A. The organization should evaluate current NDAs to ensure enforceability of legal actions.
- B. The organization should maintain the relationship with the vendor and enforce vulnerability scans.
- C. The organization should ensure all motherboards are equipped with a TPM.
- D. The organization should use a certified, trusted vendor as part of the supply chain.

**Answer: D**

#### NEW QUESTION 56

- (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 58

- (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 62

- (Exam Topic 2)

An employee was found to have performed fraudulent activities. The employee was dismissed, and the employee's laptop was sent to the IT service desk to undergo a data sanitization procedure. However, the security analyst responsible for the investigation wants to avoid data sanitization. Which of the following can the security analyst use to justify the request?

- A. Data retention
- B. Evidence retention
- C. GDPR
- D. Data correlation procedure

**Answer: A**

#### NEW QUESTION 67

- (Exam Topic 2)

A remote code execution vulnerability was discovered in the RDP. An organization currently uses RDP for remote access to a portion of its VDI environment. The analyst verified network-level authentication is enabled

Which of the following is the BEST remediation for this vulnerability?

- A. Verify the latest endpoint-protection signature is in place.
- B. Verify the corresponding patch for the vulnerability is installed^
- C. Verify the system logs do not contain indicator of compromise.
- D. Verify the threat intelligence feed is updated with the latest solutions

**Answer:** A

#### NEW QUESTION 68

- (Exam Topic 2)

Which of the following threat classifications would MOST likely use polymorphic code?

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

**Answer:** D

#### NEW QUESTION 72

- (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, Tamperin
- E. Repudiation, Information disclosur
- F. Denial of service, Elevation of privileges(STRIDE)

**Answer:** C

#### NEW QUESTION 75

- (Exam Topic 2)

A newly appointed Chief Information Security Officer (CISO) has completed a risk assessment review of the organization and wants to reduce the numerous risks that were identified. Which of the following will provide a trend of risk mitigation?

- A. Risk response
- B. Risk analysis
- C. Planning
- D. Oversight
- E. Continuous monitoring

**Answer:** A

#### NEW QUESTION 79

- (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 81**

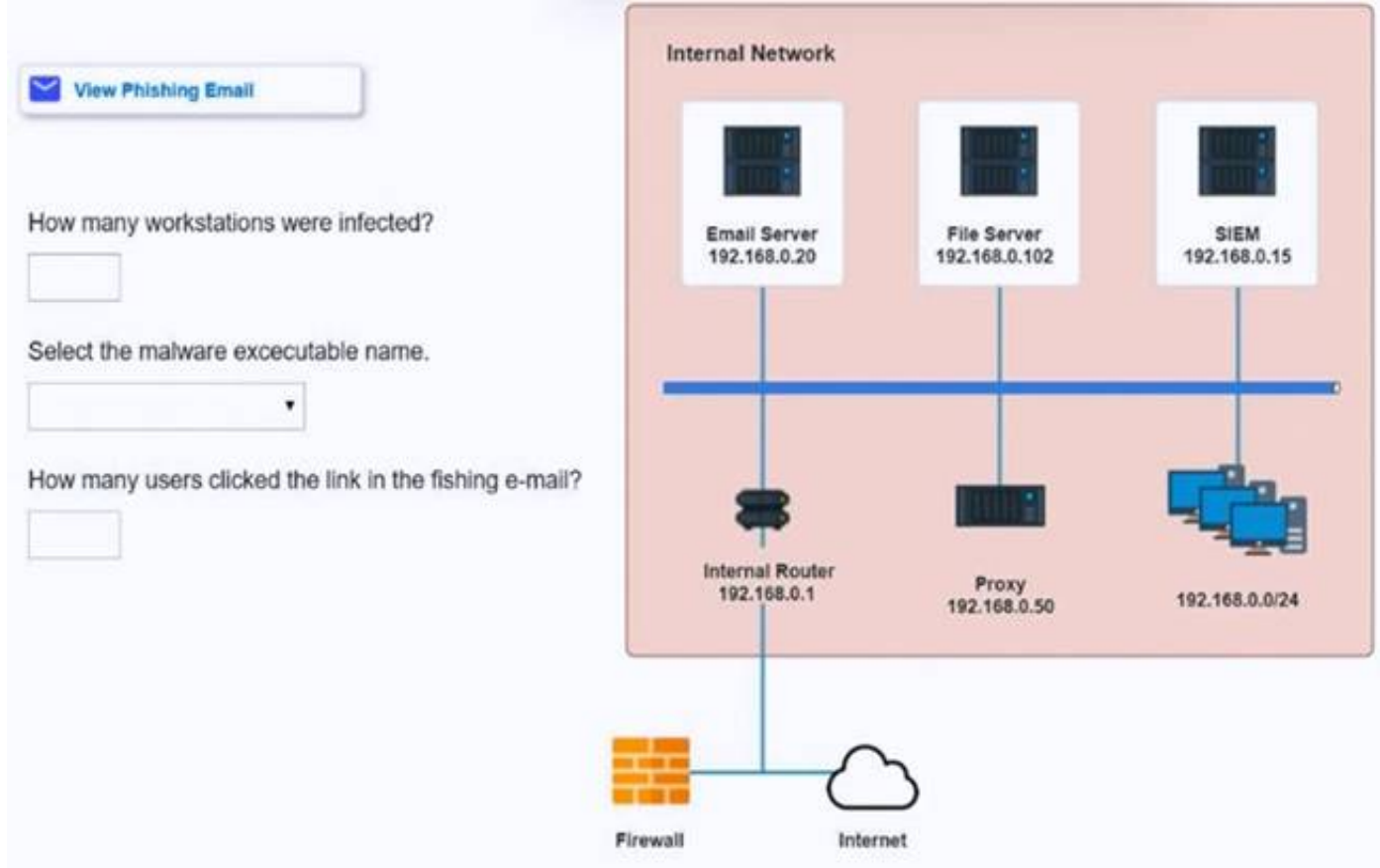
- (Exam Topic 2)

