

➤ **Vendor: CompTIA**

➤ **Exam Code: SY0-501**

➤ **Exam Name: CompTIA Security+ Certification Exam**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [May/2021](#))**

[Visit Braindump2go and Download Full Version SY0-501 Exam Dumps](#)

QUESTION 1424

A network administrator wants to further secure the routers and switches that are used on the company network. The administrator would like to achieve full packet encryption and full command logging when interacting with these devices.

Which of the following technologies should be implemented?

- A. RADIUS
- B. SAML
- C. TACACS+
- D. LDAP

Answer: C

QUESTION 1425

A security analyst runs the c: \>netstat -b command on a workstation and receives the following output:

| | | | |
|-----|--------------------|-------------------|-----------|
| TCP | 192.168.66.6:45997 | generic.com:80 | TIME_WAIT |
| TCP | 192.168.66.6:45894 | qabgco.gf.com:129 | TIME_WAIT |
| TCP | 192.168.66.6:44996 | website.com:443 | TIME_WAIT |
| TCP | 192.168.66.6:54952 | thebank.org:443 | TIME_WAIT |

The analyst notices an entry on the server for a file called WmdowsRemote.exe that is listening on port 129. Which of the following types of malware is MOST likely being used?

- A. Rootkit
- B. Spyware
- C. Backdoor
- D. Zero-day

Answer: B

QUESTION 1426

Which of the following systems, if compromised may cause a denial of service to the use of a smart TV?

- A. SCADA
- B. IoT
- C. HVAC
- D. UAV

Answer: B

[SY0-501 Exam Dumps](#) [SY0-501 Exam Questions](#) [SY0-501 PDF Dumps](#) [SY0-501 VCE Dumps](#)

<https://www.braindump2go.com/sy0-501.html>

QUESTION 1427

A company recently experienced a significant malware attack that caused all business operations to stop. After an investigation a single PC was identified as the root cause and a security analyst on the IR team disconnected the machine from the corporate network, both the wired and wireless connections. Which of the following incident response phases was just completed?

- A. Preparation
- B. Identification
- C. Containment
- D. Eradication
- E. Recovery
- F. Lessons learned

Answer: C

QUESTION 1428

Which of the following are examples of two-factor authentication? (Select THREE)

- A. Voice recognition and fingerprint
- B. Proximity reader and password
- C. User ID and password
- D. Smart card and PIN
- E. Password and TOTP
- F. Smart card and ID badge

Answer: BDE

QUESTION 1429

A security engineer wants to be able to monitor and configure network devices remotely and securely. Which of the following would be the BEST option for this objective?

- A. SNMPv3
- B. DNSSEC
- C. SFTP
- D. S/MIME
- E. AES

Answer: A

QUESTION 1430

Which of the following is a type of attack in which a hacker leverages previously obtained packets to gain access to a wireless network?

- A. Replay attack
- B. ARP poisoning
- C. Bluesnarfing
- D. IP spoofing

Answer: A

QUESTION 1431

Which of the following is a characteristic unique to a Type 1 hypervisor?

- A. Memory is directly controlled by the hypervisor

- B. There is support for two or more operating systems to run simultaneously
- C. It has the ability to pass through peripheral devices to the guest operating systems
- D. Snapshots of the guest operating systems can be taken

Answer: C

QUESTION 1432

Which of the following explains the importance of patching servers in a test environment?

- A. It identifies potential availability and stability issues before they affect production systems
- B. It prioritizes the security of the organizations critical internal systems before the external systems are secured
- C. It facilitates the update of the organization's secure baselines before impacting production.
- D. It shortens the time to patch production systems by working out issues in the test and staging environments

Answer: A

QUESTION 1433

A systems administrator performing routine maintenance notices a user's profile is sending GET requests to an external IP address. Which of the following BEST fits this IOC?

- A. Logic bomb
- B. Trojan
- C. Bots
- D. Key logger

Answer: C

QUESTION 1434

An employee of a large payroll company has a machine that recently started locking up randomly with greatly increased processor consumption.

Which of the following is the FIRST action an analyst should take to investigate this potential IoC?

- A. Actively monitor traffic from the system to see if there is some form of command and control
- B. Capture a memory dump of the system for further evaluation of malicious processes
- C. Reimage the machine from a known-good image and get it back to the employee
- D. Take a full disk image of the filesystem to analyze files for possible malicious activity.

Answer: D

QUESTION 1435

A large organization has recently noticed an increase in the number of corporate mobile devices that are being lost. These mobile devices are used exclusively for on-campus communication at the organization's international headquarters using the wireless network. Per the organization's policy the devices should not be taken off campus. The security team must find a solution that will encourage users to leave the devices on campus. Which of the following is the BEST solution?

- A. Geofencing
- B. Remote wipe
- C. Tethering
- D. Mobile device management

Answer: D

QUESTION 1436

An administrator is trying to inspect SSL traffic to evaluate if it has a malicious code injection. The administrator is

[SY0-501 Exam Dumps](#) [SY0-501 Exam Questions](#) [SY0-501 PDF Dumps](#) [SY0-501 VCE Dumps](#)

<https://www.braindump2go.com/sy0-501.html>

planning to use the inspection features of a firewall solution. Which of the following should be done after the implementation of the firewall solution?

