DUMPSBOSS.COM

CompTIA Advanced Security Practitioner (CASP) CAS-003

CompTIA CAS-003

Version Demo

Total Demo Questions: 20

Total Premium Questions: 547

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

QUESTION NO: 1

A systems administrator receives an advisory email that a recently discovered exploit is being used in another country and the financial institutions have ceased operations while they find a way to respond to the attack. Which of the following BEST describes where the administrator should look to find information on the attack to determine if a response must be prepared for the systems? (Choose two.)

A. Bug bounty websites

B. Hacker forums

C. Antivirus vendor websites

D. Trade industry association websites

E. CVE database

F. Company's legal department

ANSWER: B E

QUESTION NO: 2

Which of the following attacks can be mitigated by proper data retention policies?

A. Dumpster diving

B. Man-in-the browser

C. Spear phishing

D. Watering hole

ANSWER: A

QUESTION NO: 3 - (SIMULATION)

SIMULATION

A product development team has submitted code snippets for review prior to release.

INSTRUCTIONS

Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Code Snippet 1

```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103

Web server code:
--
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement (accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
--
```

Vulnerability 1

- ◯ Server-side request forgery
- ◯ Cross-site scripting
- ◯ Cross-request request forgery
- ◯ Indirect object reference
- ◯ SQL injection

Fix 1

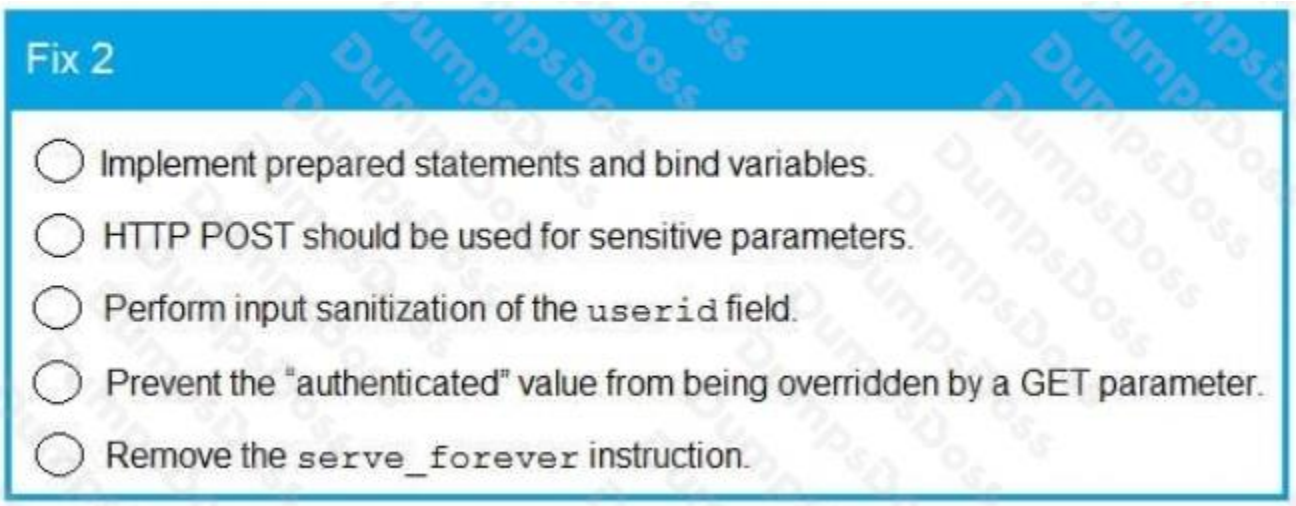
- ◯ Implement anti-forgery tokens.
- ◯ Perform output encoding of `queryResponse`.
- ◯ Ensure `userid` belongs to logged-in user.
- ◯ Inspect URLs and disallow arbitrary requests.
- ◯ Perform input sanitization of the `userid` field.

Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103

API endpoint (/searchDirectory):
…
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5', 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
  userId = request.getParam(userid)

ldapLookup = 'ldapsearch     -D "cn=' + userId + '" -W -p 389
                             -h loginserver.comptia.org
                             -b "dc=comptia,dc=org" -s sub -x "(objectclass=)"'
accountLookup = subprocess.popen(ldapLookup)

if (userExists(accountLookup))
    accountFound = true
else
    accountFound = false
…
```

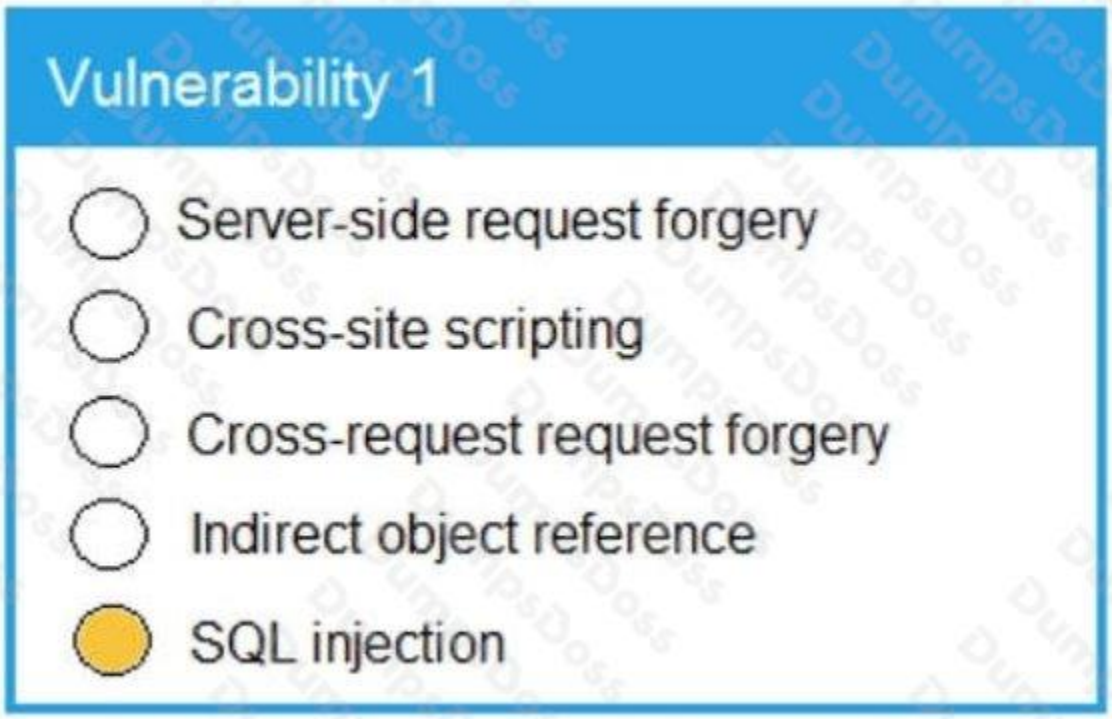
Vulnerability 2

- ◯ Command injection
- ◯ SQL injection
- ◯ Authorization bypass
- ◯ Denial of service
- ◯ Credentials passed via GET

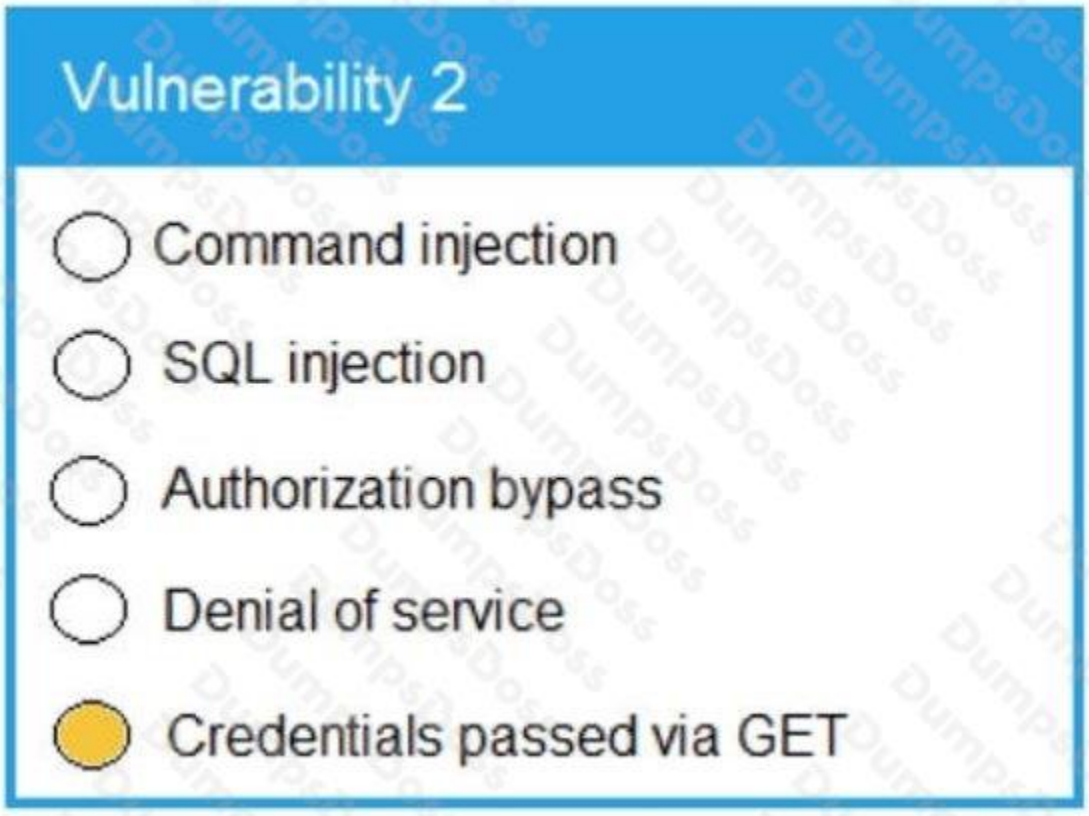


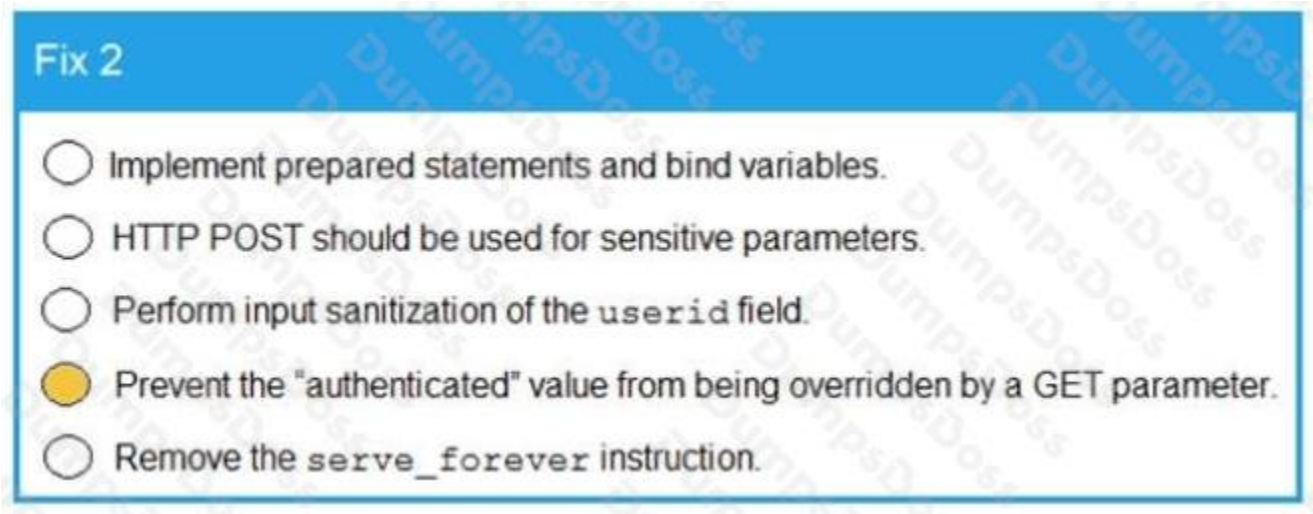
ANSWER: See explanation below.

Explanation:




Fix 1
Implement anti-forgery tokens.
Perform output encoding of queryResponse.
Ensure userid belongs to logged-in user.
Inspect URLs and disallow arbitrary requests.
Perform input sanitization of the userid field.


Vulnerability 2
Command injection
SQL injection
Authorization bypass
Denial of service
Credentials passed via GET



QUESTION NO: 4

A secure facility has a server room that currently is controlled by a simple lock and key, and several administrators have copies of the key. To maintain regulatory compliance, a second lock, which is controlled by an application on the administrators' smartphones, is purchased and installed. The application has various authentication methods that can be used. The criteria for choosing the most appropriate method are:

- It cannot be invasive to the end user.
- It must be utilized as a second factor.
- Information sharing must be avoided.
- It must have a low false acceptance rate.

Which of the following BEST meets the criteria?

A. Facial recognition

B. Swipe pattern

C. Fingerprint scanning

D. Complex passcode

E. Token card

ANSWER: C

QUESTION NO: 5 - (DRAG DROP)

DRAG DROP

A vulnerability scan with the latest definitions was performed across Sites A and B.

INSTRUCTIONS

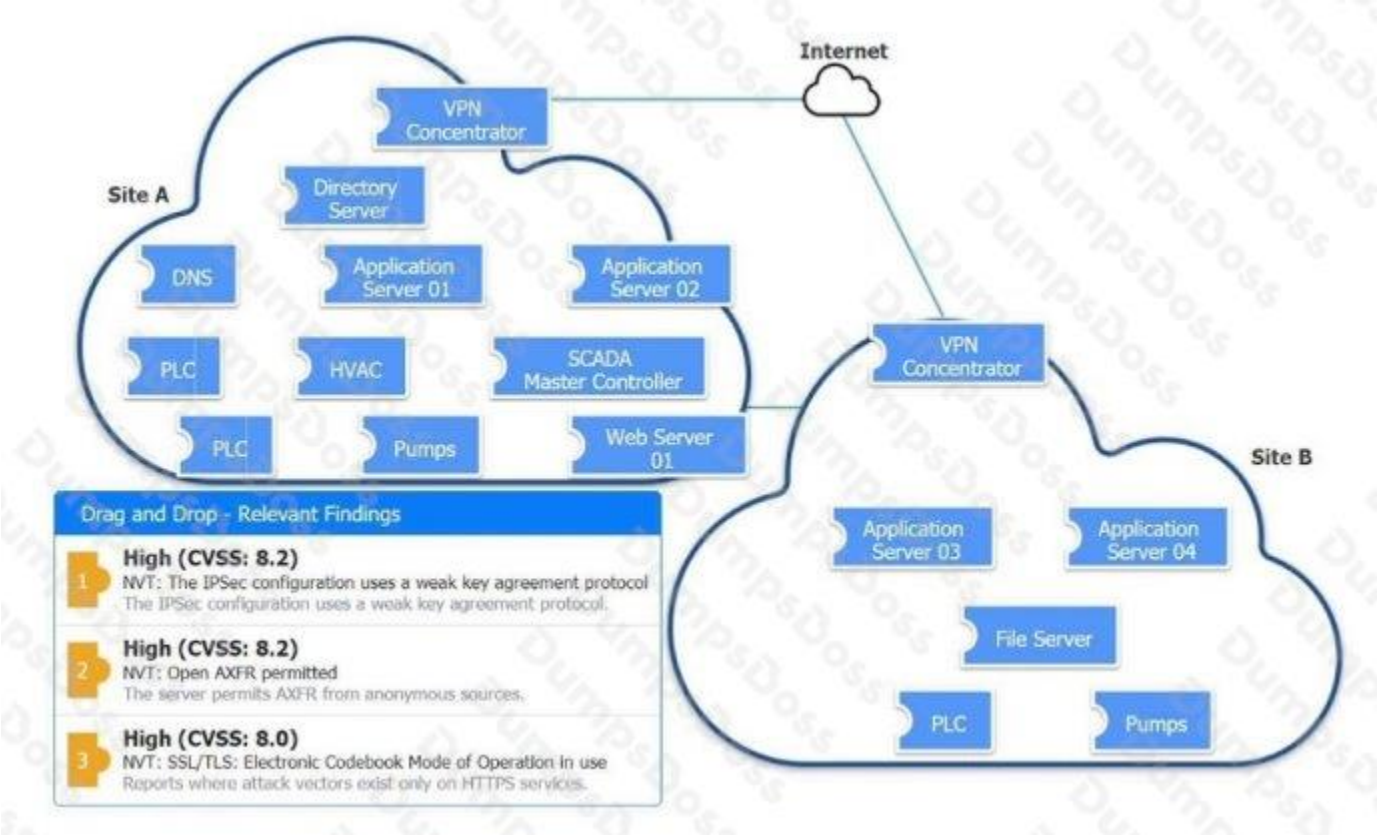
Match each relevant finding to the affected host.