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

**INSTRUCTIONS**

Review the information provided and determine the following:

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



**Phishing Email**
✕

From: IT HelpDesk <[it-helpdesk@sobergrill.com](mailto:it-helpdesk@sobergrill.com)>  
 Sent: Mon 3/7/2016 4:00 PM  
 To: Global Users <[globalusers@sobergrill.com](mailto:globalusers@sobergrill.com)>

Hi,

In the upcoming days, we will be moving our mail servers from MS Outlook to the new Netscape Navigator. Check out the new SoberGrill webmail and know if it has started working for you.

Visit the new SoberGrill webmail to see all the new features.  
 Use your current username and password at [SoberGrill Webmail](#).

Download the latest mail client [here](#).

Thank you.

IT HelpDesk



Email Server Logs - Email Server 192.168.0.20					
Date/Time	Protocol	SMTP	Source port	From	To
3/7/2016 4:17:08 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dhitz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com,adifabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:12:50 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:11:09 PM	TCP	192.168.0.34	46187	lbalk@anycorp.com	jlee@anycorp.com
3/7/2016 4:10:54 PM	TCP	192.168.0.181	34556	dhitz@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:10:38 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:10:23 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	asmith@anycorp.com
3/7/2016 4:09:34 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com
3/7/2016 4:08:49 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:07:33 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com
3/7/2016 4:07:32 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com,jlee@anycorp.com
3/7/2016 4:05:47 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com
3/7/2016 4:04:24 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com
3/7/2016 4:03:50 PM	TCP	192.168.0.181	34556	dhitz@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:03:25 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sboaz@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ibenz@anycorp.com
3/7/2016 4:01:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dsutherland@anycorp.com
3/7/2016 4:01:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lrosaler@anycorp.com
3/7/2016 4:01:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ahynson@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mdillon@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jwayman@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jehn@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ilogge@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aaveritt@anycorp.com
3/7/2016 4:01:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lephraim@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wmcneme@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	imarable@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tfausto@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kdefranco@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mworley@anycorp.com

Email Server Logs - Email Server 192.168.0.20					
Date/Time	Protocol	SMTP	Source port	From	To
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ltreiber@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mgameau@anycorp.com
3/7/2016 4:01:20 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tllossum@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	thoda@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ctsuj@anycorp.com
3/7/2016 4:01:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sprosperle@anycorp.com
3/7/2016 4:01:16 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bmontealeone@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	clensternmacher@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rgarlink@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cheroux@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mkamen@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	zdodgen@anycorp.com
3/7/2016 4:01:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhammonds@anycorp.com
3/7/2016 4:01:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	onorth@anycorp.com
3/7/2016 4:01:09 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mroane@anycorp.com
3/7/2016 4:01:07 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kbowling@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	nrachal@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jdegenhardt@anycorp.com
3/7/2016 4:01:03 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wracette@anycorp.com
3/7/2016 4:01:01 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lhammond@anycorp.com
3/7/2016 4:00:59 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dmilazzo@anycorp.com
3/7/2016 4:00:57 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kneubauer@anycorp.com
3/7/2016 4:00:55 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bboyko@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dcrofoot@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmemmott@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	chodgin@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aholler@anycorp.com
3/7/2016 4:00:51 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	abattaglia@anycorp.com
3/7/2016 4:00:49 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	halbert@anycorp.com
3/7/2016 4:00:47 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	myeoman@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wbobadilla@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lkam@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jcooks@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpolice@anycorp.com
3/7/2016 4:00:43 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mwagener@anycorp.com
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bteer@anycorp.com






Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:27:03 PM	192.168.0.153	50467	11.102.109.179	80	bestpurchase.com	POST
3/7/2016 4:26:51 PM	192.168.0.245	60021	72.104.64.186	80	visitorcenter.com	GET
3/7/2016 4:25:36 PM	192.168.0.97	46354	96.191.222.144	80	bestpurchase.com	GET
3/7/2016 4:25:10 PM	192.168.0.116	43389	35.132.243.140	80	goodguys.se	POST
3/7/2016 4:25:06 PM	192.168.0.7	45463	124.140.208.241	80	stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.188.144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80	chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214.214.167.94	80	anti-malware.com	GET
3/7/2016 4:19:48 PM	192.168.0.44	45240	218.24.114.208	80	anti-malware.com	GET
3/7/2016 4:17:52 PM	192.168.0.19	31101	103.40.104.165	80	thelastwebpage.com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.46.190	80	thebestwebsite.com	GET
3/7/2016 4:15:39 PM	192.168.0.94	63814	102.172.101.36	80	freefood.com	GET
3/7/2016 4:15:35 PM	192.168.0.47	48110	151.94.198.15	443	searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.85.107	80	securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80	chzweb.tlapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.95	42733	103.136.14.126	80	goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62813	181.139.24.22	80	pastebucket.cn	POST
3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80	chzweb.tlapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	124.169.173.216	80	funweb.cn	POST
3/7/2016 4:10:16 PM	192.168.0.9	56757	33.225.130.104	80	chzweb.tlapia.com	GET
3/7/2016 4:10:04 PM	192.168.0.112	35716	45.100.47.99	80	stopthebotnet.com	GET
3/7/2016 4:08:45 PM	192.168.0.24	50582	33.225.130.104	80	chzweb.tlapia.com	GET
3/7/2016 4:08:08 PM	192.168.0.36	37102	78.151.16.233	80	chatforfree.ru	POST
3/7/2016 4:06:40 PM	192.168.0.193	43363	95.77.193.180	80	anti-malware.com	GET
3/7/2016 4:05:14 PM	192.168.0.254	55947	33.225.130.104	80	chzweb.tlapia.com	GET
3/7/2016 4:04:37 PM	192.168.0.117	54959	182.203.42.246	80	thelastwebpage.com	GET
3/7/2016 4:04:30 PM	192.168.0.172	43947	3.60.67.249	80	thebestwebsite.com	GET
3/7/2016 4:04:21 PM	192.168.0.134	60525	33.225.130.104	80	chzweb.tlapia.com	GET

Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:03:48 PM	192.168.0.64	44114	127.36.104.33	443	searchforus.de	GET
3/7/2016 4:02:42 PM	192.168.0.250	57111	243.223.175.143	80	securethenet.com	GET
3/7/2016 4:01:34 PM	192.168.0.132	60561	33.225.130.104	80	chzweb.tlapia.com	GET
3/7/2016 4:01:33 PM	192.168.0.23	57360	239.141.52.189	80	anti-malware.com	GET
3/7/2016 4:01:01 PM	192.168.0.215	44179	161.192.122.40	80	healthreport.com	GET
3/7/2016 3:59:52 PM	192.168.0.121	56315	204.190.57.150	80	freefood.com	POST
3/7/2016 3:58:56 PM	192.168.0.18	60624	169.43.139.3	80	bestpurchase.com	POST
3/7/2016 3:58:54 PM	192.168.0.106	30163	110.234.67.223	80	visitorcenter.com	GET
3/7/2016 3:57:59 PM	192.168.0.59	33145	209.240.152.67	80	bestpurchase.com	GET
3/7/2016 3:57:03 PM	192.168.0.27	46987	23.83.170.116	80	goodguys.se	POST
3/7/2016 3:55:14 PM	192.168.0.211	31442	168.83.234.163	80	visitorcenter.com	GET
3/7/2016 3:54:31 PM	192.168.0.152	30520	141.217.181.243	80	goodguys.se	POST
3/7/2016 3:52:47 PM	192.168.0.253	36463	79.115.201.191	80	pastebucket.cn	POST
3/7/2016 3:51:44 PM	192.168.0.244	61719	14.47.142.43	80	bestpurchase.com	GET
3/7/2016 3:51:19 PM	192.168.0.65	48611	146.104.226.192	80	funweb.cn	POST
3/7/2016 3:49:54 PM	192.168.0.126	40815	171.140.162.96	80	stopthebotnet.com	GET
3/7/2016 3:49:07 PM	192.168.0.9	47625	18.23.47.44	80	stopthebotnet.com	GET
3/7/2016 3:47:38 PM	192.168.0.131	44579	139.58.55.91	80	funweb.cn	GET
3/7/2016 3:45:58 PM	192.168.0.186	62683	31.133.137.225	80	chatforfree.ru	POST
3/7/2016 3:44:05 PM	192.168.0.181	38937	150.119.71.249	80	anti-malware.com	GET
3/7/2016 3:43:33 PM	192.168.0.225	46999	131.97.167.36	80	anti-malware.com	GET
3/7/2016 3:42:56 PM	192.168.0.150	35167	152.203.213.16	80	thelastwebpage.com	GET
3/7/2016 3:42:06 PM	192.168.0.133	62976	206.194.229.42	80	thebestwebsite.com	GET
3/7/2016 3:40:21 PM	192.168.0.225	45854	38.212.240.180	80	freefood.com	GET
3/7/2016 3:39:43 PM	192.168.0.128	44304	180.208.164.237	443	searchforus.de	GET
3/7/2016 3:37:58 PM	192.168.0.186	30386	82.190.10.236	80	securethenet.com	GET
3/7/2016 3:37:49 PM	192.168.0.123	42463	252.77.216.60	80	healthreport.com	GET
3/7/2016 3:35:59 PM	192.168.0.95	34447	133.136.173.36	80	anti-malware.com	GET
3/7/2016 3:35:38 PM	192.168.0.177	38107	100.3.194.158	80	healthreport.com	GET
3/7/2016 3:34:24 PM	192.168.0.189	42791	208.238.143.104	80	freefood.com	POST



SIEM Logs - SIEM 192.168.0.15								
Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	558	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	507	lsass.exe
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.168	kmatthews	1234	mailclient.exe
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1889	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	638	lsass.exe
Audit Success	3/7/2016 4:11:39 PM	4634	Logoff	An account was logged off.	192.168.0.82	gromney	682	lsass.exe
Audit Success	3/7/2016 4:11:28 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	1831	lsass.exe
Audit Success	3/7/2016 4:11:11 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	1912	lsass.exe
Audit Success	3/7/2016 4:10:48 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	635	explorer.exe

 View Phishing Email

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

How many workstations were infected?

Select the malware executable name.

mailclient.exe

winlogon.exe  
excel.exe  
iexplore.exe  
notepad.exe  
chrome.exe  
explorer.exe  
time.exe  
cmd.exe  
lsass.exe  
winword.exe  
outlook.exe  
**mailclient.exe**  
firefox.exe  
svchost.exe  
putty.exe

Internal Network

Email Server 192.168.0.20

File Server 192.168.0.102

SIEM 192.168.0.15

Internal Router 192.168.0.1

Proxy 192.168.0.50

192.168.0.0/24

Firewall

Internet

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

6 infected  
7 clicked isass.exe

**NEW QUESTION 86**

- (Exam Topic 2)

An organization supports a large number of remote users. Which of the following is the BEST option to protect the data on the remote users' laptops?

