SY0-501$^{\text{Q\&As}}$

CompTIA Security+ Certification Exam

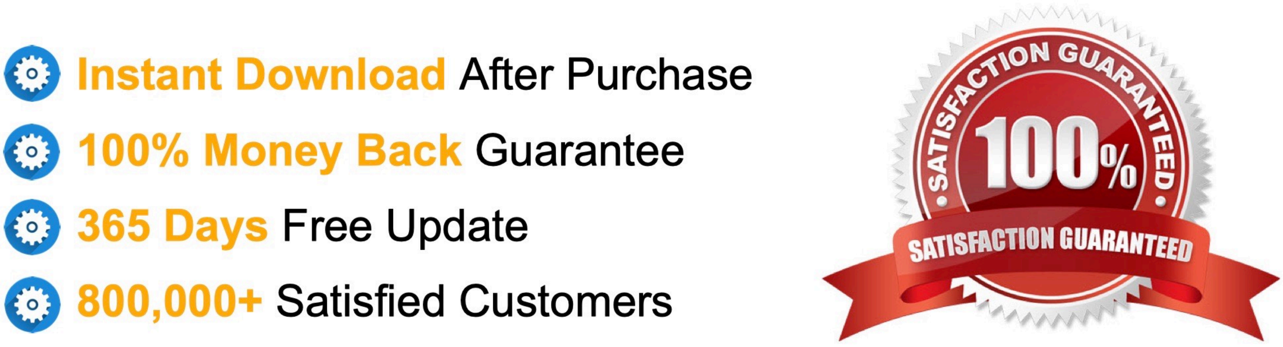
Pass CompTIA SY0-501 Exam with 100% Guarantee

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

https://www.leads4pass.com/sy0-501.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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

A recent internal audit is forcing a company to review each internal business unit\\'s VMs because the cluster they are installed on is in danger of running out of computer resources. Which of the following vulnerabilities exist?

A. Buffer overflow

B. End-of-life systems

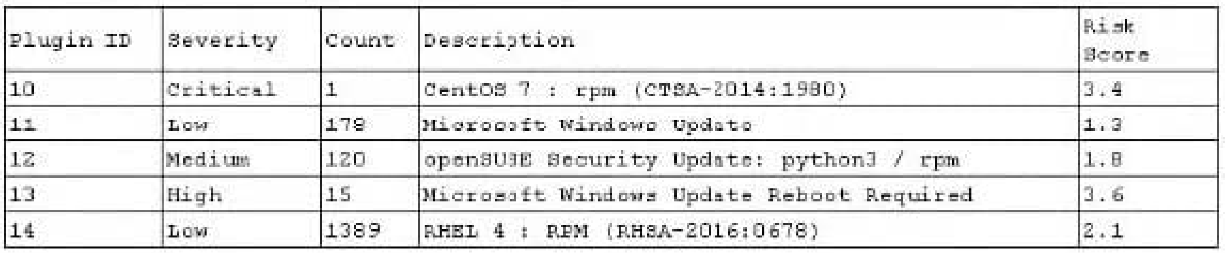
C. System sprawl

D. Weak configuration

Correct Answer: C

QUESTION 2

A network administrator was provided the following output from a vulnerability scan.



Plugin ID	Severity	Count	Description	Risk Score
10	Critical	1	CentOS 7 : rpm (CTSA-2014:1980)	3.4
11	Low	178	Microsoft Windows Update	1.3
12	Medium	120	openSUSE Security Update: python3 / rpm	1.8
13	High	15	Microsoft Windows Update Reboot Required	3.6
14	Low	1389	RHEL 4 : RPM (RHSA-2016:0678)	2.1

The network administrator has been instructed to prioritize remediation efforts based on overall risk to the enterprise. Which of the following plugin IDs should be remediated FIRST?

A. 10

B. 11

C. 12

D. 13

E. 14

Correct Answer: D

QUESTION 3

The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate severs at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?

A. Implement deduplication at the network level between the two locations

B. Implement deduplication on the storage array to reduce the amount of drive space needed

C. Implement deduplication on the server storage to reduce the data backed up

D. Implement deduplication on both the local and remote servers

Correct Answer: B

QUESTION 4

An email recipient is unable to open a message encrypted through PKI that was sent from another organization. Which of the following does the recipient need to decrypt the message?

