CAS-003Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are:

Each lab must be on a separate network segment.

Labs must have access to the Internet, but not other lab networks.

Student devices must have network access, not simple access to hosts on the lab networks.

Students must have a private certificate installed before gaining access.

Servers must have a private certificate installed locally to provide assurance to the students.

All students must use the same VPN connection profile.

Which of the following components should be used to achieve the design in conjunction with directory services?

A. L2TP VPN over TLS for remote connectivity, SAML for federated authentication, firewalls between each lab segment

B. SSL VPN for remote connectivity, directory services groups for each lab group, ACLs on routing equipment

C. IPSec VPN with mutual authentication for remote connectivity, RADIUS for authentication, ACLs on network equipment

D. Cloud service remote access tool for remote connectivity, OAuth for authentication, ACL on routing equipment

Correct Answer: C

IPSec VPN with mutual authentication meets the certificates requirements.

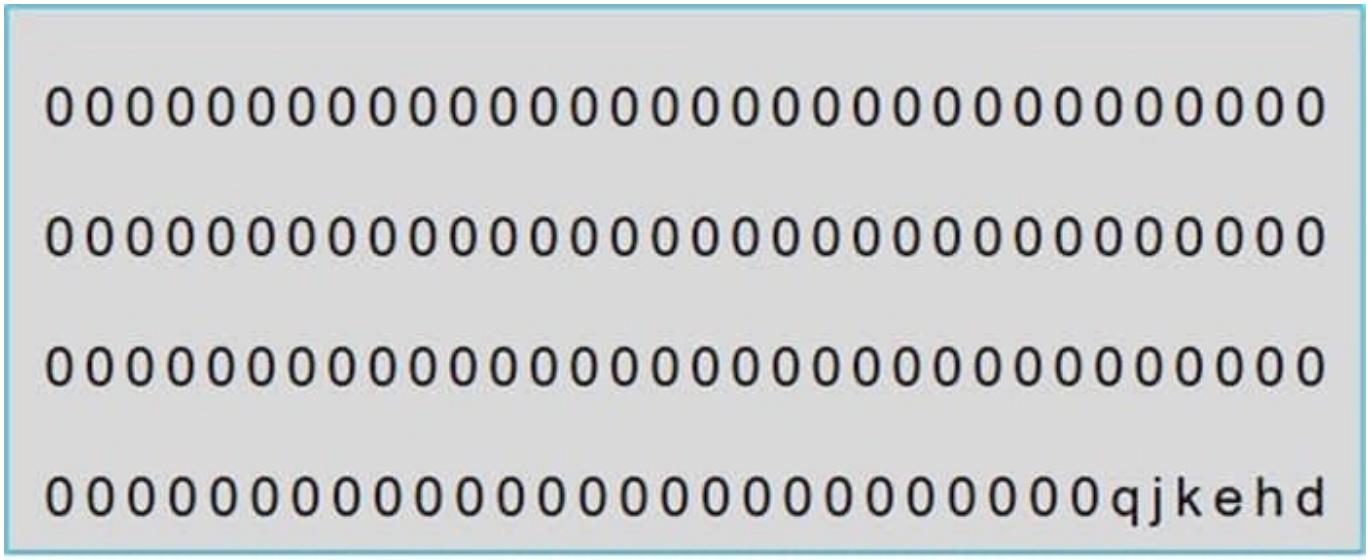
RADIUS can be used with the directory service for the user authentication.

ACLs (access control lists) are the best solution for restricting access to network hosts.

QUESTION 2

A systems administrator has installed a disk wiping utility on all computers across the organization and configured it to perform a seven-pass wipe and an additional pass to overwrite the disk with zeros. The company has also instituted a policy that requires users to erase files containing sensitive information when they are no longer needed.

To ensure the process provides the intended results, an auditor reviews the following content from a randomly selected decommissioned hard disk:



Which of the following should be included in the auditor\\'s report based in the above findings?

