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

The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administer has determined that attackers are still able to detect the presence of

the wireless network despite the fact the SSID has been disabled.

Which of the following would further obscure the presence of the wireless network?

A. Upgrade the encryption to WPA or WPA2

B. Create a non-zero length SSID for the wireless router

C. Reroute wireless users to a honeypot

D. Disable responses to a broadcast probe request

Correct Answer: D

QUESTION 2

After a user reports stow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.

The systems administrator reviews the output below:

```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address     Foreign Address        State
TCP   0.0.0.0:135       0.0.0.0:0              LISTENING       RpcSs [svchost.exe]
TCP   0.0.0.0:445       0.0.0.0:0              LISTENING       [svchost.exe]

TCP   192.168.1.10:5000 10.37.213.20           ESTABLISHED     winserver.exe
UDP   192.168.1.10:1900 *.*                                    SSDPSVR
```

Based on the above information, which of the following types of malware was installed on the user\\'s computer?

A. RAT

B. Keylogger

C. Spyware

D. Worm

E. Bot

Correct Answer: A

QUESTION 3

A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations. Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)

A. SCP

B. TFTP

C. SNMP

D. FTP

E. SMTP

F. FTPS

Correct Answer: AF

QUESTION 4

A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

A. An attacker can access and change the printer configuration.

B. SNMP data leaving the printer will not be properly encrypted.

C. An MITM attack can reveal sensitive information.

D. An attacker can easily inject malicious code into the printer firmware.

E. Attackers can use the PCL protocol to bypass the firewall of client computers.

Correct Answer: B

QUESTION 5

Which of the following AES modes of operation provide authentication? (Select two.)

A. CCM

B. CBC

C. GCM

D. DSA

E. CFB

Correct Answer: AC

QUESTION 6

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 7

Which of the following security controls does an iris scanner provide?

A. Logical

B. Administrative

C. Corrective

D. Physical

E. Detective

F. Deterrent

Correct Answer: D

QUESTION 8

An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request. Which of the following secure protocols is the developer MOST likely to use?

A. FTPS

B. SFTP

C. SSL

D. LDAPS

Correct Answer: C

QUESTION 9

A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack. News outlets discover a certain type of refrigerator was explogted and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong?

A. SoC

B. ICS

C. IoT

D. MFD

Correct Answer: C

QUESTION 10

A system administrator is configuring a site-to-site VPN tunnel. Which of the following should be configured on the VPN concentrator during the IKE phase?

A. RIPEMD

B. ECDHE

C. Diffie-Hellman

D. HTTPS

Correct Answer: C

QUESTION 11

A security administrator suspects that data on a server has been exhilarated as a result of unauthorized remote access. Which of the following would assist the administrator in con-firming the suspicions? (Select TWO)