A. The sender\\'s private key

B. The recipient\\'s private key

C. The recipient\\'s public key

D. The CA\\'s root certificate

E. The sender\\'s public key

F. An updated CRL

Correct Answer: E

QUESTION 5

Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

A. Logic bomb

B. Trojan

C. Scareware

D. Ransomware

Correct Answer: A

QUESTION 6

A systems administrator is installing and configuring an application service that requires access to read and write to log and configuration files on a local hard disk partition. The service must run as an account with authorization to interact with the file system. Which of the following would reduce the attack surface added by the service and account? (Choose two.)

A. Use a unique managed service account.

B. Utilize a generic password for authenticating.

C. Enable and review account audit logs.

D. Enforce least possible privileges for the account.

E. Add the account to the local administrators group.

F. Use a guest account placed in a non-privileged users group.

Correct Answer: AD

QUESTION 7

When sending messages using symmetric encryption, which of the following must happen FIRST?

A. Exchange encryption key

B. Establish digital signatures

C. Agree on an encryption method

D. Install digital certificates

Correct Answer: C

QUESTION 8

Joe, a user at a company, clicked an email link that led to a website that infected his workstation. Joe was connected to the network, and the virus spread to the network shares. The protective measures failed to stop this virus, and it has continued to evade detection. Which of the following should a security administrator implement to protect the environment from this malware?