A. The hard disk contains bad sectors

B. The disk has been degaussed.

C. The data represents part of the disk BIOS.

D. Sensitive data might still be present on the hard drives.

Correct Answer: A

QUESTION 3

Company policy requires that all company laptops meet the following baseline requirements:

Software requirements:

Antivirus Anti-malware Anti-spyware Log monitoring Full-disk encryption Terminal services enabled for RDP Administrative access for local users

Hardware restrictions:

Bluetooth disabled FireWire disabled WiFi adapter disabled

Ann, a web developer, reports performance issues with her laptop and is not able to access any network resources. After further investigation, a bootkit was discovered and it was trying to access external websites. Which of the following hardening techniques should be applied to mitigate this specific issue from reoccurring? (Select TWO).

A. Group policy to limit web access

B. Restrict VPN access for all mobile users

C. Remove full-disk encryption

D. Remove administrative access to local users

E. Restrict/disable TELNET access to network resources

F. Perform vulnerability scanning on a daily basis

G. Restrict/disable USB access

Correct Answer: DG

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) while at the same time masking its existence or the existence of other software. A bootkit is similar to a rootkit except the malware infects the master boot record on a hard disk. Malicious software such as bootkits or rootkits typically require administrative privileges to be installed.

Therefore, one method of preventing such attacks is to remove administrative access for local users.

A common source of malware infections is portable USB flash drives. The flash drives are often plugged into less secure computers such as a user\\'s home computer and then taken to work and plugged in to a work computer. We can prevent this from happening by restricting or disabling access to USB devices.

QUESTION 4

SIMULATION

A product development team has submitted code snippets for review pnor 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 bang 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

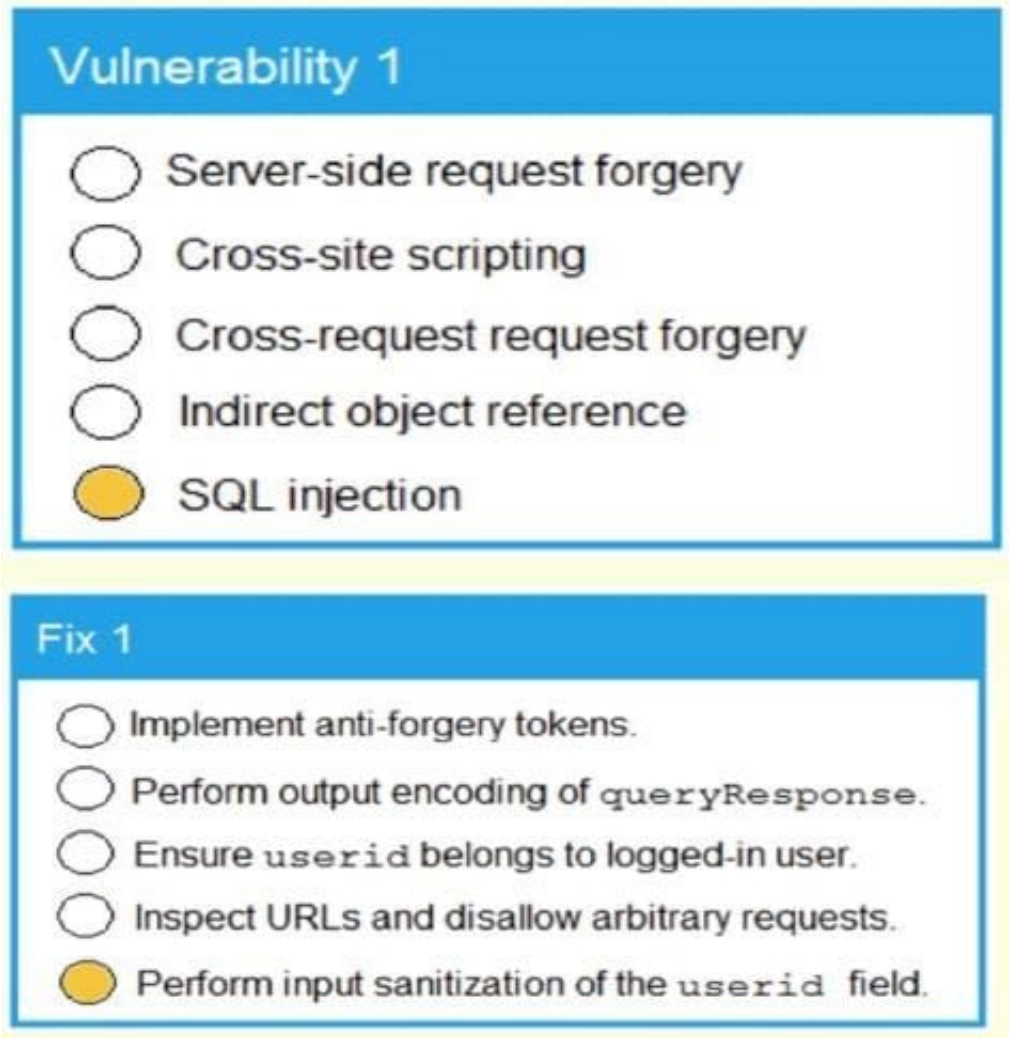
- ◯ Command injection
- ◯ SQL injection
- ◯ Authorization bypass
- ◯ Denial of service
- ◯ Credentials passed via GET

