- **Vendor:** CompTIA
- **Exam Code:** SY0-501
- **Exam Name:** CompTIA Security+ Certification Exam
- **New Updated Questions from Braindump2go (Updated in May/2021)**

QUESTION 1409
An organization with very high security needs wants to implement a biometric system. It is required to minimize unauthorized access by ensuring authorized personnel are not denied access. Which of the following solutions will work?

A. A device with a low false acceptance rate and a high false rejection rate
B. A device with a high false acceptance rate and a high false rejection rate
C. A device with a high false acceptance rate and a low false rejection rate
D. A device with a low false acceptance rate and a low false rejection rate

Answer: D

QUESTION 1410
Which of the following has the potential to create a DoS attack on a system?

A. A server room WiFi thermostat with default credentials
B. A surveillance camera that has been replaced and is not plugged in
C. A disabled user account that has not been deleted
D. A wireless access point with WPA2 connected to the network

Answer: A

QUESTION 1411
Which of the following generates reports that show the number of systems that are associated with POODLE, 3DES, and SMBv1 listings?

A. A protocol analyzer
B. A UTM appliance
C. A vulnerability scanner
D. A honeypot

Answer: C

QUESTION 1412
An organization's Chief Information Officer (CIO) read an article that identified leading hacker trends and attacks, one of which is the alteration of URLs to IP addresses resulting in users being redirected to malicious websites. To reduce the chances of this happening in the organization, which of the following secure protocols should be implemented?

A. DNSSEC

B. IPSec
C. LDAPS
D. HTTPS

Answer: A

QUESTION 1413
The phones at a business are being replaced with VoIP phones that get plugged in-line between the switch and PC. The voice and data networks still need to be kept separate. Which of the following would allow for this?

A. NAT
B. Intranet
C. Subnetting
D. VLAN

Answer: D

QUESTION 1414
A security analyst recommends implementing SSL for an existing web service. A technician installs the SSL certificate and successfully tests the connection on the server. Soon after, the help desk begins receiving calls from users who are unable to log in. After further investigation, it becomes clear that no users have successfully connected to the web server since the certificate installation. Which of the following is MOST likely the issue?

A. Incorrect firewall rules are blocking HTTPS traffic.
B. Users are still accessing the IP address and not the HTTPS address.
C. Workstations need an updated trusted sites list.
D. Users are not using tokens to log on.

Answer: C

QUESTION 1415
Which of the following impacts MOST likely results from poor exception handling?

A. Widespread loss of confidential data
B. Network-wide resource exhaustion
C. Privilege escalation
D. Local disruption of services

Answer: C

QUESTION 1416
After deploying an antivirus solution on some network-isolated industrial computers, the service desk team received a trouble ticket about the following message being displayed on the computers' screens:
Your AV protection has blocked an unknown application while performing suspicious activities. The application was put in quarantine.
Which of the following would be the SAFEST next step to address the issue?

A. Immediately delete the detected file from the quarantine to secure the environment and clear the alert from the antivirus console.
B. Perform a manual antivirus signature update directly from the antivirus vendor's cloud.
C. Centrally activate a full scan for the entire set of industrial computers, looking for new threats.
D. Check the antivirus vendor's documentation about the security modules, incompatibilities, and software whitelisting.

Answer: D

QUESTION 1417
During incident response procedures, technicians capture a unique identifier for a piece of malware running in memory. This captured information is referred to as:

A. a hash value.
B. the SSID.
C. the GUID.
D. a system image.

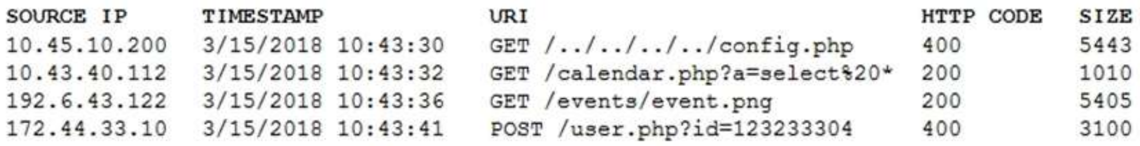
Answer: A

QUESTION 1418
A user's laptop is experiencing general slowness following the user's return from an extended time out of the office. After a week, the security team looks at the laptop, but nothing appears out of order. The only noticeable issue is that svchost.exe keeps launching even after the security team kills the process. After running netstat, the team notes svchost.exe is listening on port 443. Using an IoC creation tool, a security analyst does the following:
OR--
File MD5 contains adf321122abce28873aad3e12f262a12c
AND
PROCESS name contains svchost.exe
PROCESS arguments does not contain -k
AND
FILENAME contains svchost.exe
FILE DIRECTORY is not %system32%
Based on the IoCs created and the netstat output, which of the following types of malware is present?

A. Backdoor
B. Crypto-malware
C. Rootkit
D. Logic bomb

Answer: C

QUESTION 1419
An analyst is reviewing the following web-server log after receiving an alert from the DLP system about multiple PII records being transmitted in cleartext:



```
SOURCE IP      TIMESTAMP            URI                                HTTP CODE   SIZE
10.45.10.200   3/15/2018 10:43:30   GET /../../../../config.php        400         5443
10.43.40.112   3/15/2018 10:43:32   GET /calendar.php?a=select%20*     200         1010
192.6.43.122   3/15/2018 10:43:36   GET /events/event.png              200         5405
172.44.33.10   3/15/2018 10:43:41   POST /user.php?id=123233304        400         3100
```

Which of the following IP addresses is MOST likely involved in the data leakage attempt?

A. 10.43.40.112
B. 10.45.10.200
C. 172.44.33.10
D. 192.6.43.122

Answer: C

QUESTION 1420
A security analyst needs a solution that can execute potential malware in a restricted and isolated environment for analysis. In which of the following technologies is the analyst interested?

A. Sandboxing

B. Staging
C. DMZ
D. Honeypot

Answer: A

QUESTION 1421
A penetration tester is testing passively for vulnerabilities on a company's network. Which of the following tools should the penetration tester use? (Choose two.)

A. Zenmap
B. Wireshark
C. Nmap
D. tcpdump
E. Nikto
F. Snort

Answer: CE

QUESTION 1422
A security analyst wants to prevent current employees who previously worked in different departments from accessing resources that are no longer necessary for their present job roles. Which of the following policies would meet this objective?

A. Job rotation
B. Discretionary account
C. Least privilege
D. Mandatory vacation
E. Separation of duties

Answer: C

QUESTION 1423
A company is determining where to host a hot site, and one of the locations being considered is in another country. Which of the following should be considered when evaluating this option?

A. Mean RTO
B. Mean RPO
C. Data sovereignty
D. Data destruction laws
E. Backup media recycling policies

Answer: C