A. Install a definition-based antivirus.

B. Implement an IDS/IPS.

C. Implement a heuristic behavior-detection solution.

D. Implement CASB to protect the network shares.

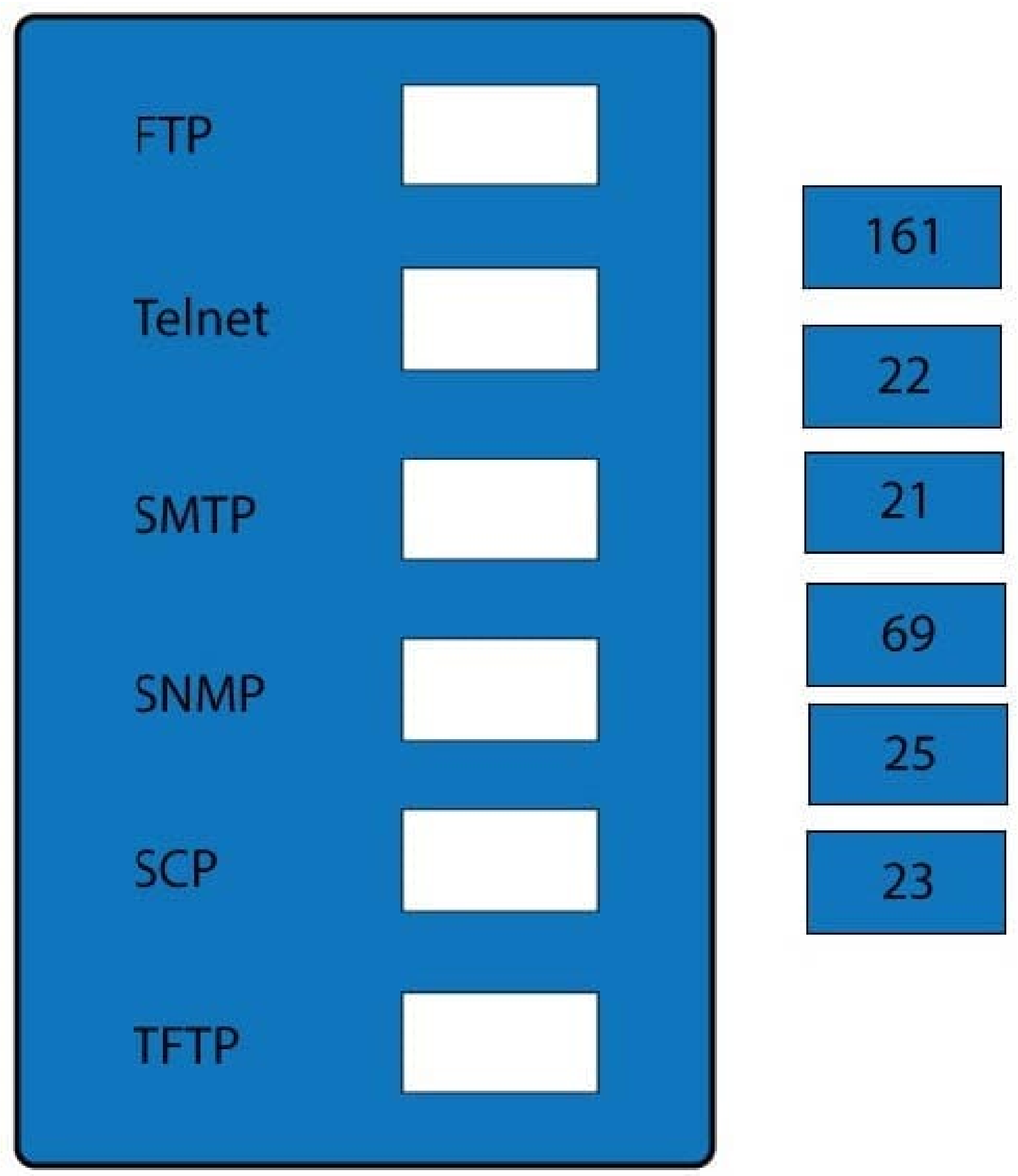
Correct Answer: B

QUESTION 9

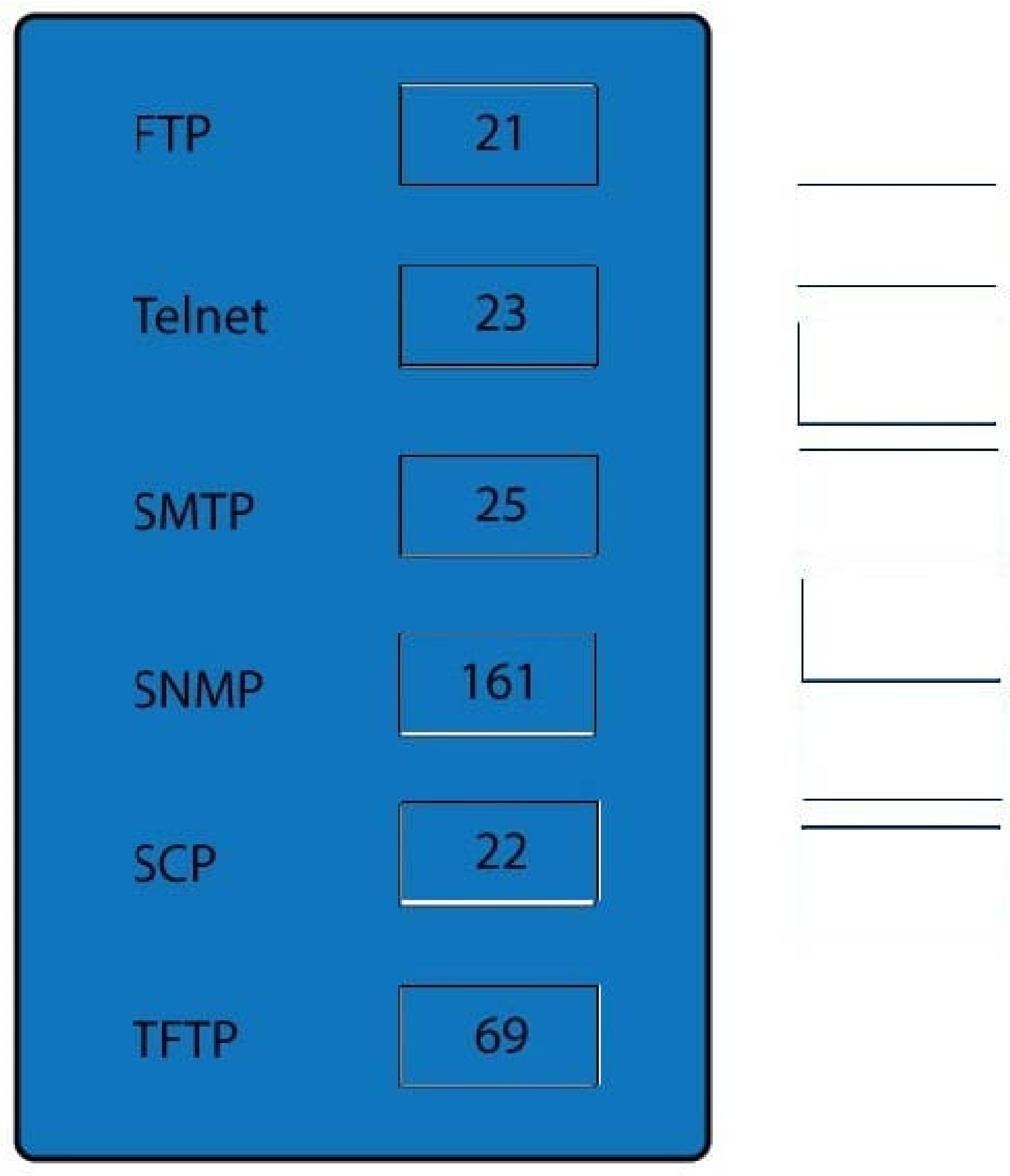
DRAG DROP

Drag and drop the correct protocol to its default port.

Select and Place:



Correct Answer:



FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

FTP uses TCP port 21.

Telnet uses port 23.

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure filetransfer facility based on SSH and Remote Copy Protocol (RCP).

Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).

SMTP uses TCP port 25.

Port 69 is used by TFTP.

SNMP makes use of UDP ports 161 and 162.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 42, 45, 51

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 10

A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?

A. It can protect multiple domains

B. It provides extended site validation

C. It does not require a trusted certificate authority

D. It protects unlimited subdomains

Correct Answer: B

QUESTION 11

A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network. Which of the following security measures did the technician MOST likely implement to cause this Scenario?

A. Deactivation of SSID broadcast

B. Reduction of WAP signal output power

C. Activation of 802.1X with RADIUS

D. Implementation of MAC filtering

E. Beacon interval was decreased

Correct Answer: A

QUESTION 12

A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?

A. Time-of-day restrictions

B. Permission auditing and review

C. Offboarding

D. Account expiration

