RC0-501 Q&As

CompTIA Security+ Recertification Exam

Pass CompTIA RC0-501 Exam with 100% Guarantee

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

https://www.leads4pass.com/rc0-501.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

QUESTION 1

An auditor wants to test the security posture of an organization by running a tool that will display the following:

```
JIMS            <00> UNIQUE     Registered
WORKGROUP       <00> GROUP      Registered
JIMS            <00> UNIQUE     Registered
```

Which of the following commands should be used?

A. nbtstat

B. nc

C. arp

D. ipconfig

Correct Answer: A

QUESTION 2

During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could best prevent this from occurring again?

A. Credential management

B. Group policy management

C. Acceptable use policy

D. Account expiration policy

Correct Answer: B

QUESTION 3

When identifying a company\\'s most valuable assets as part of a BIA, which of the following should be the FIRST priority?

A. Life

B. Intellectual property

C. Sensitive data

D. Public reputation

Correct Answer: A

QUESTION 4

A security administrator has found a hash in the environment known to belong to malware. The administrator then finds this file to be in in the preupdate area of the OS, which indicates it was pushed from the central patch system.

File: winx86_adobe_flash_upgrade.exe Hash: 99ac28bede43ab869b853ba62c4ea243

The administrator pulls a report from the patch management system with the following output: Given the above outputs, which of the following MOST likely happened?

Install Date	Package Name	Target Devices	Hash
10/10/2017	java_11.2_x64.exe	HQ PC's	01ab28bbde63aa879b35kba62cdes283
10/10/2017	winx86_adobe_flash_upgrade.exe	HQ PC's	99ac28bede43ab869b853ba62c4ea243

A. The file was corrupted after it left the patch system.

B. The file was infected when the patch manager downloaded it.

C. The file was not approved in the application whitelist system.

D. The file was embedded with a logic bomb to evade detection.

Correct Answer: B

QUESTION 5

A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

A. 1

B. 2

C. 3

D. 4

Correct Answer: B

QUESTION 6

Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened. The network and security teams perform the following actions:

Shut down all network shares.

Run an email search identifying all employees who received the malicious message. Reimage all devices belonging to users who opened the attachment. Next, the teams want to re-enable the network shares. Which of the following BEST

describes this phase of the incident response process?

A. Eradication

B. Containment

C. Recovery

D. Lessons learned

Correct Answer: C

QUESTION 7

A company\\'s user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are MOST likely occurring? (Choose two.)

A. Replay

B. Rainbow tables

C. Brute force

D. Pass the hash

E. Dictionary

Correct Answer: CE

QUESTION 8

A system\\'s administrator has finished configuring firewall ACL to allow access to a new web server.

```
PERMIT TCP from: ANY to: 192.168.1.10:80
PERMIT TCP from: ANY to: 192.168.1.10:443
DENY TCP from: ANY to: ANY
```

The security administrator confirms form the following packet capture that there is network traffic from the internet to the web server:

```
TCP 10.23.243.2:2000->192.168.1.10:80 POST/default's
TCP 172.16.4.100:1934->192.168.1.10:80 GET/session.aspx?user1_sessionid=
a12ad8741d8f7e7ac723847cBaa8231a
```

The company\\'s internal auditor issues a security finding and requests that immediate action be taken. With which of the following is the auditor MOST concerned?

A. Misconfigured firewall

B. Clear text credentials

C. Implicit deny

D. Default configuration

Correct Answer: B

QUESTION 9

Malicious traffic from an internal network has been detected on an unauthorized port on an application server. Which of the following network-based security controls should the engineer consider implementing?

