QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

CompTIA

CS0-001

CompTIA CSA+ Certification

QUESTION: 170
Scan results identify critical Apache vulnerabilities on a company's web servers. A security analyst believes many of these results are false positives because the web environment mostly consists of Windows servers. Which of the following is the BEST method of verifying the scan results?

A. Run a service discovery scan on the identified servers.
B. Refer to the identified servers in the asset inventory.
C. Perform a top-ports scan against the identified servers.
D. Review logs of each host in the SIEM.

Answer: A

QUESTION: 171
A company has received the results of an external vulnerability scan from its approved scanning vendor. The company is required to remediate these vulnerabilities for clients within 72 hours of acknowledgement of the scan results. Which of the following contract breaches would result if this remediation is not provided for clients within the time frame?

A. Service level agreement
B. Regulatory compliance
C. Memorandum of understanding
D. Organizational governance

Answer: A

QUESTION: 172
A Linux-based file encryption malware was recently discovered in the wild. Prior to running the malware on a preconfigured sandbox to analyze its behavior, a security professional executes the following command:
umount –a –t cifs,nfs Which of the following is the main reason for executing the above command?

A. To ensure the malware is memory bound.

B. To limit the malware's reach to the local host.
C. To back up critical files across the network
D. To test if the malware affects remote systems

Answer: B

QUESTION: 173
A systems administrator is trying to secure a critical system. The administrator has placed the system behind a firewall, enabled strong authentication, and required all administrators of this system to attend mandatory training. Which of the following BEST describes the control being implemented?

A. Audit remediation
B. Defense in depth
C. Access control
D. Multifactor authentication

Answer: B

QUESTION: 174
A retail corporation with widely distributed store locations and IP space must meet PCI requirements relating to vulnerability scanning. The organization plans to outsource this function to a third party to reduce costs. Which of the following should be used to communicate expectations related to the execution of scans?

A. Vulnerability assessment report
B. Lessons learned documentation
C. SLA
D. MOU

Answer: C

QUESTION: 175
The Chief Information Security Officer (CISO) asked for a topology discovery to be conducted and verified against the asset inventory. The discovery is failing and not providing reliable or complete data. The syslog shows the following information:

```
Mar 16 14:58:31 myhost nslcd [16637]    :  [0e0f76] LDAP result  ( )  failed unable to authenticate
Mar 16 14:58:32 myhost nslcd [52255a]   :  [0e0f76] LDAP result  ( )  failed unable to contact
Mar 16 14:58:40 myhost nslcd [16637]    :  [0e0f76] LDAP result  ( )  failed to authenticate
Mar 16 14:58:42 myhost nslcd [52255a]   :  [0e0f76] LDAP result  ( )  failed unable to contact
```

Which of the following describes the reason why the discovery is failing?

A. The scanning tool lacks valid LDAP credentials.
B. The scan is returning LDAP error code 52255a.
C. The server running LDAP has antivirus deployed.
D. The connection to the LDAP server is timing out.
E. The LDAP server is configured on the wrong port.

Answer: A

QUESTION: 176
A cybersecurity professional wants to determine if a web server is running on a remote host with the IP address 192.168.1.100. Which of the following can be used to perform this task?

A. nc 192.168.1.100 -1 80
B. ps aux 192.168.1.100
C. nmap 192.168.1.100 –p 80 –A
D. dig www 192.168.1.100
E. ping –p 80 192.168.1.100

Answer: C

QUESTION: 177
Weeks before a proposed merger is scheduled for completion, a security analyst has noticed unusual traffic patterns on a file server that contains financial information. Routine scans are not detecting the signature of any known exploits or malware. The following entry is seen in the ftp server logs: tftp –I 10.1.1.1 GET fourthquarterreport.xls Which of the following is the BEST course of action?

A. Continue to monitor the situation using tools to scan for known exploits.
B. Implement an ACL on the perimeter firewall to prevent data exfiltration.
C. Follow the incident response procedure associate with the loss of business critical data.
D. Determine if any credit card information is contained on the server containing the

financials.

Answer: C

QUESTION: 178
The primary difference in concern between remediating identified vulnerabilities found in general- purpose IT network servers and that of SCADA systems is that:

A. change and configuration management processes do not address SCADA systems.
B. doing so has a greater chance of causing operational impact in SCADA systems.
C. SCADA systems cannot be rebooted to have changes to take effect.
D. patch installation on SCADA systems cannot be verified.

Answer: B

QUESTION: 179
A security analyst at a small regional bank has received an alert that nation states are attempting to infiltrate financial institutions via phishing campaigns. Which of the following techniques should the analyst recommend as a proactive measure to defend against this type of threat?

A. Honeypot
B. Location-based NAC
C. System isolation
D. Mandatory access control
E. Bastion host

Answer: B

QUESTION: 180
A security analyst is concerned that unauthorized users can access confidential data stored in the production server environment. All workstations on a particular network segment have full access to any server in production. Which of the following should be deployed in the production environment to prevent unauthorized access? (Choose two.)

A. DLP system
B. Honeypot

C. Jump box
D. IPS
E. Firewall

Answer: E

QUESTION: 181
A cybersecurity analyst is reviewing log data and sees the output below:

```
POST:// payload.php HTTP/1.1
HOST: localhost
Accept: */*
Referrer: http://localhost
**********
HTTP /1.1 403 Forbidden
connection : close
```

Which of the following technologies MOST likely generated this log?

A. Stateful inspection firewall
B. Network-based intrusion detection system
C. Web application firewall
D. Host-based intrusion detection system

Answer: C