After associating the finding with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

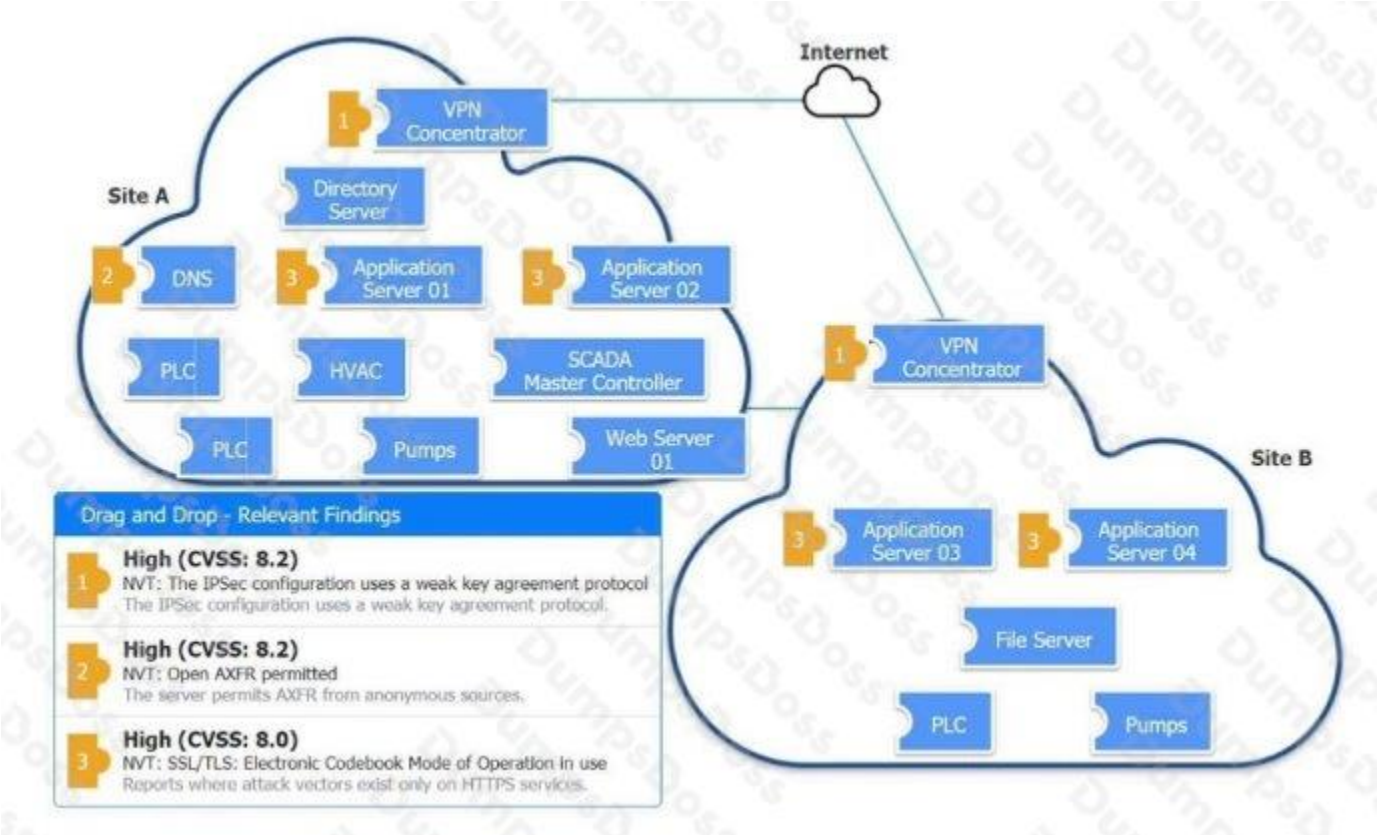
Each finding may be used more than once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Select and Place:



ANSWER:



Explanation:

QUESTION NO: 6

A security administrator is updating a company's SCADA authentication system with a new application. To ensure interoperability between the legacy system and the new application, which of the following stakeholders should be involved in the configuration process before deployment? (Choose two.)

A. Network engineer

B. Service desk personnel

C. Human resources administrator

D. Incident response coordinator

E. Facilities manager

F. Compliance manager

ANSWER: A E

QUESTION NO: 7

A school contracts with a vendor to devise a solution that will enable the school library to lend out tablet computers to students while on site. The tablets must adhere to string security and privacy practices. The school's key requirements are to:

- Maintain privacy of students in case of loss
- Have a theft detection control in place
- Be compliant with defined disability requirements
- Have a four-hour minimum battery life

Which of the following should be configured to BEST meet the requirements? (Choose two.)

A. Remote wiping

B. Geofencing

C. Antivirus software

D. TPM

E. FDE

F. Tokenization

ANSWER: B E

QUESTION NO: 8

A company is the victim of a phishing and spear-phishing campaign. Users are clicking on website links that look like common bank sites and entering their credentials accidentally. A security engineer decides to use a layered defense to prevent the phishing or lessen its impact. Which of the following should the security engineer implement? (Choose two.)

A. Spam filter

B. Host intrusion prevention

C. Client certificates

D. Log monitoring

E. Content filter

F. Data loss prevention

ANSWER: A E

QUESTION NO: 9

