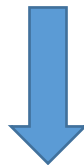


CompTIA CySA+ Certification CS0-001 Exam



- Vendor: CompTIA
- Exam Code: CS0-001
- Exam Name: CompTIA Cybersecurity Analyst (CySA+)

Get Complete Version Exam CS0-001 Dumps with VCE and PDF Here



<https://www.passleader.com/cs0-001.html>

QUESTION 1

Which of the following BEST describes the offensive participants in a tabletop exercise?

- A. Red team
- B. Blue team
- C. System administrators
- D. Security analysts
- E. Operations team

Answer: A

QUESTION 2

After analyzing and correlating activity from multiple sensors, the security analyst has determined a group from a high-risk country is responsible for a sophisticated breach of the company network and continuous administration of targeted attacks for the past three months. Until now, the attacks went unnoticed. This is an example of ____.

- A. privilege escalation
- B. advanced persistent threat
- C. malicious insider threat
- D. spear phishing

Answer: B

QUESTION 3

A system administrator who was using an account with elevated privileges deleted a large amount of log files generated by a virtual hypervisor in order to free up disk space. These log files are needed by the security team to analyze the health of the virtual machines. Which of the following compensating controls would help prevent this from reoccurring? (Select TWO.)

- A. Succession planning
- B. Separation of duties
- C. Mandatory vacation
- D. Personnel training
- E. Job rotation

Answer: BD

QUESTION 4

A security analyst received a compromised workstation. The workstation's hard drive may contain evidence of criminal activities. Which of the following is the FIRST thing the analyst must do to ensure the integrity of the hard drive while performing the analysis?

- A. Make a copy of the hard drive.
- B. Use write blockers.
- C. Runrm -Rcommand to create a hash.
- D. Install it on a different machine and explore the content.

Answer: B

QUESTION 5

File integrity monitoring states the following files have been changed without a written request or

approved change. The following change has been made:

```
chmod 777 -Rv /usr
```

Which of the following may be occurring?

- A. The ownership of /usr has been changed to the current user.
- B. Administrative functions have been locked from users.
- C. Administrative commands have been made world readable/writable.
- D. The ownership of /usr has been changed to the root user.

Answer: C

QUESTION 6

A security analyst has created an image of a drive from an incident. Which of the following describes what the analyst should do NEXT?

- A. The analyst should create a backup of the drive and then hash the drive.
- B. The analyst should begin analyzing the image and begin to report findings.
- C. The analyst should create a hash of the image and compare it to the original drive's hash.
- D. The analyst should create a chain of custody document and notify stakeholders.

Answer: C

QUESTION 7

An organization is requesting the development of a disaster recovery plan. The organization has grown and so has its infrastructure. Documentation, policies, and procedures do not exist. Which of the following steps should be taken to assist in the development of the disaster recovery plan?

- A. Conduct a risk assessment.
- B. Develop a data retention policy.
- C. Execute vulnerability scanning.
- D. Identify assets.

Answer: D

QUESTION 8

A company wants to update its acceptable use policy (AUP) to ensure it relates to the newly implemented password standard, which requires sponsored authentication of guest wireless devices. Which of the following is MOST likely to be incorporated in the AUP?

- A. Sponsored guest passwords must be at least ten characters in length and contain a symbol.
- B. The corporate network should have a wireless infrastructure that uses open authentication standards.
- C. Guests using the wireless network should provide valid identification when registering their wireless devices.
- D. The network should authenticate all guest users using 802.1x backed by a RADIUS or LDAP server.

Answer: C

QUESTION 9

An analyst was tasked with providing recommendations of technologies that are PKI X.509 compliant for a variety of secure functions. Which of the following technologies meet the compatibility requirement? (Select THREE.)

- A. 3DES

- B. AES
- C. IDEA
- D. PKCS
- E. PGP
- F. SSL/TLS
- G. TEMPEST

Answer: BDF

QUESTION 10

After completing a vulnerability scan, the following output was noted:

```
CVE-2011-3389  
QID 42366 - SSLv3.0 / TLSv1.0 Protocol weak CBC mode Server side vulnerability  
  
Check with:  
  
openssl s_client -connect qualys.jive.mobile.com:443 -tls1 -cipher "AES:CAMELLIA:SEED:3DES:DES"
```

Which of the following vulnerabilities has been identified?