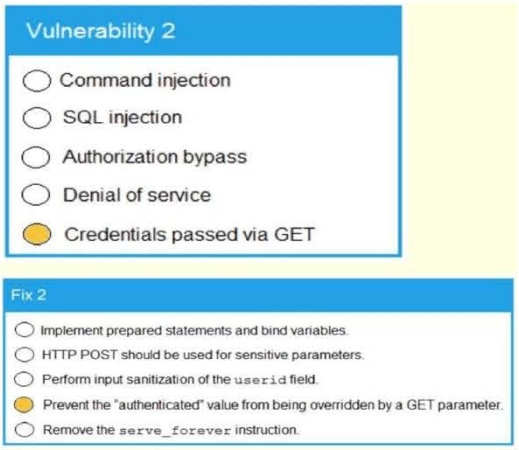
Fix 2

- ◯ Implement prepared statements and bind variables.
- ◯ HTTP POST should be used for sensitive parameters.
- ◯ Perform input sanitization of the `userid` field.
- ◯ Prevent the "authenticated" value from being overridden by a GET parameter.
- ◯ Remove the `serve_forever` instruction.

A. Check the answer in explanation below.

Correct Answer: A




Vulnerability 2
Command injection
SQL injection
Authorization bypass
Denial of service
Credentials passed via GET
Fix 2
Implement prepared statements and bind variables.
HTTP POST should be used for sensitive parameters.
Perform input sanitization of the userid field.
Prevent the "authenticated" value from being overridden by a GET parameter.
Remove the serve_forever instruction.

QUESTION 5

Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP address. The company uses the following internal IP address ranges: 192.10.1.0/24 for the corporate site and 192.10.2.0/24 for the remote