An insurance company has two million customers and is researching the top transactions on its customer portal. It identifies that the top transaction is currently password reset. Due to users not remembering their secret questions, a large number of calls are consequently routed to the contact center for manual password resets. The business wants to develop a mobile application to improve customer engagement in the future, continue with a single factor of authentication, minimize management overhead of the solution, remove passwords, and eliminate to the contact center. Which of the following techniques would BEST meet the requirements? (Choose two.)

A. Magic link sent to an email address

B. Customer ID sent via push notification

C. SMS with OTP sent to a mobile number

D. Third-party social login

E. Certificate sent to be installed on a device

F. Hardware tokens sent to customers

ANSWER: C E

QUESTION NO: 10

A company recently developed a new mobile application that will be used to access a sensitive system. The application and the system have the following requirements:

- The application contains sensitive encryption material and should not be accessible over the network.
- The system should not be exposed to the Internet.
- Communication must be encrypted and authenticated by both the server and the client.

Which of the following can be used to install the application on the mobile device? (Choose two.)

A. TPM

B. Internet application store

C. HTTPS

D. USB OTG

E. Sideloading

F. OTA

ANSWER: D F

QUESTION NO: 11

Within the past six months, a company has experienced a series of attacks directed at various collaboration tools. Additionally, sensitive information was compromised during a recent security breach of a remote access session from an unsecure site. As a result, the company is requiring all collaboration tools to comply with the following:

- Secure messaging between internal users using digital signatures
- Secure sites for video-conferencing sessions
- Presence information for all office employees
- Restriction of certain types of messages to be allowed into the network.

Which of the following applications must be configured to meet the new requirements? (Choose two.)

A. Remote desktop

B. VoIP

C. Remote assistance

D. Email

E. Instant messaging

F. Social media websites

ANSWER: A D

QUESTION NO: 12

Ann, a user, brings her laptop to an analyst after noticing it has been operating very slowly. The security analyst examines the laptop and obtains the following output:

```
Active Connections
Proto     Local Address        Foreign Address      State        PID
TCP       0.0.0.0:135          0.0.0.0:0            Listening    513
TCP       0.0.0.0.:445         0.0.0.0:0            Listening    4
TCP       10.11.43.115:139     0.0.0.0:0            Listening    4
TCP       10.11.43.115:65246   208.113.65.18:443    Established  3522
TCP       10.11.43.115:65248   208.113.65.18:443    Established  3522
```

Which of the following will the analyst most likely use NEXT?

A. Process explorer

B. Vulnerability scanner

C. Antivirus

D. Network enumerator

ANSWER: B

QUESTION NO: 13

A forensic analyst must image the hard drive of a computer and store the image on a remote server. The analyst boots the computer with a live Linux distribution. Which of the following will allow the analyst to copy and transfer the file securely to the remote server?

A. dd if=/dev/sda | sha256 | ssh –o username=user, password=mypass –p 2000 remote.server.com

B. dcfldd if=/dev/sda hash=sha256 sha256log=sha.log | cryptcat –k $key remote.server.com 2000

C. nc remote.server.com 5555 –e 'dcfldd if=/dev/sda of=./image.dd' | sha256 > sha256.log'

D. ssh –D 5555 user@remote.server.com; dd if=/dev/sda* | nc localhost 5555 'sha256 > sha.txt'

ANSWER: D

QUESTION NO: 14

An organization wants to arm its cybersecurity defensive suite automatically with intelligence on zero-day threats shortly after they emerge. Acquiring tools and services that support which of the following data standards would BEST enable the organization to meet this objective?

A. XCCDF

B. OVAL

C. STIX

D. CWE

E. CVE

ANSWER: E

QUESTION NO: 15

A forensic analyst suspects that a buffer overflow exists in a kernel module. The analyst executes the following command:

```
dd if=/dev/ram of=/tmp/mem/dmp
```

The analyst then reviews the associated output:

```
^34^#AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/bin/bash^21^03#45
```

However, the analyst is unable to find any evidence of the running shell.

Which of the following of the MOST likely reason the analyst cannot find a process ID for the shell?

A. The NX bit is enabled

B. The system uses ASLR

C. The shell is obfuscated

D. The code uses dynamic libraries

ANSWER: C

QUESTION NO: 16

A new database application was added to a company's hosted VM environment. Firewall ACLs were modified to allow database users to access the server remotely. The company's cloud security broker then identified abnormal from a database user on-site. Upon further investigation, the security team noticed the user ran code on a VM that provided access to the hypervisor directly and access to other sensitive data.

Which of the following should the security team do to help mitigate future attacks within the VM environment? (Choose two.)

A. Install the appropriate patches.

B. Install perimeter NGFW.

C. Configure VM isolation.

D. Deprovision database VM.

E. Change the user's access privileges.

F. Update virus definitions on all endpoints.

ANSWER: A C

QUESTION NO: 17

A security researcher is gathering information about a recent spoke in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.

Based on the information available to the researcher, which of the following is the MOST likely threat profile?

A. Nation-state-sponsored attackers conducting espionage for strategic gain.

B. Insiders seeking to gain access to funds for illicit purposes.

C. Opportunists seeking notoriety and fame for personal gain.

D. Hacktivists rolling out a marketing campaign to change landing pages.

ANSWER: D

QUESTION NO: 18

A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:

```
C:\nslookup -querytype=MX comptia.org
Server: Unknown
Address: 198.51.100.45

comptia.org MX preference=10, mail exchanger = 92.68.102.33
comptia.org MX preference=20, mail exchanger = exchgl.comptia.org
exchgl.comptia.org       Internet address = 192.168.102.67
```

Which of the following should the penetration tester conclude about the command output?

A. The public/private views on the Comptia.org DNS servers are misconfigured

B. Comptia.org is running an older mail server, which may be vulnerable to exploits

C. The DNS SPF records have not been updated for Comptia.org

D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack

ANSWER: B

QUESTION NO: 19

A security administrator is troubleshooting RADIUS authentication issues from a newly implemented controller-based wireless deployment. The RADIUS server contains the following information in its logs:

```
A RADIUS message was received from the invalid RADIUS client IP address 10.35.55.10
```

Based on this information, the administrator reconfigures the RADIUS server, which results in the following log data:

```
An Access-Request was received from RADIUS client 10.35.55.10
with a Message-Authenticator attribute that is not valid
```

To correct this error message, the administrator makes an additional change to the RADIUS server. Which of the following did the administrator reconfigure on the RADIUS server? (Choose two.)

A. Added the controller address as an authorized client

B. Registered the RADIUS server to the wireless controller

C. Corrected a mismatched shared secret

D. Renewed the expired client certificate

E. Reassigned the RADIUS policy to the controller

F. Modified the client authentication method

ANSWER: A C

QUESTION NO: 20

Which of the following is the primary cybersecurity-related difference between the goals of a risk assessment and a business impact analysis?

A. Broad spectrum threat analysis

B. Adherenece to quantitative vs. qualitative methods

C. A focus on current state without regard to cost

D. Measurements of ALE vs.SLE and downtime

ANSWER: A