- A. Export the certificate chain to the WAF
- B. Store all private keys in the DMZ escrow server
- C. Generate the new firewall certificate and import it to all the user's endpoints
- D. Import the private certificate of each user to the firewall

Answer: A

QUESTION 1437

During a recent security audit, an organization discovered that server configurations were changed without documented approval. The investigators have confirmed that configuration changes require elevated permissions, and the investigation has failed to identify specific user accounts that are making the configuration changes. Which of the following is MOST likely occurring?

- A. Users have been sharing superuser account passwords
- B. Privileged accounts are being used by systems administrators
- C. Intruders have compromised the servers and enabled guest accounts
- D. Administrators are logging in to the servers using service accounts

Answer: A

QUESTION 1438

A security administrator is reviewing the following report from an organization's patch management system that has only wired workstations which are utilized daily:

| PC name | Finance application version | Browser version | Antivirus version | Last IP address | Last connection |
|---------|-----------------------------|-----------------|-------------------|-----------------|-----------------|
| ACCT-1 | 2.0 | 57.20 | 1.0 | 172.16.4.18/16 | 6 days |
| ACCT-2 | 2.30 | 56.80 | 1.2 | 172.17.30.17/16 | 8 hours |
| HR-1 | 2.0 | 56.80 | 1.1 | 172.16.4.27/16 | 1 hour |
| SALES-1 | 2.30 | 56.80 | 1.2 | 172.16.4.9/16 | 2 hours |
| SALES-2 | N/A | 56.80 | 1.2 | 172.16.4.16/16 | 1 day |

Which of the following is the GREATEST security concern for the administrator?

- A. The browser version on ACCT-1 is newer than the rest.
- B. The status of ACCT-1 is not accurately reported
- C. SALES-2 does not have the finance application installed
- D. ACCT-2 is no longer connecting from the organization's network

Answer: B

QUESTION 1439

An analyst is trying to obtain a signed certificate from a CA by pasting a public key into the CA's web request form; however it does not work and an error is generated.

Which of the following does the analyst need to paste into the web request form?

- A. A private key
- B. A CSR
- C. The OID
- D. A certificate Chain

Answer: C

QUESTION 1440

An organization is collecting logs from its critical infrastructure and a large number of the events are common system activities with identical logs. This is causing the SI EM to consume a large amount of disk space, which may result in the organization having to purchase additional disks to store the logs. Which of the following should the organization do to help mitigate this problem?

- A. Enable event deduplication
- B. Enable log correlation
- C. Enable log aggregation
- D. Enable log filtering.

Answer: C

QUESTION 1441

Which of the following BEST describes a defense-in-depth strategy?

- A. A security administrator places a web server behind two firewalls from two different vendors with only ports 80 and 443 open
- B. The security architect scans servers daily with a vulnerability scanner and conducts weekly penetration-testing exercises
- C. The security team configures an application-whitelisting program on endpoints and installs NIDS.
- D. Outbound traffic travels through a proxy and a stateful firewall with ports 80 and 443 open

Answer: C

QUESTION 1442

A security analyst wants to obfuscate some code and decides to use ROT13. Which of the following is an example of the text "HELLO WORLD" in ROT13?

- A. DLROWOLLEH
- B. URYYB JBEYQ
- C. KHOOR ZRUOG
- D. QYEBJ BYYRU

Answer: B

QUESTION 1443

During an assessment a security analyst was asked to use a service account to perform a vulnerability scan against the main application server.

Which of the following BEST classifies this type of test?

- A. Non-intrusive test
- B. Credentialed test
- C. Escalation of privilege test
- D. Initial exploitation test

Answer: B

QUESTION 1444

Joe a user visited a banking website from a saved bookmark and logged in with his credentials After logging in. Joe discovered he could not access any resources and none of his account information would display. The next day, the bank called to report his account had been compromised. Which of the following MOST likely would have prevented this from occurring?

- A. SSH

- B. TLS
- C. LDAPS
- D. DNSSEC

Answer: B

QUESTION 1445

Passive reconnaissance during a penetration test consists of:

- A. open-source intelligence gathering
- B. social engineering to obtain target information
- C. non-intrusive vulnerability scanning
- D. probing the target network in a methodical manner

Answer: A

QUESTION 1446

Which of the following has a direct impact on whether a company can meet the RTO?

- A. MTTR
- B. MTBF
- C. ARO
- D. RPO

Answer: A

QUESTION 1447

A security administrator learns that PII, which was gathered by the organization, has been found in an open forum. As a result, several C-level executives found their identities were compromised and they were victims of a recent whaling attack.

Which of the following would prevent these problems in the future? (Select TWO)

- A. Implement a reverse proxy
- B. Implement an email DLP
- C. Implement a spam filter
- D. Implement a host-based firewall
- E. Implement a HI DS

Answer: BC

QUESTION 1448

A government contractor has a security requirement that any service in use must not be accessible by a non-governmental agency.

The contractor is trying to reduce costs by moving the on-premises virtual servers to the cloud in a single-tenant environment.

Which of the following would BEST meet the requirements?

- A. Public PaaS
- B. Public SaaS
- C. Public IaaS
- D. Private PaaS
- E. Private SaaS
- F. Private IaaS

Answer: F