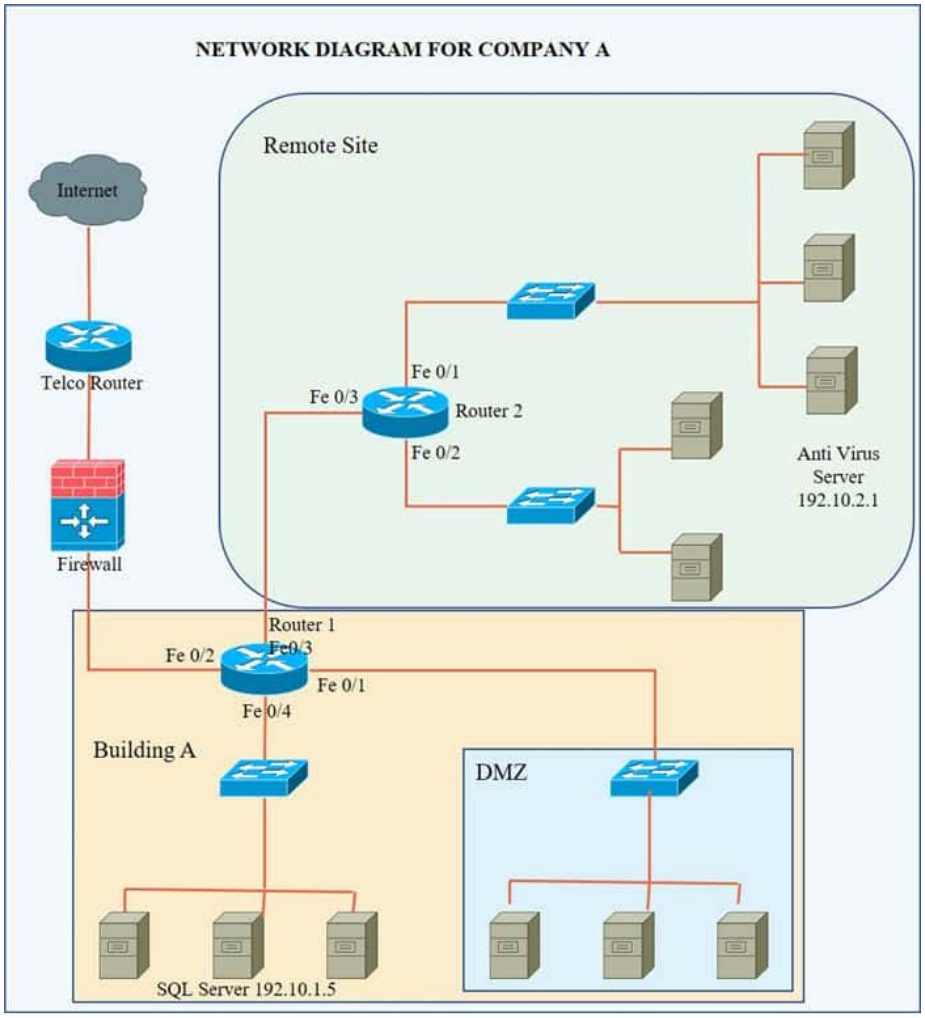
site. The Telco router interface uses the 192.10.5.0/30 IP range.

Instructions: Click on the simulation button to refer to the Network Diagram for Company A.

Click on Router 1, Router 2, and the Firewall to evaluate and configure each device.

Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.

Task 2: Reconfigure the appropriate devices to prevent the attacks from continuing to target the SQL server and other servers on the corporate network.



