Exam : CS0-001

Title : CompTIA Cybersecurity Analyst (CySA+) Exam

Vendor : CompTIA

Version : DEMO

A vulnerability scan returned the following results for a web server that hosts multiple wiki sites:

Apache-HTTPD-cve-2014-023: Apache HTTPD: mod_cgid denial of service CVE-2014-0231 Due to a flaw found in mod_cgid, a server using mod_cgid to host CGI scripts could be vulnerable to a DoS attack caused by a remote attacker who is exploiting a weakness in non-standard input, causing processes to hang indefinitely.

The security analyst has confirmed the server hosts standard CGI scripts for the wiki sites, does not have mod_cgid installed, is running Apache 2.2.22, and is not behind a WAF. The server is located in the DMZ, and the purpose of the server is to allow customers to add entries into a publicly accessible database.

Which of the following would be the MOST efficient way to address this finding?

A. Disable the HTTP service and use only HTTPS to access the server.
B. Upgrade to the newest version of Apache.
C. Place the server behind a WAF to prevent DoS attacks from occurring.
D. Document the finding as a false positive.

Answer: D

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

Answer: C

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

Answer: B
NO.4 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. Implement a separate logical network segment for management interfaces.
B. Analyze normal behavior on the network and configure the IDS to alert on deviations from normal.
C. Install and configure NAC services to allow only authorized devices to connect to the network.
D. Remove and replace the managed switch with an unmanaged one.

**Answer:** A

NO.5 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. Network Intrusion Prevention
B. Mandatory Access Control
C. Port security
D. WPA2

**Answer:** C

NO.6 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. Organizational governance
B. Virtual hosts
C. Asset isolation
D. Log disposition
E. Processor utilization

**Answer:** B

NO.7 A technician recently fixed a computer with several viruses and spyware programs on it and notices the Internet settings were set to redirect all traffic through an unknown proxy. This type of attack is known as which of the following?

A. Shoulder surfing
B. Man-in-the-middle
C. Social engineering
D. Phishing

**Answer:** B

NO.8 A technician receives an alert indicating an endpoint is beaconing to a suspect dynamic DNS domain. Which of the following countermeasures should be used to BEST protect the network in response to this alert?

(Choose two.)
A. Isolate the infected endpoint to prevent the potential spread of malicious activity.
B. Set up a sinkhole for that dynamic DNS domain to prevent communication.
C. Implement an internal honeypot to catch the malicious traffic and trace it.
D. Perform a risk assessment and implement compensating controls.
E. Ensure the IDS is active on the network segment where the endpoint resides.

**Answer:** A,B

**NO.9** Which of the following are essential components within the rules of engagement for a penetration test? (Select TWO).
A. Authorization
B. Business justification
C. Payment terms
D. List of system administrators
E. Schedule

**Answer:** A,E

**NO.10** A vulnerability scan has returned the following information:

```
Detailed Results
10.10.10.214 (LOTUS-10-214)

Windows Shares
Category: Windows
CVE ID: -
Vendor Ref: -
Bugtraq ID: -
Service Modified - 4.16.2014

Enumeration Results:
print6   C:\windows\system32\spool\drivers
ofcscan C:\Program Files\Trend Micro\OfficeScan\PCCSRV
Temp     C:\temp
```

Which of the following describes the meaning of these results?
A. Trend Micro has a known exploit that must be resolved or patched.
B. No CVE is present, so it is a false positive caused by Lotus running on a Windows server.
C. There is an unknown bug in a Lotus server with no Bugtraq ID.
D. Connecting to the host using a null session allows enumeration of share names.

**Answer:** D

**NO.11** Which of the following tools should an analyst use to scan for web server vulnerabilities?
A. Qualys
B. Wireshark
C. ArcSight
D. SolarWinds

Answer: C

NO.12 A cybersecurity analyst wants to use ICMP ECHO_REQUEST on a machine while using Nmap. Which of the following is the correct command to accomplish this?
A. $ nmap -PE 192.168.1.7
B. $ nmap --traceroute 192.168.1.7
C. $ ping --PE 192.168.1.7
D. $ nmap -PO 192.168.1.7

Answer: A

NO.13 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 nsclcl [16637] : [0e0f76] LDAP result ( ) failed unable to authenticate
Mar 16 14:58:32 myhost nsclcl [52255a] : [0e0f76] LDAP result ( ) failed unable to contact
Mar 16 14:58:40 myhost nsclcl [16637] : [0e0f76] LDAP result ( ) failed to authenticate
Mar 16 14:58:42 myhost nsclcl [52255a] : [0e0f76] LDAP result ( ) failed unable to contact

Which of the following describes the reason why the discovery is failing?
A. The LDAP server is configured on the wrong port.
B. The scanning tool lacks valid LDAP credentials.
C. The scan is returning LDAP error code 52255a.
D. The connection to the LDAP server is timing out.
E. The server running LDAP has antivirus deployed.

Answer: B

NO.14 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

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
</tr>
</tbody>
</table>

# 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 is running a vulnerable SSH server.

Answer: B
C. The company web server has been compromised.
D. The company email server has been compromised.

**Answer:** A

**NO.15** Which of the allowing is a best practice with regard to interacting with the media during an incident?
A. Release financial information on the impact of damages caused by the incident.
B. Designate a single port of contact and at least one backup for contact with the media.
C. Allow any senior management level personnel with knowledge of the incident to discuss it.
D. Stipulate that incidents are not to be discussed with the media at any time during the incident.

**Answer:** B

**NO.16** Management wants to scan servers for vulnerabilities on a periodic basis. Management has decided that the scan frequency should be determined only by vendor patch schedules and the organization's application deployment schedule. Which of the following would force the organization to conduct an out-of-cycle vulnerability scan?
A. False positives identified in production
B. Newly discovered PII on a server
C. A critical bug fix in the organization's application
D. A vendor releases a critical patch update

**Answer:** D

**NO.17** In order to leverage the power of data correlation with Nessus, a cybersecurity analyst must first be able to create a table for the scan results.

Given the following snippet of code:
```
CREATE TABLE MyResults ( ID INT AUTO_INCREMENT, IP TEXT, Port Text, PluginID INT, Type TEXT, Description TEXT, PRIMARY KEY ID (ID) );
```
Which of the following output items would be correct?

A. Option A
B. Option B
C. Option C

<table>
<thead>
<tr>
<th>ID</th>
<th>IP</th>
<th>Port</th>
<th>PluginID</th>
<th>Type</th>
<th>Description</th>
<th>Primarykey</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>192.168.1.2</td>
<td>System (445/tcp)</td>
<td>1000</td>
<td>A</td>
<td>System Scan</td>
<td>2</td>
</tr>
</tbody>
</table>

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

Answer: A

NO. 18 A security analyst is performing a forensic analysis on a machine that was the subject of some historic SIEM alerts. The analyst noticed some network connections utilizing SSL on non-common ports, copies of svchost.exe and cmd.exe in %TEMP% folder, and RDP files that had connected to external IPs. Which of the following threats has the security analyst uncovered?

A. APT
B. Ransomware
C. DDoS
D. Software vulnerability

Answer: A