- A. PKI transfer vulnerability.
- B. Active Directory encryption vulnerability.
- C. Web application cryptography vulnerability.
- D. VPN tunnel vulnerability.

Answer: A

QUESTION 11

A security analyst is adding input to the incident response communication plan. A company officer has suggested that if a data breach occurs, only affected parties should be notified to keep an incident from becoming a media headline. Which of the following should the analyst recommend to the company officer?

- A. The first responder should contact law enforcement upon confirmation of a security incident in order for a forensics team to preserve chain of custody.
- B. Guidance from laws and regulations should be considered when deciding who must be notified in order to avoid fines and judgements from non-compliance.
- C. An externally hosted website should be prepared in advance to ensure that when an incident occurs victims have timely access to notifications from a non-compromised recourse.
- D. The HR department should have information security personnel who are involved in the investigation of the incident sign non-disclosure agreements so the company cannot be held liable for customer data that might be viewed during an investigation.

Answer: A

QUESTION 12

A company has recently launched a new billing invoice website for a few key vendors. The cybersecurity analyst is receiving calls that the website is performing slowly and the pages sometimes time out. The analyst notices the website is receiving millions of requests, causing the service to become unavailable. Which of the following can be implemented to maintain the availability of the website?

- A. VPN

- B. Honeypot
- C. Whitelisting
- D. DMZ
- E. MAC filtering

Answer: C

QUESTION 13

A cybersecurity analyst has received the laptop of a user who recently left the company. The analyst types `history` into the prompt, and sees this line of code in the latest bash history:

```
> for i in seq 255; ping -c 1 192.168.0.$i; done
```

This concerns the analyst because this subnet should not be known to users within the company. Which of the following describes what this code has done on the network?

- A. Performed a ping sweep of the Class C network.
- B. Performed a half open SYB scan on the network.
- C. Sent 255 ping packets to each host on the network.
- D. Sequentially sent an ICMP echo reply to the Class C network.

Answer: A

QUESTION 14

A security audit revealed that port 389 has been used instead of 636 when connecting to LDAP for the authentication of users. The remediation recommended by the audit was to switch the port to 636 wherever technically possible. Which of the following is the BEST response?

- A. Correct the audit. This finding is a well-known false positive; the services that typically run on 389 and 636 are identical.
- B. Change all devices and servers that support it to 636, as encrypted services run by default on 636.
- C. Change all devices and servers that support it to 636, as 389 is a reserved port that requires root access and can expose the server to privilege escalation attacks.
- D. Correct the audit. This finding is accurate, but the correct remediation is to update encryption keys on each of the servers to match port 636.

Answer: B

QUESTION 15

A security analyst is reviewing IDS logs and notices the following entry:

```
(where email=john@john.com and password=' or 20==20')
```

Which of the following attacks is occurring?

- A. Cross-site scripting
- B. Header manipulation
- C. SQL injection
- D. XML injection

Answer: C

QUESTION 16

A company that is hiring a penetration tester wants to exclude social engineering from the list of authorized activities. Which of the following documents should include these details?

- A. Acceptable use policy
- B. Service level agreement
- C. Rules of engagement
- D. Memorandum of understanding
- E. Master service agreement

Answer: B

QUESTION 17

A reverse engineer was analyzing malware found on a retailer's network and found code extracting track data in memory. Which of the following threats did the engineer MOST likely uncover?

- A. POS malware
- B. Rootkit
- C. Key logger
- D. Ransomware

Answer: A

QUESTION 18

Due to new regulations, a company has decided to institute an organizational vulnerability management program and assign the function to the security team. Which of the following frameworks would BEST support the program? (Select TWO.)

- A. COBIT
- B. NIST
- C. ISO 27000 series
- D. ITIL
- E. OWASP

Answer: DE

QUESTION 19

A system administrator recently deployed and verified the installation of a critical patch issued by the company's primary OS vendor. This patch was supposed to remedy a vulnerability that would allow an adversary to remotely execute code from over the network. However, the administrator just ran a vulnerability assessment of networked systems, and each of them still reported having the same vulnerability. Which of the following is the MOST likely explanation for this?

