- **Vendor:** CompTIA
- **Exam Code:** CS0-002
- **Exam Name:** CompTIA CSA+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in July/2020)**

QUESTION 46
In the development stage of the incident response policy, the security analyst needs to determine the stakeholders for the policy. Who of the following would be the policy stakeholders?

A. Human resources, legal, public relations, management
B. Chief information Officer (CIO), Chief Executive Officer, board of directors, stockholders
C. IT, human resources, security administrator, finance
D. Public information officer, human resources, audit, customer service

Answer: B

QUESTION 47
Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application? (Choose two.)

A. Parameterized queries
B. Session management
C. Input validation
D. Output encoding
E. Data protection
F. Authentication

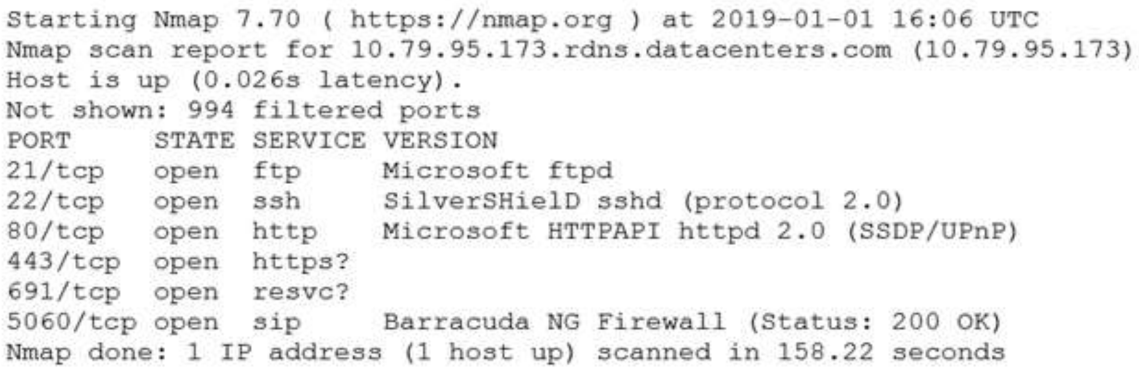
Answer: AC

QUESTION 48
A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server.
Which of the following is the FIRST step the analyst should take?

A. Create a full disk image of the server's hard drive to look for the file containing the malware.
B. Run a manual antivirus scan on the machine to look for known malicious software.
C. Take a memory snapshot of the machine to capture volatile information stored in memory.
D. Start packet capturing to look for traffic that could be indicative of command and control from the miner.

Answer: D

QUESTION 49
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. tracert 10.79.95.173

Answer: D

QUESTION 50
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

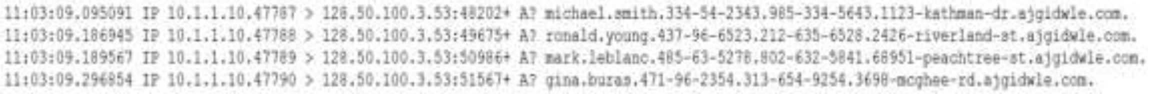
Answer: AE

QUESTION 51
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

QUESTION 52
A security analyst is reviewing packet captures from a system that was compromised. The system was already isolated from the network, but it did have network access for a few hours after being compromised. When viewing the capture in a packet analyzer, the analyst sees the following:



```
11:03:09.095091 IP 10.1.1.10.47787 > 128.50.100.3.53:48202+ A? michael.smith.334-54-2343.985-334-5643.1123-kathman-dr.ajgidwle.com.
11:03:09.186945 IP 10.1.1.10.47788 > 128.50.100.3.53:49675+ A? ronald.young.437-96-6523.212-635-6528.2426-riverland-st.ajgidwle.com.
11:03:09.189567 IP 10.1.1.10.47789 > 128.50.100.3.53:50986+ A? mark.leblanc.485-63-5278.802-632-5841.68951-peachtree-st.ajgidwle.com.
11:03:09.296854 IP 10.1.1.10.47790 > 128.50.100.3.53:51567+ A? gina.buras.471-96-2354.313-654-9254.3698-mcghee-rd.ajgidwle.com.
```

Which of the following can the analyst conclude?

A. Malware is attempting to beacon to 128.50.100.3.
B. The system is running a DoS attack against ajgidwle.com.
C. The system is scanning ajgidwle.com for PII.
D. Data is being exfiltrated over DNS.