- A. Use whole disk encryption.
- B. Require the use of VPNs.
- C. Require employees to sign an NDA.
- D. implement a DLP solution.

**Answer:** A

**NEW QUESTION 91**

- (Exam Topic 2)

A security analyst is reviewing the network security monitoring logs listed below:

```
-----  
Count:2 Event#3.3505 2020-01-30 10:40 UTC  
GPL WEB_SERVER robots.txt access  
10.1.1.128 -> 10.0.0.10  
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704  
Protocol: 6 sport=45260 -> dport=80  
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=23415 chksum=0  
-----
```

```
Count:22 Event#3.3507 2020-01-30 10:40 UTC  
ET WEB_SPECIFIC_APPS PHPStudy Remote Code Execution Backdoor  
10.1.1.129 -> 10.0.0.10  
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704  
Protocol: 6 sport=65200 -> dport=80  
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=26814 chksum=0  
-----
```

```
Count:30 Event#3.3522 2020-01-30 10:40 UTC  
ET WEB_SERVER WEB-PHP phpinfo access  
10.1.1.130 -> 10.0.0.10  
IPVer=4 hlen=5 tos=0 dlen=269 ID=0 flags=0 offset=0 ttl=0 chksum=22704  
Protocol: 6 sport=58175 -> dport=80  
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=22875 chksum=0  
-----
```

```
Count:22 Event#3.3728 2020-01-30 10:40 UTC  
GPL WEB_SERVER 403 Forbidden  
10.0.0.10 -> 10.1.1.129  
IPVer=4 hlen=5 tos=0 dlen=533 ID=0 flags=0 offset=0 ttl=0 chksum=20471  
Protocol: 6 sport=80 -> dport=65200  
Seq=0 Ack=0 Off=5 Res=0 Flags=***** Win=0 urp=59638 chksum=0  
-----
```

Which of the following is the analyst MOST likely observing? (Select TWO).

- A. 10.1.1.128 sent malicious requests, and the alert is a false positive.
- B. 10.1.1.129 sent potential malicious requests to the web server.
- C. 10.1.1.129 sent non-malicious requests, and the alert is a false positive.
- D. 10.1.1.128 sent potential malicious traffic to the web server.
- E. 10.1.1.129 successfully exploited a vulnerability on the web server.

**Answer:** AC

**NEW QUESTION 93**

- (Exam Topic 2)

A security analyst is auditing firewall rules with the goal of scanning some known ports to check the firewall's behavior and responses. The analyst executes the following commands:

```
#nmap -p22 -sS 10.0.1.200  
#hping3 -S -c1 -p22 10.0.1.200
```

The analyst then compares the following results for port 22: nmap returns "Closed"

hping3 returns "flags=RA"

Which of the following BEST describes the firewall rule?

- A. DNAT --to-destination 1.1.1.1:3000



- B. REJECT with —tcp-reset
- C. LOG —log-tcp-sequence
- D. DROP

**Answer:** B

**Explanation:**

No doubt does the nmap result mean its being rejected as it returns closed. However, what threw me for a loop was the hping3 response. After further web surfing I found that the "flag=RA" means actually means "flag= RST, ACK" which means that it too was rejected.

**NEW QUESTION 98**

- (Exam Topic 2)

Which of the following data security controls would work BEST to prevent real PII from being used in an organization's test cloud environment?

- A. Digital rights management
- B. Encryption
- C. Access control
- D. Data loss prevention
- E. Data masking

**Answer:** E

**Explanation:**

Data masking is a way to create a fake, but a realistic version of your organizational data. The goal is to protect sensitive data, while providing a functional alternative when real data is not needed—for example, in user training, sales demos, or software testing.

**NEW QUESTION 102**

- (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 107**

- (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 111**

- (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 114**

- (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 115

- (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 118

- (Exam Topic 2)

A security team identified some specific known tactics and techniques to help mitigate repeated credential access threats, such as account manipulation and brute forcing. Which of the following frameworks or models did the security team MOST likely use to identify the tactics and techniques'?

- A. Kill chain
- B. Diamond Model of Intrusion Analysis
- C. MITRE ATT&CK
- D. ITIL

**Answer:** C

#### NEW QUESTION 119

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 122

- (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 126

- (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 130

- (Exam Topic 1)

An analyst is reviewing a list of vulnerabilities, which were reported from a recent vulnerability scan of a Linux server. Which of the following is MOST likely to be a false positive?

- A. OpenSSH/OpenSSL Package Random Number Generator Weakness
- B. Apache HTTP Server Byte Range DoS
- C. GDI+ Remote Code Execution Vulnerability (MS08-052)

- D. HTTP TRACE / TRACK Methods Allowed (002-1208)
- E. SSL Certificate Expiry

**Answer:** C

#### NEW QUESTION 132

- (Exam Topic 1)

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

- A. Establish an alternate site with active replication to other regions
- B. Configure a duplicate environment in the same region and load balance between both instances
- C. Set up every cloud component with duplicated copies and auto scaling turned on
- D. Create a duplicate copy on premises that can be used for failover in a disaster situation

**Answer:** A

#### NEW QUESTION 133

- (Exam Topic 1)

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

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

**Answer:** B

#### Explanation:

Reference: <https://www.secureworks.com/blog/advanced-persistent-threats-apt-b>

#### NEW QUESTION 136

- (Exam Topic 1)

A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-m-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 139

- (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 140

- (Exam Topic 1)