A. ACLs

B. HIPS

C. NAT

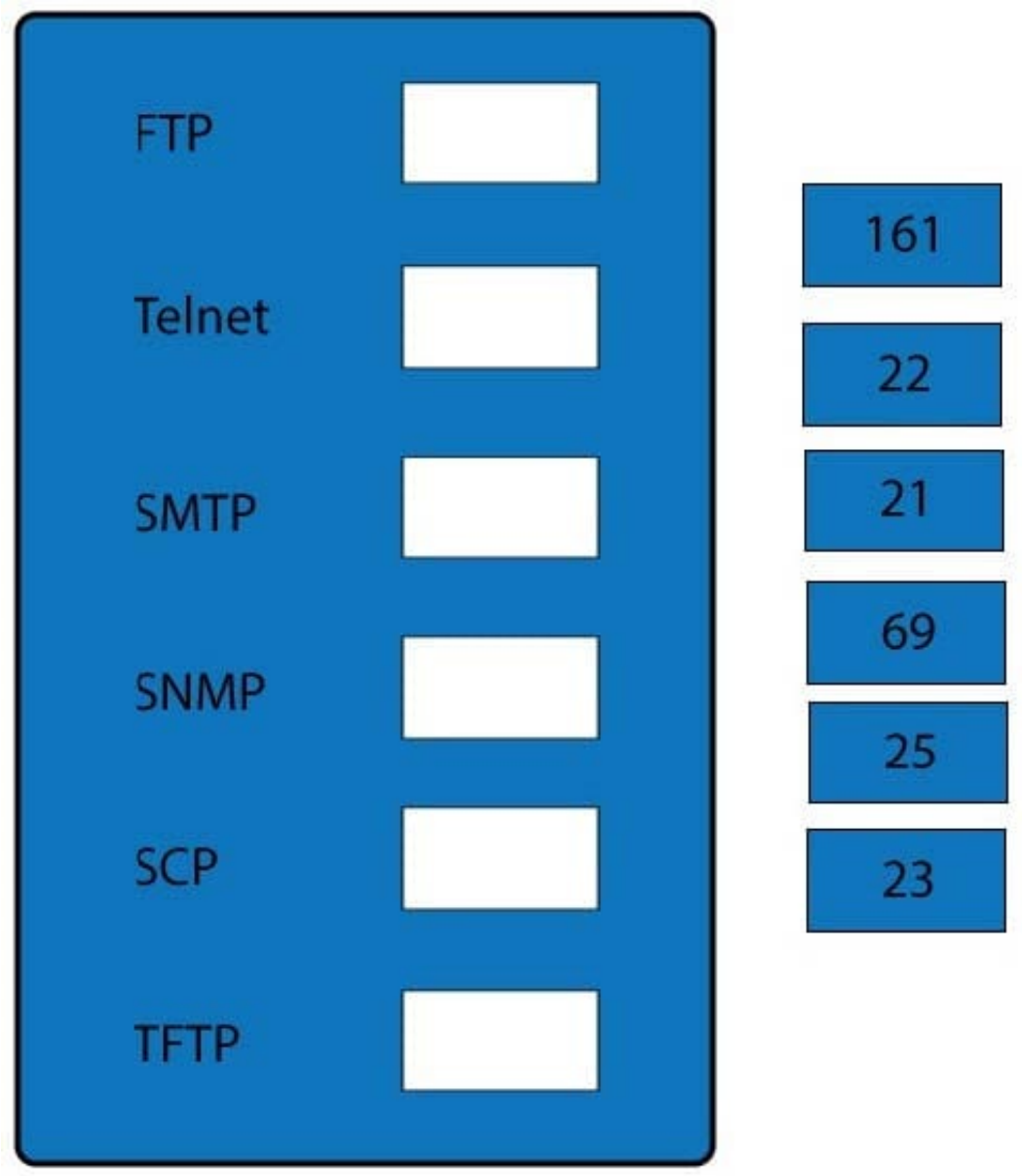
D. MAC filtering

Correct Answer: A

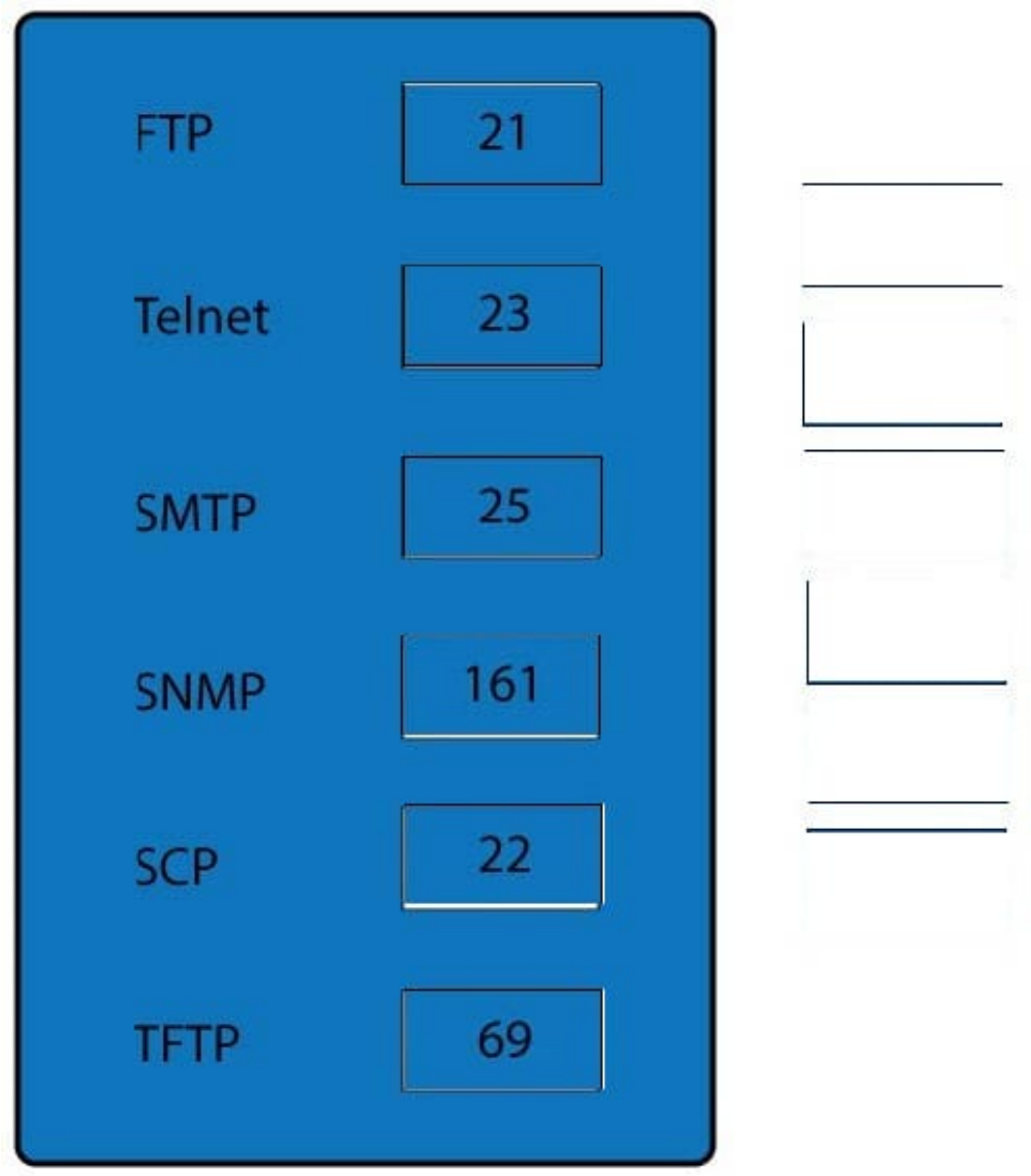
QUESTION 10

Drag and drop the correct protocol to its default port.

Select and Place:



Correct Answer:



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 11

Company policy requires the use if passphrases instead if passwords. Which of the following technical controls MUST be in place in order to promote the use of passphrases?

A. Reuse

B. Length

C. History

D. Complexity

Correct Answer: D

QUESTION 12

The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers\\' names and credit card numbers with the PIN. Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted

B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance

C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files

D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

Correct Answer: C

QUESTION 13

A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user\\'s computers without exception. Which of the following should the administrator do to prevent all unapproved software from running on the user\\'s computer?

A. Deploy antivirus software and configure it to detect and remove pirated software

B. Configure the firewall to prevent the downloading of executable files

C. Create an application whitelist and use OS controls to enforce it

D. Prevent users from running as administrator so they cannot install software.

Correct Answer: C

QUESTION 14

A company\\'s AUP requires:

Passwords must meet complexity requirements.

Passwords are changed at least once every six months.

Passwords must be at least eight characters long.

An auditor is reviewing the following report:

Username	Last login	Last changed
Carol	2 hours	90 days
David	2 hours	30 days
Ann	1 hour	247 days
Joe	0.5 hours	7 days

Which of the following controls should the auditor recommend to enforce the AUP?

A. Account lockout thresholds

B. Account recovery

C. Password expiration

D. Prohibit password reuse

Correct Answer: C

QUESTION 15

While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy. Which of the following tool or technology would work BEST for obtaining more information on this traffic?

A. Firewall logs

B. IDS logs

C. Increased spam filtering

D. Protocol analyzer

Correct Answer: B