Correct Answer: C

QUESTION 13

An organization electronically processes sensitive data within a controlled facility. The Chief Information Security Officer (CISO) wants to limit emissions from emanating from the facility. Which of the following mitigates this risk?

A. Upgrading facility cabling to a higher standard of protected cabling to reduce the likelihood of emission spillage

B. Hardening the facility through the use of secure cabinetry to block emissions

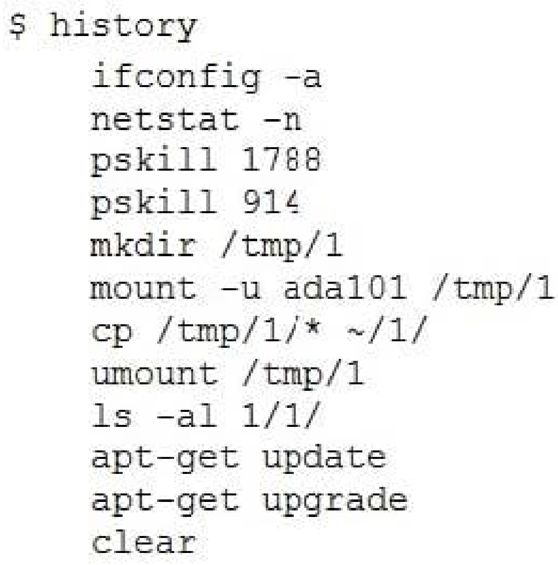
C. Hardening the facility with a Faraday cage to contain emissions produced from data processing

D. Employing security guards to ensure unauthorized personnel remain outside of the facility

Correct Answer: C

QUESTION 14

A company has forbidden the use of external media within its headquarters location. A security analyst is working on adding additional repositories to a server in the environment when the analyst notices some odd processes running on the system. The analyst runs a command and sees the following:



```
$ history
    ifconfig -a
    netstat -n
    pskill 1788
    pskill 914
    mkdir /tmp/1
    mount -u ada101 /tmp/1
    cp /tmp/1/* ~/1/
    umount /tmp/1
    ls -al 1/1/
    apt-get update
    apt-get upgrade
    clear
```

Given this output, which of the following security issues has been discovered?

A. A misconfigured HIDS

B. A malware installation

C. A policy violation

D. The activation of a Trojan

Correct Answer: B

QUESTION 15

Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?

A. Shibboleth

B. RADIUS federation

C. SAML

D. OAuth

E. OpenID connect

Correct Answer: B

Reference: http://archive.oreilly.com/pub/a/wireless/2005/01/01/authentication.html