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

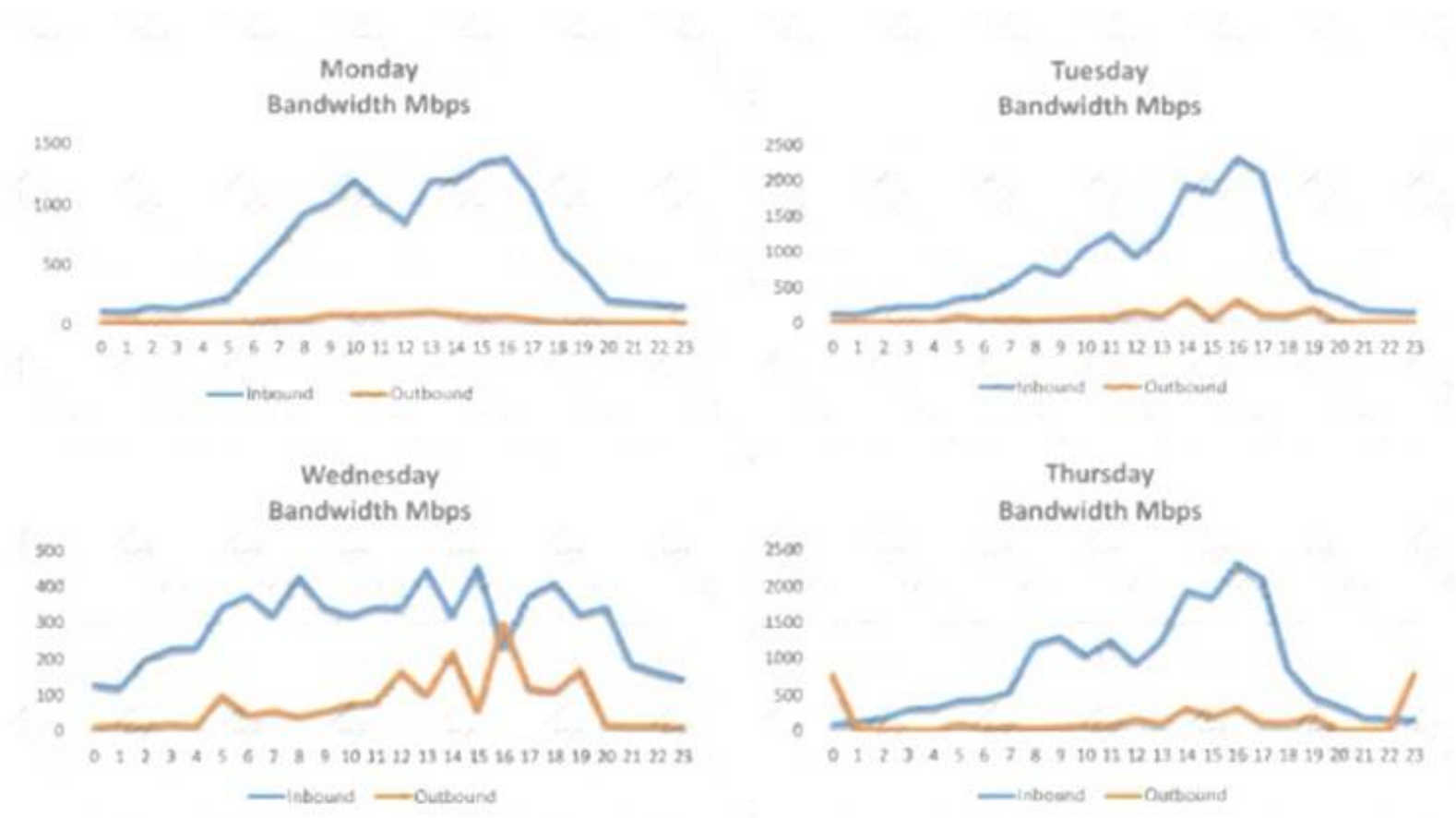
- A. Reverse engineering
- B. Application log collectors
- C. Workflow orchestration
- D. API integration
- E. Scripting

**Answer:** D

#### NEW QUESTION 145

- (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 150

- (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 153

- (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 154

- (Exam Topic 1)

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

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

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



This is an example of:

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

**Answer:** A

#### NEW QUESTION 158

- (Exam Topic 1)

A cybersecurity analyst is responding to an incident. The company's leadership team wants to attribute the incident to an attack group. Which of the following models would BEST apply to the situation?

- A. Intelligence cycle
- B. Diamond Model of Intrusion Analysis
- C. Kill chain
- D. MITRE ATT&CK

**Answer:** B

#### NEW QUESTION 161

- (Exam Topic 1)

As part of a review of modern response plans, which of the following is MOST important for an organization to understand when establishing the breach notification period?

- A. Organizational policies
- B. Vendor requirements and contracts
- C. Service-level agreements
- D. Legal requirements

**Answer:** D

#### NEW QUESTION 166

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 171

- (Exam Topic 1)

A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application. Which of the following is a security concern when using a PaaS solution?

- A. The use of infrastructure-as-code capabilities leads to an increased attack surface.
- B. Patching the underlying application server becomes the responsibility of the client.
- C. The application is unable to use encryption at the database level.
- D. Insecure application programming interfaces can lead to data compromise.

**Answer:** D

#### NEW QUESTION 175

- (Exam Topic 1)

Bootloader malware was recently discovered on several company workstations. All the workstations run Windows and are current models with UEFI capability. Which of the following UEFI settings is the MOST likely cause of the infections?

- A. Compatibility mode
- B. Secure boot mode
- C. Native mode
- D. Fast boot mode

**Answer:** A

#### NEW QUESTION 178

- (Exam Topic 1)

A development team signed a contract that requires access to an on-premises physical server. Access must be restricted to authorized users only and cannot be connected to the Internet. Which of the following solutions would meet this requirement?