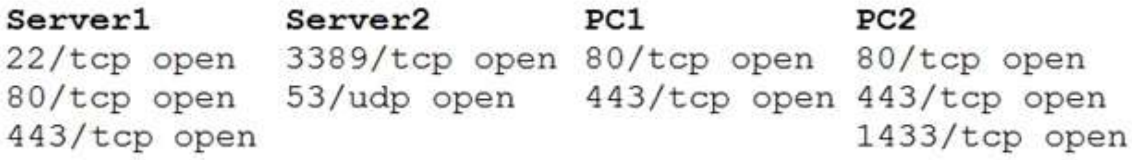
Answer: C

QUESTION 53
It is important to parameterize queries to prevent __________.

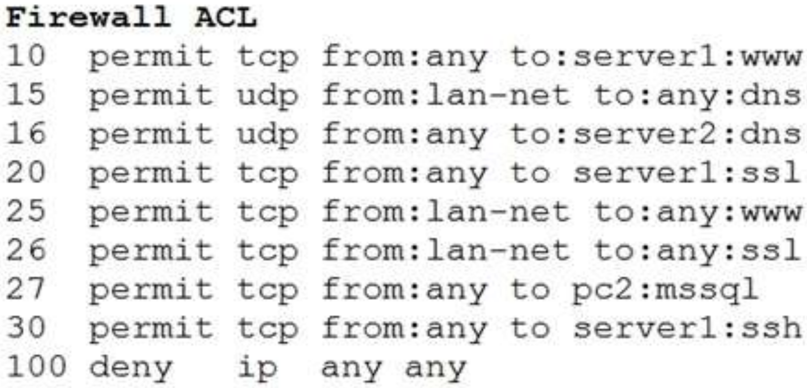
A. the execution of unauthorized actions against a database.
B. a memory overflow that executes code with elevated privileges.
C. the establishment of a web shell that would allow unauthorized access.
D. the queries from using an outdated library with security vulnerabilities.

Answer: A

QUESTION 54
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: E

QUESTION 55

After reviewing security logs, it is noticed that sensitive data is being transferred over an insecure network. Which of the following would a cybersecurity analyst BEST recommend that the organization implement?

A. Use a VPN
B. Update the data classification matrix.
C. Segment the networks.
D. Use FIM.
E. Use a digital watermark.

Answer: A

QUESTION 56
The help desk has reported that users are reusing previous passwords when prompted to change them.
Which of the following would be the MOST appropriate control for the security analyst to configure to prevent password reuse? (Choose two.)

A. Implement mandatory access control on all workstations.
B. Implement role-based access control within directory services.
C. Deploy Group Policy Objects to domain resources.
D. Implement scripts to automate the configuration of PAM on Linux hosts.
E. Deploy a single-sing-on solution for both Windows and Linux hosts.

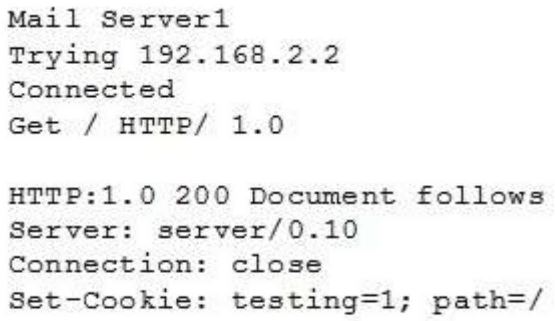
Answer: CD

QUESTION 57
A business recently installed a kiosk that is running on a hardened operating system as a restricted user. The kiosk user application is the only application that is allowed to run. A security analyst gets a report that pricing data is being modified on the server, and management wants to know how this is happening. After reviewing the logs, the analyst discovers the root account from the kiosk is accessing the files. After validating the permissions on the server, the analyst confirms the permissions from the kiosk do not allow to write to the server data.
Which of the following is the MOST likely reason for the pricing data modifications on the server?

A. Data on the server is not encrypted, allowing users to change the pricing data.
B. The kiosk user account has execute permissions on the server data files.
C. Customers are logging off the kiosk and guessing the root account password.
D. Customers are escaping the application shell and gaining root-level access.

Answer: D

QUESTION 58
A cybersecurity analyst is currently checking a newly deployed server that has an access control list applied. When conducting the scan, the analyst received the following code snippet of results:



```
Mail Server1
Trying 192.168.2.2
Connected
Get / HTTP/ 1.0

HTTP:1.0 200 Document follows
Server: server/0.10
Connection: close
Set-Cookie: testing=1; path=/
```

Which of the following describes the output of this scan?

A. The analyst has discovered a False Positive, and the status code is incorrect providing an OK message.

B. The analyst has discovered a True Positive, and the status code is correct providing a file not found error message.

C. The analyst has discovered a True Positive, and the status code is incorrect providing a forbidden message.

D. The analyst has discovered a False Positive, and the status code is incorrect providing a server error message.

Answer: B