Log | Command Prompt — Router1

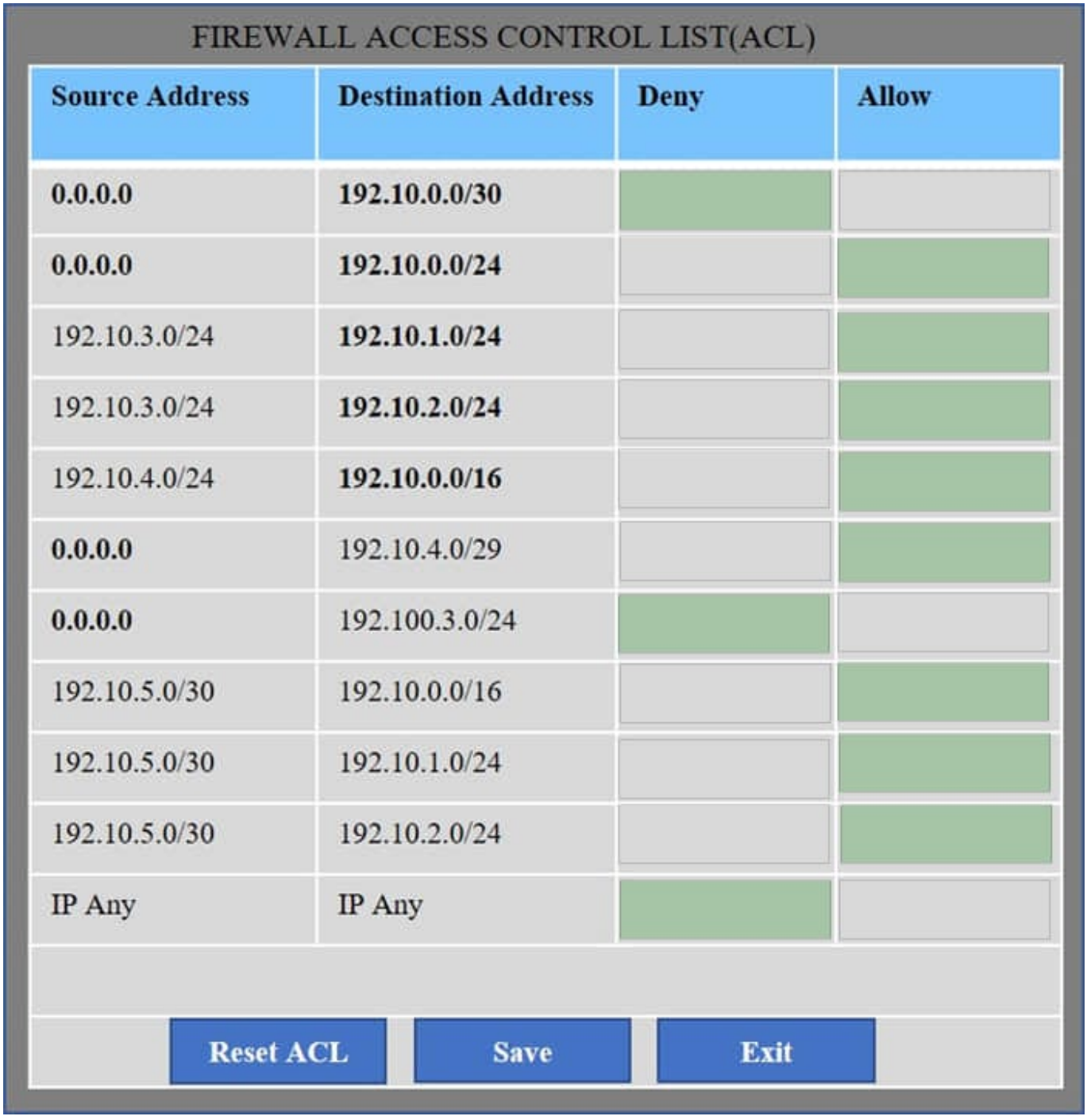
```
*Jul 15 10:47:27: %FW-6-OMOT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29:775:%Router1:ICMP Echo Request – from 192.10.3.204 to 192.10.1.5
*Jul 15 14:47:29.776:%Router1:list 101 permitted icmp 192.10.3.204(FastEthernet0/3)->
192.10.1.5, 6 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router1: list 101 permitted tcp 192.10.3.204(57222)(FastEthernet0/3
)->192.10.1.5(80), 3 packets.
```

Log | Command Prompt — Router2

```
*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29:777:%Router2:ICMP Echo Request – from 192.10.3.254 to 192.10.2.1
*Jul 15 14:47:29.778:%Router2:list 101 permitted icmp 192.10.3.254(FastEthernet0/2)->
192.10.2.1, 5 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router2: list 101 permitted tcp 192.10.3.254(35650)(FastEthernet0/2
)->192.10.2.1(80), 2 packets.
```

Hot Area:

Correct Answer:



We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.30.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:

CAS-003 Practice Test CAS-003 Exam Questions CAS-003 Braindumps