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

**Answer:** D

#### NEW QUESTION 181

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 185

- (Exam Topic 1)

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

```
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.s/soap/envelope/ "><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-instance "></s:Body></s:Envelope> 192.168.1.22 - -
api.somesite.com 200 0 1006 1001 0 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap
<<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/><a:Username>somebody@companyname.com 192.168.5.66 - - api.somesite.com 200 0 11558
1712 2024 192.168.4.89
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation></s:Body>< 192.168.1.22 - - api.somesite.com 200 0 1003 1011
307 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><IsLoggedIn+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="
http://www.w3.org/2001/XMLSchema-instance"><a:Authentication>
<a:ApiToken>kmL4kr2CwwWBan5BReGv5Djb7syxXTNKcWfUjSjd</a:ApiToken><a:ImpersonateUserId>0
<a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authe 192.168.5.66 - - api.somesite.com 200 0 1378 1209
48 192.168.4.89
```

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

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

**Answer:** B

#### NEW QUESTION 190

- (Exam Topic 1)

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

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

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

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

**Answer:** B

#### NEW QUESTION 191

- (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 196**

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

Reference: <https://www.cybereason.com/blog/blog-the-eight-steps-to-threat-hunting>

**NEW QUESTION 200**

- (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 204**

- (Exam Topic 1)

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

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

**Answer:** A

**NEW QUESTION 206**

- (Exam Topic 1)

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

A)

```
BadReputationIp - - [2019-04-12 10:43:2] "GET /etc/passwd" 403 1023
```

B)

```
BadReputationIp - - [2019-04-12 10:43:2] "GET /index.html?src=../../ssh/id_rsa" 401 17044
```

C)

```
BadReputationIp - - [2019-04-12 10:43:2] "GET /a.php?src=/etc/passwd" 403 11056
```

D)

```
BadReputationIp - - [2019-04-12 10:43:2] "GET /a.php?src=../../ssh/id_rsa" 200 15036
```

E)

```
BadReputationIp - - [2019-04-12 10:43:2] "GET /favicon.ico?src=../usr/share/icons" 200 19064
```

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



**Answer:** D

#### NEW QUESTION 209

- (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 214

- (Exam Topic 1)

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

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

**Answer:** A

#### Explanation:

Reference: <https://bluedot.io/library/what-is-geofencing/>

#### NEW QUESTION 219

- (Exam Topic 1)

A security analyst is supporting an embedded software team. Which of the following is the BEST recommendation to ensure proper error handling at runtime?

- A. Perform static code analysis.
- B. Require application fuzzing.
- C. Enforce input validation
- D. Perform a code review

**Answer:** B

#### NEW QUESTION 221

- (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/la -l /proc/1301/exe
- D. kill -9 1301

**Answer:** A

#### NEW QUESTION 224

- (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 229

- (Exam Topic 1)

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

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

Which of the following is MOST likely a false positive?

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

**Answer:** B

#### NEW QUESTION 231

- (Exam Topic 1)

A security analyst is investigating malicious traffic from an internal system that attempted to download proxy avoidance software as identified from the firewall logs but the destination IP is blocked and not captured. Which of the following should the analyst do?

- A. Shut down the computer
- B. Capture live data using Wireshark
- C. Take a snapshot
- D. Determine if DNS logging is enabled.
- E. Review the network logs.

**Answer:** D

#### Explanation:

The DNS debug log provides extremely detailed data about all DNS information that is sent and received by the DNS server, similar to the data that can be gathered using packet capture tools such as network monitor.

<https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn80066>

#### NEW QUESTION 236

- (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 239

- (Exam Topic 1)

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

Tool A reported the following:

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

Tool B reported the following:

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

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

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

**Answer:** CE

#### NEW QUESTION 244

- (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 246

- (Exam Topic 1)

It is important to parameterize queries to prevent:

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

**Answer:** A

#### Explanation:

Reference: <https://stackoverflow.com/QUESTION NO:s/4712037/what-is-parameterized-query>

#### NEW QUESTION 251

- (Exam Topic 3)

A company's security team recently discovered a number of workstations that are at the end of life. The workstation vendor informs the team that the product is no longer supported and patches are no longer available. The company is not prepared to cease its use of these workstations. Which of the following would be the BEST method to protect these workstations from threats?

- A. Deploy whitelisting to the identified workstations to limit the attack surface.
- B. Determine the system process criticality and document it.
- C. Isolate the workstations and air gap them when it is feasible.
- D. Increase security monitoring on the workstations.

**Answer:** C

#### NEW QUESTION 253

- (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 254

- (Exam Topic 3)

A security analyst is concerned the number of security incidents being reported has suddenly gone down. Daily business interactions have not changed, and no following should the analyst review FIRST?

- A. The DNS configuration
- B. Privileged accounts
- C. The IDS rule set
- D. The firewall ACL

**Answer:** C

#### NEW QUESTION 259

- (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 260**

- (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 264**

- (Exam Topic 3)

Industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacks used privilege escalation to gain access to SCADA administration and access management solutions would help to mitigate this risk?

- A. Multifactor authentication
- B. Manual access reviews
- C. Endpoint detection and response
- D. Role-based access control

**Answer:** C

**NEW QUESTION 265**

- (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 269**

- (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 273**

- (Exam Topic 3)

A vulnerability scanner has identified an out-of-support database software version running on a server. The software update will take six to nine months to complete. The management team has agreed to a one-year extended support contract with the software vendor. Which of the following BEST describes the risk treatment in this scenario?