A. Networking access control

B. DLP alerts

C. Log analysis

D. File integrity monitoring

E. Host firewall rules

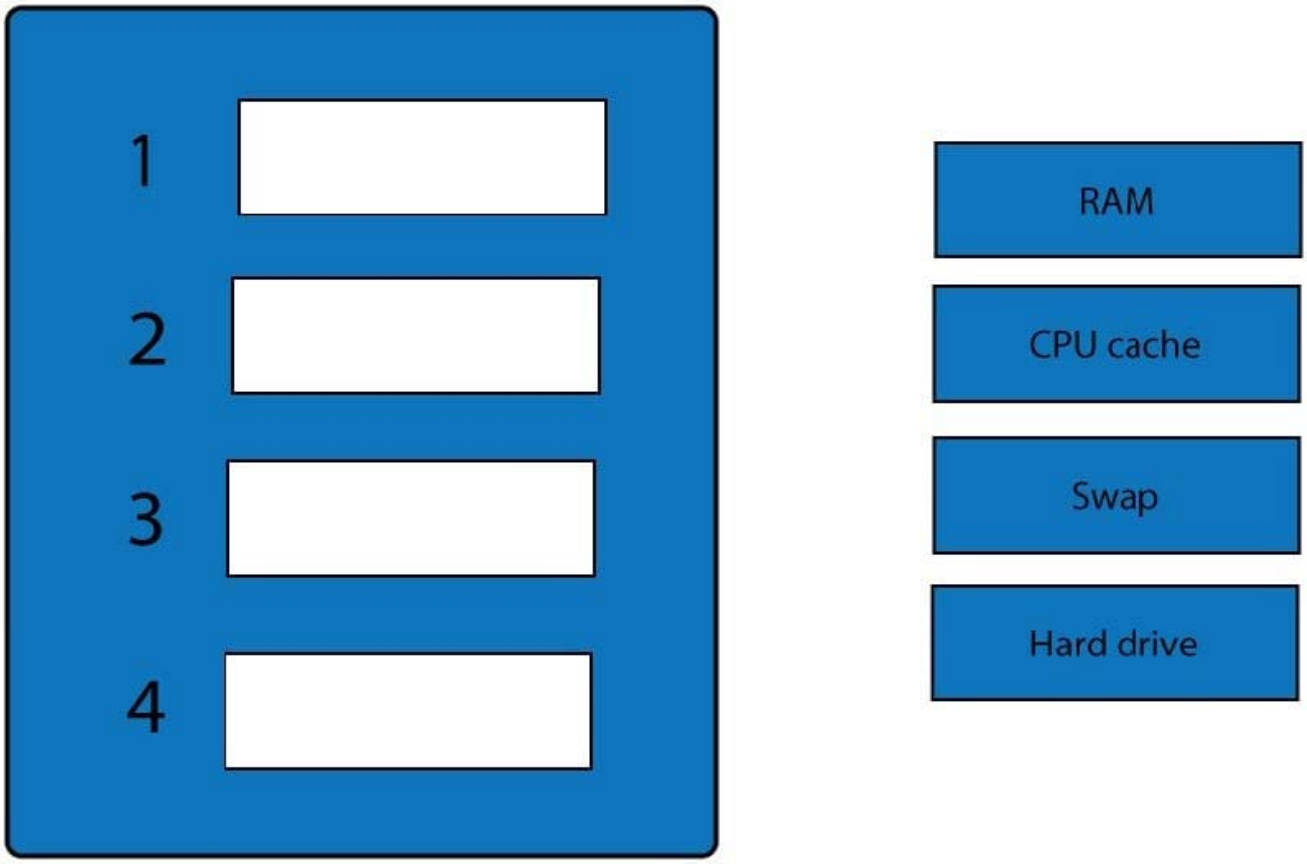
Correct Answer: BC

QUESTION 12

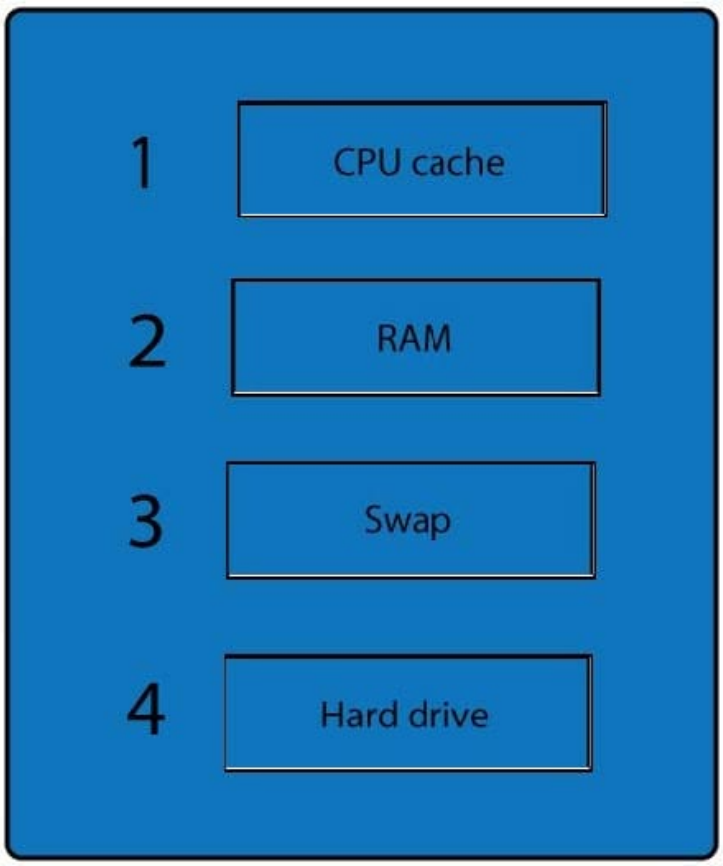
A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the

correct order in which the forensic analyst should preserve them.

Select and Place:



Correct Answer:



When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone.

Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and

printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and

expenses associated with the investigation.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 453

QUESTION 13

A systems administrator is reviewing the following information from a compromised server: Given the above information, which of the following processes was MOST likely exploited via a remote buffer overflow attack?

Process	DEP	Local Address	Remote Address
LSASS	YES	0.0.0.0.	10.210.100.62
APACHE	NO	0.0.0.0	10.130.210.20
MySQL	NO	127.0.0.1	127.0.0.1
TFTP	YES	191.168.1.10	10.34.221.96

A. Apache

B. LSASS

C. MySQL

D. TFTP

Correct Answer: A

QUESTION 14

A security administrator needs an external vendor to correct an urgent issue with an organization\\'s physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system. Which of the following methods should the security administrator select the best balances security and efficiency?

A. Temporarily permit outbound internet access for the pacs so desktop sharing can be set up

B. Have the external vendor come onsite and provide access to the PACS directly

C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing

D. Set up a web conference on the administrator\\'s pc; then remotely connect to the pacs

Correct Answer: C

QUESTION 15

A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access. Which of the following would be the BEST course of action?

A. Modify all the shared files with read only permissions for the intern.

B. Create a new group that has only read permissions for the files.

C. Remove all permissions for the shared files.

D. Add the intern to the "Purchasing" group.

Correct Answer: B

RC0-501 VCE Dumps RC0-501 Practice Test RC0-501 Exam Questions