- A. The administrator entered the wrong IP range for the assessment.
- B. The administrator did not wait long enough after applying the patch to run the assessment.
- C. The patch did not remediate the vulnerability.
- D. The vulnerability assessment returned false positives.

Answer: C

QUESTION 20

An incident response report indicates a virus was introduced through a remote host that was

connected to corporate resources. A cybersecurity analyst has been asked for a recommendation to solve this issue. Which of the following should be applied?

- A. MAC
- B. TAP
- C. NAC
- D. ACL

Answer: C

QUESTION 21

Review the following results:

Source	Destination	Protocol	Length	Info
172.29.0.109	8.8.8.8	DNS	74	Standard query 0x9ada A itsec.eicp.net
8.8.8.8	172.29.0.109	DNS	90	Standard query response 0x9ada A itsec.eicp.net A 123.120.110.212
172.29.0.109	123.120.110.212	TCP	78	49294 - 8088 [SYN] seq=0 Win=65635 Len=0 MSS=1460 WS=16 TSval=560397766 Tsecr=0 SACK_PERM=1
123.120.110.212	172.29.0.109	TCP	78	8088-49294 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=OMSS=1426 WS=4 TSval=0 Tsecr=0 SACK_PERM=1al=560402112 TSecr=240871
172.29.0.109	172.29.0.255	NBNS	92	Namequery NB WORKGROUP<ID>
54.240.190.21	172.29.0.109	TCP	60	443 - 49294 [RST] Seq=1 Win=0 Len=0
66.235.133.62	172.29.0.109	TCP	60	80 - 49294 [RST] Seq=1 Win=0 Len=0
123.120.110.212	172.29.0.109	TCP	67	8088-49294 [PSH, ACK] Seq=459 ACK=347 Win 255204 Len=1 TSval=241898 TSecr=560402112
172.29.0.109	123.120.110.212	TCP	66	49294-8088 [ACK] Seq=347 Ack=460 Win=131056 Len=0 TSval=560504900 TSecr=241898

Which of the following has occurred?

- A. This is normal network traffic.
- B. 123.120.110.212 is infected with a Trojan.
- C. 172.29.0.109 is infected with a worm.
- D. 172.29.0.109 is infected with a Trojan.

Answer: A

QUESTION 22

A security analyst is creating baseline system images to remediate vulnerabilities found in different operating systems. Each image needs to be scanned before it is deployed. The security analyst must ensure the configurations match industry standard benchmarks and the process can be repeated frequently. Which of the following vulnerability options would BEST create the process requirements?

- A. Utilizing an operating system SCAP plugin
- B. Utilizing an authorized credential scan
- C. Utilizing a non-credential scan
- D. Utilizing a known malware plugin

Answer: A

QUESTION 23

A network technician is concerned that an attacker is attempting to penetrate the network, and wants to set a rule on the firewall to prevent the attacker from learning which IP addresses are valid on the network. Which of the following protocols needs to be denied?

- A. TCP
- B. SMTP

- C. ICMP
- D. ARP

Answer: C

QUESTION 24

An analyst wants to use a command line tool to identify open ports and running services on a host along with the application that is associated with those services and port. Which of the following should the analyst use?

- A. Wireshark
- B. Qualys
- C. Netstat
- D. Nmap
- E. Ping

Answer: C

QUESTION 25

In order to meet regulatory compliance objectives for the storage of PHI, vulnerability scans must be conducted on a continuous basis. The last completed scan of the network returned 5,682 possible vulnerabilities. The Chief Information Officer (CIO) would like to establish a remediation plan to resolve all known issues. Which of the following is the BEST way to proceed?

- A. Attempt to identify all false positives and exceptions, and then resolve all remaining items.
- B. Hold off on additional scanning until the current list of vulnerabilities have been resolved.
- C. Place assets that handle PHI in a sandbox environment, and then resolve all vulnerabilities.
- D. Reduce the scan to items identified as critical in the asset inventory, and resolve these issues first.

Answer: D

QUESTION 26

An administrator has been investigating the way in which an actor had been exfiltrating confidential data from a web server to a foreign host. After a thorough forensic review, the administrator determined the server's BIOS had been modified by rootkit installation. After removing the rootkit and flashing the BIOS to a known good state, which of the following would BEST protect against future adversary access to the BIOS, in case another rootkit is installed?