- A. The extended support mitigates any risk associated with the software.
- B. The extended support contract changes this vulnerability finding to a false positive.
- C. The company is transferring the risk for the vulnerability to the software vendor.
- D. The company is accepting the inherent risk of the vulnerability.

**Answer:** D

**Explanation:**

Risk Acceptance

o A risk response that involves determining that a risk is within the organization's risk appetite and no countermeasures other than ongoing monitoring will be needed Mitigation

Control Avoidance Changing plans Transference Insurance Acceptance Low risk

**NEW QUESTION 274**

- (Exam Topic 3)

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

```
[root@localhost /root]# 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 > 128.50.100.23.80  
10.254.2.25.6782 > 128.50.100.23.80  
10.254.2.25.6783 > 128.50.100.23.80  
10.254.2.25.6784 > 128.50.100.23.80
```

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 275

- (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: A**

#### NEW QUESTION 276

- (Exam Topic 3)

A security analyst is scanning the network to determine if a critical security patch was applied to all systems in an enterprise. The Organization has a very low tolerance for risk when it comes to resource availability. Which of the following is the BEST approach for configuring and scheduling the scan?

- A. Make sure the scan is credentialed, covers all hosts in the patch management system, and is scheduled during business hours so it can be terminated if it affects business operations.
- B. Make sure the scan is uncredentialed, covers all hosts in the patch management system, and is scheduled during off-business hours so it has the least impact on operations.
- C. Make sure the scan is credentialed, has the latest software and signature versions, covers all external hosts in the patch management system and is scheduled during off-business hours so it has the least impact on operations.
- D. Make sure the scan is credentialed, uses a trusted plug-in set, scans all host IP addresses in the enterprise, and is scheduled during off-business hours so it has the least impact on operations.

**Answer: D**

#### NEW QUESTION 281

- (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 to reduce the likelihood 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 285

- (Exam Topic 3)

A security analyst is correlating, ranking, and enriching raw data into a report that will be interpreted by humans or machines to draw conclusions and create actionable recommendations Which of the following steps in the intelligence cycle is the security analyst performing?

- A. Analysis and production
- B. Processing and exploitation
- C. Dissemination and evaluation
- D. Data collection
- E. Planning and direction

**Answer:** A

**Explanation:**

Analysis is a human process that turns processed information into intelligence that can inform decisions. Depending on the circumstances, the decisions might involve whether to investigate a potential threat, what actions to take immediately to block an attack, how to strengthen security controls, or how much investment in additional security resources is justified. <https://www.recordedfuture.com/threat-intelligence-lifecycle-phases>

**NEW QUESTION 286**

- (Exam Topic 3)

A company's domain has been spoofed 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 is 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 290**

- (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 291**

- (Exam Topic 3)

A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

- A. Deterrent
- B. Preventive
- C. Compensating
- D. Detective

**Answer:** C

**Explanation:**

A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time.

"Compensating controls are additional security measures that you take to address a vulnerability without remediating the underlying issue."

**NEW QUESTION 294**

- (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 296**

- (Exam Topic 3)

Which of the following factors would determine the regulations placed on data under data sovereignty laws?



- A. What the company intends to do with the data it owns
- B. The company's data security policy
- C. The type of data the company stores
- D. The data laws of the country in which the company is located

Answer: D

### NEW QUESTION 297

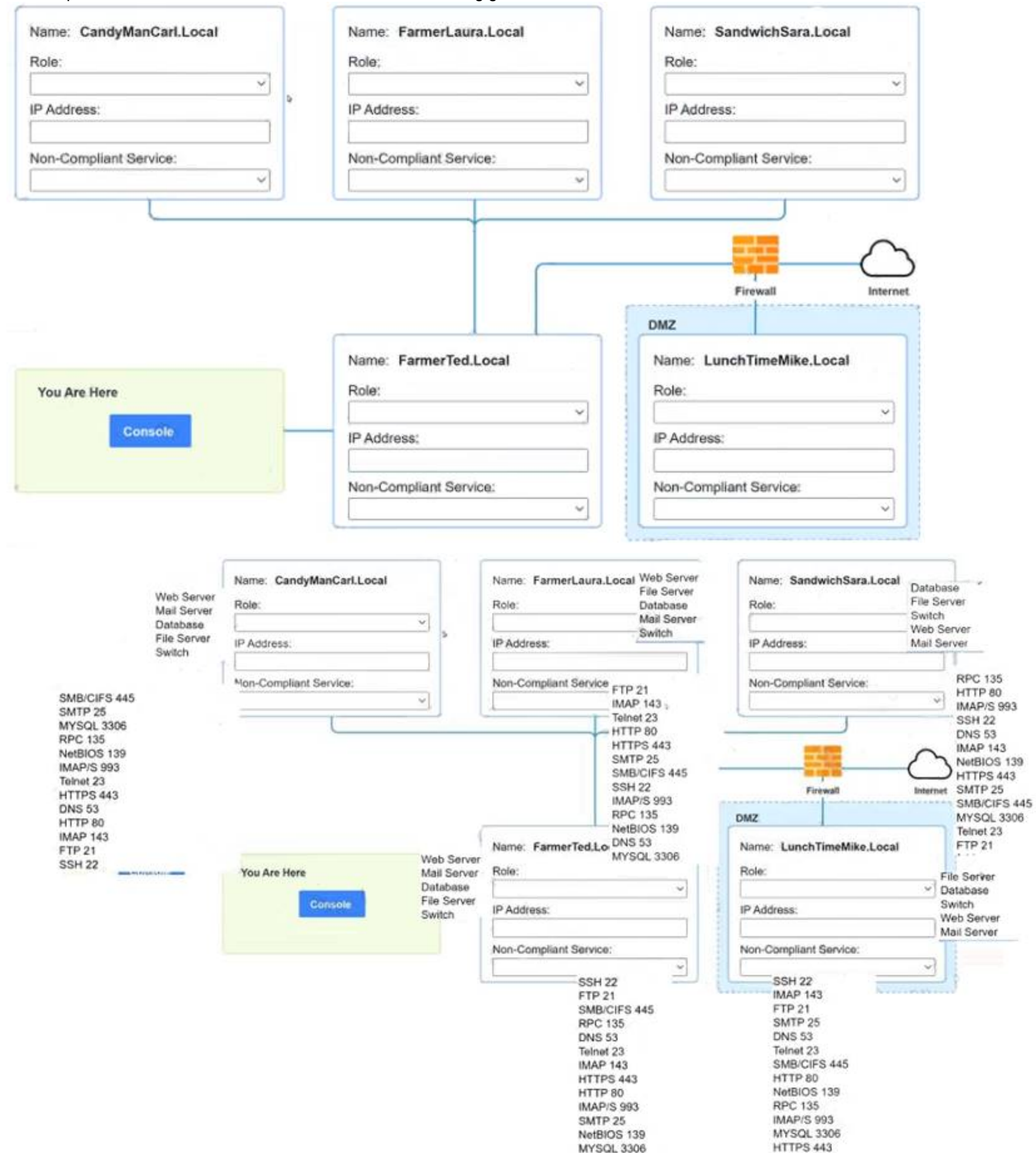
- (Exam Topic 3)