- A. Anti-malware application
- B. Host-based IDS
- C. TPM data sealing
- D. File integrity monitoring

Answer: C

QUESTION 27

A security analyst is reviewing the following log after enabling key-based authentication:


```
Dec 21 11:00:57 comptia sshd[5657]: Failed password for root from
95.58.255.62 port 38980 ssh2
Dec 21 20:08:26 comptia sshd[5768]: Failed password for root from
91.205.189.15 port 38156 ssh2
Dec 21 20:08:30 comptia sshd[5770]: Failed password for nobody from
91.205.189.15 port 38556 ssh2
Dec 21 20:08:34 comptia sshd[5772]: Failed password for invalid user
asterisk from 91.205.189.15 port 38864 ssh2
Dec 21 20:08:38 comptia sshd[5774]: Failed password for invalid user
sjobeck from 91.205.189.15 port 39157 ssh2
Dec 21 20:08:42 comptia sshd[5776]: Failed password for root from
91.205.189.15 port 39467 ssh2
```

Given the above information, which of the following steps should be performed NEXT to secure the system?

- A. Disable anonymous SSH logins.
- B. Disable password authentication for SSH.
- C. Disable SSHv1.
- D. Disable remote root SSH logins.

Answer: B

QUESTION 28

A cybersecurity analyst has received a report that multiple systems are experiencing slowness as a result of a DDoS attack. Which of the following would be the BEST action for the cybersecurity analyst to perform?

- A. Continue monitoring critical systems.
- B. Shut down all server interfaces.
- C. Inform management of the incident.
- D. Inform users regarding the affected systems.

Answer: C

QUESTION 29

A security professional is analyzing the results of a network utilization report. The report includes the following information:

IP Address	Server Name	Server Uptime	Historical	Current
172.20.2.58	web.srvr.03	30D 12H 52M 09S	41.3GB	37.2GB
172.20.1.215	dev.web.srvr.01	30D 12H 52M 09S	1.81GB	2.2GB
172.20.1.22	hr.dbprod.01	30D 12H 17M 22S	2.24GB	29.97GB
172.20.1.26	mrktg.file.srvr.02	30D 12H 41M 09S	1.23GB	0.34GB
172.20.1.28	acctn.file.srvr.01	30D 12H 52M 09S	3.62GB	3.57GB
172.20.1.30	R&D.file.srvr.01	1D 4H 22M 01S	1.24GB	0.764GB

Which of the following servers needs further investigation?

- A. hr.dbprod.01
- B. R&D.file.srvr.01
- C. mrktg.file.srvr.02
- D. web.srvr.03

Answer: B

QUESTION 30

A cybersecurity analyst has several SIEM event logs to review for possible APT activity. The analyst was given several items that include lists of indicators for both IP addresses and domains. Which of the following actions is the BEST approach for the analyst to perform?

- A. Use the IP addresses to search through the event logs.
- B. Analyze the trends of the events while manually reviewing to see if any of the indicators match.
- C. Create an advanced query that includes all of the indicators, and review any of the matches.
- D. Scan for vulnerabilities with exploits known to have been used by an APT.

Answer: B

QUESTION 31

A system administrator has reviewed the following output:

```
#nmap server.local
Nmap scan report for server.local (10.10.2.5)
Host is up (0.3452354s latency)
Not shown:997 closed ports

PORT      STATE      Service
22/tcp    open      ssh
80/tcp    open      http

#nc server.local 80
220 server.local Company SMTP server (Postfix/2.3.3)
#nc server.local 22
SSH-2.0-OpenSSH_7.1p2 Debian-2
#
```

Which of the following can a system administrator infer from the above output?

- A. The company email server is running a non-standard port.
- B. The company email server has been compromised.
- C. The company is running a vulnerable SSH server.
- D. The company web server has been compromised.

Answer: A

QUESTION 32

An analyst has received unusual alerts on the SIEM dashboard. The analyst wants to get payloads that the hackers are sending toward the target systems without impacting the business operation. Which of the following should the analyst implement?

- A. Honeypot
- B. Jump box
- C. Sandboxing
- D. Virtualization

Answer: A

QUESTION 33

An analyst finds that unpatched servers have undetected vulnerabilities because the vulnerability

scanner does not have the latest set of signatures. Management directed the security team to have personnel update the scanners with the latest signatures at least 24 hours before conducting any scans, but the outcome is unchanged. Which of the following is the BEST logical control to address the failure?

- A. Configure a script to automatically update the scanning tool.
- B. Manually validate that the existing update is being performed.
- C. Test vulnerability remediation in a sandbox before deploying.
- D. Configure vulnerability scans to run in credentialed mode.

Answer: A

QUESTION 34

A cybersecurity analyst has received an alert that well-known "call home" messages are continuously observed by network sensors at the network boundary. The proxy firewall successfully drops the messages. After determining the alert was a true positive, which of the following represents the MOST likely cause?

- A. Attackers are running reconnaissance on company resources.
- B. Commands are attempting to reach a system infected with a botnet trojan.
- C. An insider is trying to exfiltrate information to a remote network.
- D. Malware is running on a company system.

Answer: B

QUESTION 35

Which of the following items represents a document that includes detailed information on when an incident was detected, how impactful the incident was, and how it was remediated, in addition to incident response effectiveness and any identified gaps needing improvement?

- A. Forensic analysis report
- B. Chain of custody report
- C. Trends analysis report
- D. Lessons learned report

Answer: A

QUESTION 36

After scanning the main company's website with the OWASP ZAP tool, a cybersecurity analyst is reviewing the following warning:

```
The AUTOCOMPLETE output is not disabled in HTML FORM/INPUT  
containing password type input. Passwords may be stored in  
browsers and retrieved.
```

The analyst reviews a snippet of the offending code:

```
<form action="authenticate.php">  
  Username:<br>  
  <input type="text" name="username" value="" autofocus><br>  
  Password: <br>  
  <input type="password" name="password" value="" maxlength="32"><br>  
  <input type="submit" value="submit">  
</form>
```

Which of the following is the BEST course of action based on the above warning and code snippet?

- A. The analyst should implement a scanner exception for the false positive.
- B. The system administrator should disable SSL and implement TLS.
- C. The developer should review the code and implement a code fix.
- D. The organization should update the browser GPO to resolve the issue.

Answer: D

QUESTION 37

An alert has been distributed throughout the information security community regarding a critical Apache vulnerability. Which of the following courses of action would ONLY identify the known vulnerability?

- A. Perform an unauthenticated vulnerability scan on all servers in the environment.
- B. Perform a scan for the specific vulnerability on all web servers.
- C. Perform a web vulnerability scan on all servers in the environment.
- D. Perform an authenticated scan on all web servers in the environment.

Answer: B

QUESTION 38

Which of the following commands would a security analyst use to make a copy of an image for forensics use?

- A. dd
- B. wget
- C. touch
- D. rm

Answer: A

QUESTION 39

As part of an upcoming engagement for a client, an analyst is configuring a penetration testing application to ensure the scan complies with information defined in the SOW. Which of the following types of information should be considered based on information traditionally found in the SOW? (Select TWO.)

- A. Timing of the scan
- B. Contents of the executive summary report
- C. Excluded hosts
- D. Maintenance windows
- E. IPS configuration

F. Incident response policies

Answer: AC

QUESTION 40

An HR employee began having issues with a device becoming unresponsive after attempting to open an email attachment. When informed, the security analyst became suspicious of the situation, even though there was not any unusual behavior on the IDS or any alerts from the antivirus software. Which of the following BEST describes the type of threat in this situation?

- A. Packet of death
- B. Zero-day malware
- C. PII exfiltration
- D. Known virus

Answer: B

QUESTION 41

An organization wants to remediate vulnerabilities associated with its web servers. An initial vulnerability scan has been performed, and analysts are reviewing the results. Before starting any remediation, the analysts want to remove false positives to avoid spending time on issues that are not actual vulnerabilities. Which of the following would be an indicator of a likely false positive?

- A. Reports show the scanner compliance plug-in is out-of-date.
- B. Any items labeled 'low' are considered informational only.
- C. The scan result version is different from the automated asset inventory.
- D. HTTPS entries indicate the web page is encrypted securely.

Answer: B

QUESTION 42

Company A permits visiting business partners from Company B to utilize Ethernet ports available in Company A's conference rooms. This access is provided to allow partners the ability to establish VPNs back to Company B's network. The security architect for Company A wants to ensure partners from Company B are able to gain direct Internet access from available ports only, while Company A employees can gain access to the Company A internal network from those same ports. Which of the following can be employed to allow this?