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

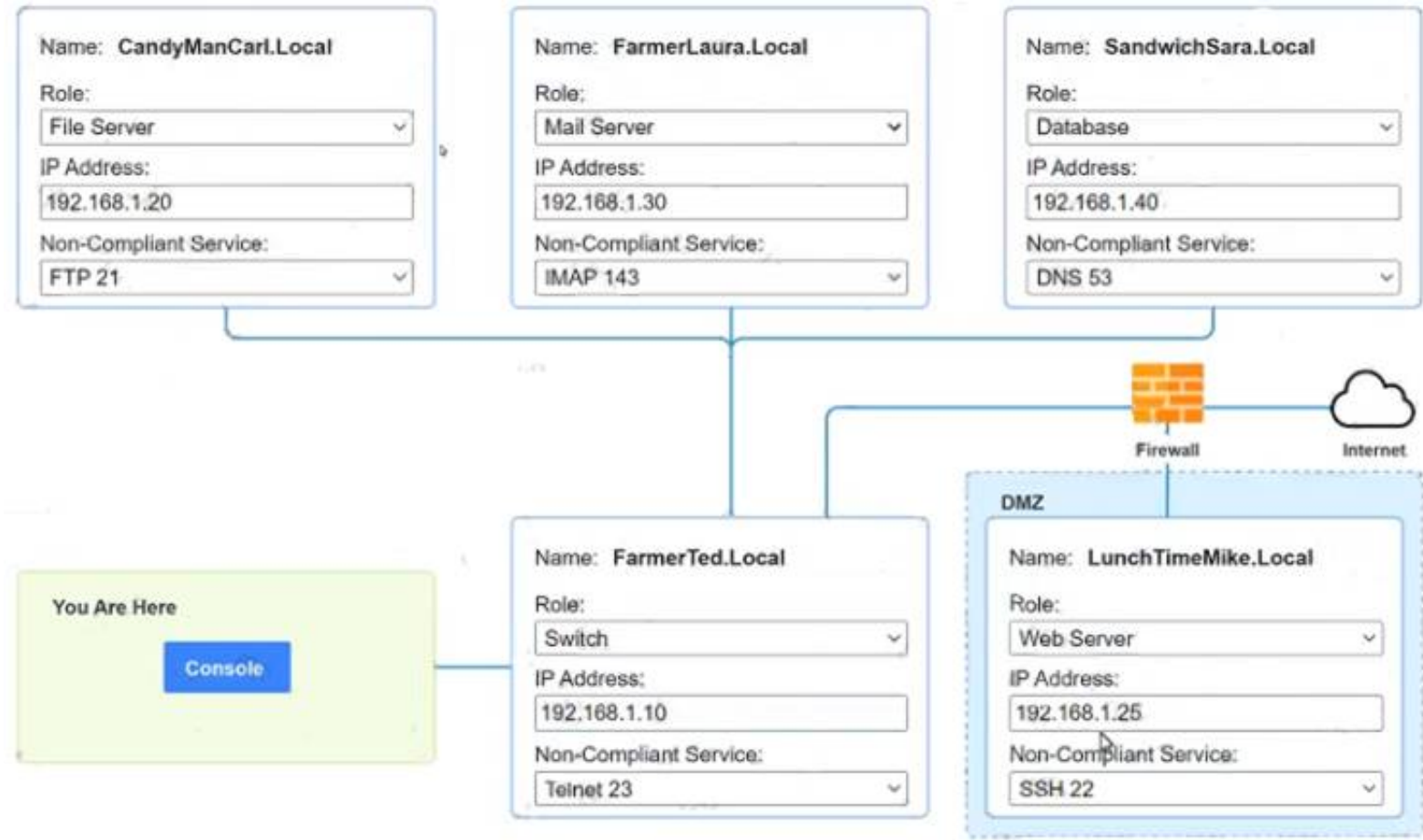


A. Mastered

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 301

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

### CS0-002 Practice Exam Features:

- \* CS0-002 Questions and Answers Updated Frequently
- \* CS0-002 Practice Questions Verified by Expert Senior Certified Staff
- \* CS0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CS0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CS0-002 Practice Test Here](#)**