- A. ACL
- B. SIEM
- C. MAC
- D. NAC
- E. SAML

Answer: A

QUESTION 43

After reviewing the following packet, a cybersecurity analyst has discovered an unauthorized service is running on a company's computer:

```
16:26:42.943463 IP 192.168.1.10:25 > 10.38.219.20:3389 Flags  
[P.], seq 1768:1901, ackl, win 511, options [nop,nop,TS val  
271989777 ecr 475239494], length 133
```

Which of the following ACLs, if implemented, will prevent further access ONLY to the unauthorized service and will not impact other services?

- A. DENY TCP ANY HOST 10.38.219.20 EQ 3389
- B. DENY IP HOST 10.38.219.20 ANY EQ 25
- C. DENY IP HOST 192.168.1.10 HOST 10.38.219.20 EQ 3389
- D. DENY TCP ANY HOST 192.168.1.10 EQ 25

Answer: A

QUESTION 44

The new Chief Technology Officer (CTO) is seeking recommendations for network monitoring services for the local intranet. The CTO would like the capability to monitor all traffic to and from the gateway, as well as the capability to block certain content. Which of the following recommendations would meet the needs of the organization?

- A. Recommend setup of IP filtering on both the internal and external interfaces of the gateway router.
- B. Recommend installation of an IDS on the internal interface and a firewall on the external interface of the gateway router.
- C. Recommend installation of a firewall on the internal interface and a NIDS on the external interface of the gateway router.
- D. Recommend installation of an IPS on both the internal and external interfaces of the gateway router.

Answer: C

QUESTION 45

While a threat intelligence analyst was researching an indicator of compromise on a search engine, the web proxy generated an alert regarding the same indicator. The threat intelligence analyst states that related sites were not visited but were searched for in a search engine. Which of the following MOST likely happened in this situation?

- A. The analyst is not using the standard approved browser.
- B. The analyst accidentally clicked a link related to the indicator.
- C. The analyst has prefetch enabled on the browser in use.
- D. The alert is unrelated to the analyst's search.

Answer: C

QUESTION 46

An analyst is observing unusual network traffic from a workstation. The workstation is communicating with a known malicious site over an encrypted tunnel. A full antivirus scan with an updated antivirus signature file does not show any sign of infection. Which of the following has occurred on the workstation?

- A. Zero-day attack
- B. Known malware attack
- C. Session hijack

D. Cookie stealing

Answer: A

QUESTION 47

A university wants to increase the security posture of its network by implementing vulnerability scans of both centrally managed and student/employee laptops. The solution should be able to scale, provide minimum false positives and high accuracy of results, and be centrally managed through an enterprise console. Which of the following scanning topologies is BEST suited for this environment?

- A. A passive scanning engine located at the core of the network infrastructure
- B. A combination of cloud-based and server-based scanning engines
- C. A combination of server-based and agent-based scanning engines
- D. An active scanning engine installed on the enterprise console

Answer: D

QUESTION 48

A cybersecurity analyst is completing an organization's vulnerability report and wants it to reflect assets accurately. Which of the following items should be in the report?

- A. Processor utilization
- B. Virtual hosts
- C. Organizational governance
- D. Log disposition
- E. Asset isolation

Answer: B

QUESTION 49

A threat intelligence feed has posted an alert stating there is a critical vulnerability in the kernel. Unfortunately, the company's asset inventory is not current. Which of the following techniques would a cybersecurity analyst perform to find all affected servers within an organization?

- A. A manual log review from data sent to syslog
- B. An OS fingerprinting scan across all hosts
- C. A packet capture of data traversing the server network
- D. A service discovery scan on the network

Answer: B

QUESTION 50

A cybersecurity analyst traced the source of an attack to compromised user credentials. Log analysis revealed that the attacker successfully authenticated from an unauthorized foreign country. Management asked the security analyst to research and implement a solution to help mitigate attacks based on compromised passwords. Which of the following should the analyst implement?

- A. Self-service password reset
- B. Single sign-on
- C. Context-based authentication
- D. Password complexity

Answer: C

QUESTION 51

A technician is running an intensive vulnerability scan to detect which ports are open to exploit. During the scan, several network services are disabled and production is affected. Which of the following sources would be used to evaluate which network service was interrupted?

- A. Syslog
- B. Network mapping
- C. Firewall logs
- D. NIDS

Answer: A

QUESTION 52

A software patch has been released to remove vulnerabilities from company's software. A security analyst has been tasked with testing the software to ensure the vulnerabilities have been remediated and the application is still functioning properly. Which of the following tests should be performed NEXT?

- A. Fuzzing
- B. User acceptance testing
- C. Regression testing
- D. Penetration testing

Answer: C

QUESTION 53

During a routine review of firewall logs, an analyst identified that an IP address from the organization's server subnet had been connecting during nighttime hours to a foreign IP address, and had been sending between 150 and 500 megabytes of data each time. This had been going on for approximately one week, and the affected server was taken offline for forensic review. Which of the following is MOST likely to drive up the incident's impact assessment?

- A. PII of company employees and customers was exfiltrated.
- B. Raw financial information about the company was accessed.
- C. Forensic review of the server required fall-back on a less efficient service.
- D. IP addresses and other network-related configurations were exfiltrated.
- E. The local root password for the affected server was compromised.

Answer: A

QUESTION 54

When network administrators observe an increased amount of web traffic without an increased number of financial transactions, the company is MOST likely experiencing which of the following attacks?

- A. Bluejacking
- B. ARP cache poisoning
- C. Phishing
- D. DoS

Answer: D

QUESTION 55

A threat intelligence analyst who works for a technology firm received this report from a vendor:
"There has been an intellectual property theft campaign executed against organizations in the technology industry. Indicators for this activity are unique to each intrusion. The information that appears to be targeted is R&D data. The data exfiltration appears to occur over months via uniform TTPs. Please execute a defensive operation regarding this attack vector."

Which of the following combinations suggests how the threat should MOST likely be classified and the type of analysis that would be MOST helpful in protecting against this activity?

- A. Polymorphic malware and secure code analysis
- B. Insider threat and indicator analysis
- C. APT and behavioral analysis
- D. Ransomware and encryption

Answer: B

QUESTION 56

The help desk informed a security analyst of a trend that is beginning to develop regarding a suspicious email that has been reported by multiple users. The analyst has determined the email includes an attachment named invoice.zip that contains the following files:

- Locky.js
- xerty.ini
- xerty.lib

Further analysis indicates that when the .zip file is opened, it is installing a new version of ransomware on the devices. Which of the following should be done FIRST to prevent data on the company NAS from being encrypted by infected devices?

- A. Disable access to the company VPN.
- B. Email employees instructing them not to open the invoice attachment.
- C. Set permissions on file shares to read-only.
- D. Add the URL included in the .js file to the company's web proxy filter.

Answer: B

QUESTION 57

After running a packet analyzer on the network, a security analyst has noticed the following output:

```
11:52:04 10.10.10.65.39769 > 192.168.50.147.80;  
S 2585925862:2585925862(0) win 4096 (ttl 29, id 48666)  
  
11:52:04 10.10.10.65.39769 > 192.168.50.147.81;  
S 2585925862:2585925862(0) win 4096 (ttl 29, id 65179)  
  
11:52:04 10.10.10.65.39769 > 192.168.50.147.83;  
S 2585925862:2585925862(0) win 4096 (ttl 29, id 42056)  
  
11:52:04 10.10.10.65.39769 > 192.168.50.147.82;  
S 2585925862:2585925862(0) win 4096 (ttl 29, id 41568)
```

Which of the following is occurring?

- A. A ping sweep
- B. A port scan
- C. A network map
- D. A service discovery

Answer: B

QUESTION 58

A database administrator contacts a security administrator to request firewall changes for a connection to a new internal application. The security administrator notices that the new application uses a port typically monopolized by a virus. The security administrator denies the request and suggests a new port or service be used to complete the application's task. Which of the following is the security administrator practicing in this example?

- A. Explicit deny
- B. Port security
- C. Access control lists
- D. Implicit deny

Answer: C

QUESTION 59

An organization has recently recovered from an incident where a managed switch had been accessed and reconfigured without authorization by an insider. The incident response team is working on developing a lessons learned report with recommendations. Which of the following recommendations will BEST prevent the same attack from occurring in the future?

- A. Remove and replace the managed switch with an unmanaged one.
- B. Implement a separate logical network segment for management interfaces.
- C. Install and configure NAC services to allow only authorized devices to connect to the network.
- D. Analyze normal behavior on the network and configure the IDS to alert on deviations from normal.

Answer: B

QUESTION 60

A cybersecurity analyst is reviewing the current BYOD security posture. The users must be able to

synchronize their calendars, email, and contacts to a smartphone or other personal device. The recommendation must provide the most flexibility to users. Which of the following recommendations would meet both the mobile data protection efforts and the business requirements described in this scenario?

- A. Develop a minimum security baseline while restricting the type of data that can be accessed.
- B. Implement a single computer configured with USB access and monitored by sensors.
- C. Deploy a kiosk for synchronizing while using an access list of approved users.
- D. Implement a wireless network configured for mobile device access and monitored by sensors.

Answer: D

QUESTION 61

A security analyst has been asked to remediate a server vulnerability. Once the analyst has located a patch for the vulnerability, which of the following should happen NEXT?

- A. Start the change control process.
- B. Rescan to ensure the vulnerability still exists.
- C. Implement continuous monitoring.
- D. Begin the incident response process.

Answer: A

QUESTION 62

A software assurance lab is performing a dynamic assessment on an application by automatically generating and inputting different, random data sets to attempt to cause an error/failure condition. Which of the following software assessment capabilities is the lab performing AND during which phase of the SDLC should this occur? (Select TWO.)

- A. Fuzzing
- B. Behavior modeling
- C. Static code analysis
- D. Prototyping phase
- E. Requirements phase
- F. Planning phase

Answer: AC

QUESTION 63

Law enforcement has contacted a corporation's legal counsel because correlated data from a breach shows the organization as the common denominator from all indicators of compromise. An employee overhears the conversation between legal counsel and law enforcement, and then posts a comment about it on social media. The media then starts contacting other employees about the breach. Which of the following steps should be taken to prevent further disclosure of information about the breach?

- A. Security awareness about incident communication channels
- B. Request all employees verbally commit to an NDA about the breach
- C. Temporarily disable employee access to social media
- D. Law enforcement meeting with employees

Answer: A

QUESTION 64

A recent vulnerability scan found four vulnerabilities on an organization's public Internet-facing IP addresses. Prioritizing in order to reduce the risk of a breach to the organization, which of the following should be remediated FIRST?

- A. A cipher that is known to be cryptographically weak.
- B. A website using a self-signed SSL certificate.
- C. A buffer overflow that allows remote code execution.
- D. An HTTP response that reveals an internal IP address.

Answer: C

QUESTION 65

A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

- A. Transitive access
- B. Spoofing
- C. Man-in-the-middle
- D. Replay

Answer: C

QUESTION 66

A company discovers an unauthorized device accessing network resources through one of many network drops in a common area used by visitors. The company decides that it wants to quickly prevent unauthorized devices from accessing the network but policy prevents the company from making changes on every connecting client. Which of the following should the company implement?

- A. Port security
- B. WPA2
- C. Mandatory Access Control
- D. Network Intrusion Prevention

Answer: A

QUESTION 67

Which of the following best practices is used to identify areas in the network that may be vulnerable to penetration testing from known external sources?

- A. Blue team training exercises
- B. Technical control reviews
- C. White team training exercises
- D. Operational control reviews

Answer: A

QUESTION 68

A cybersecurity analyst is currently investigating a server outage. The analyst has discovered the

following value was entered for the username: 0xbfff601a. Which of the following attacks may be occurring?

- A. Buffer overflow attack
- B. Man-in-the-middle attack
- C. Smurf attack
- D. Format string attack
- E. Denial of service attack

Answer: D

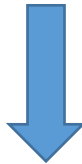
QUESTION 69

External users are reporting that a web application is slow and frequently times out when attempting to submit information. Which of the following software development best practices would have helped prevent this issue?

- A. Stress testing
- B. Regression testing
- C. Input validation
- D. Fuzzing

Answer:

Get Complete Version Exam CS0-001 Dumps with VCE and PDF Here



<https://www.passleader.com/cs0-001.html>