**QUESTION 1**

A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment?

A. A perimeter firewall and IDS

B. An air gapped computer network

C. A honeypot residing in a DMZ

D. An ad hoc network with NAT

E. A bastion host

Correct Answer: B

**QUESTION 2**

An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection. Which of the following AES modes of operation would meet this integrity-only requirement?

A. HMAC

B. PCBC

C. CBC

D. GCM

E. CFB

Correct Answer: A

**QUESTION 3**

A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

A. PFX

B. PEM

C. DER

D. CER

Correct Answer: B

**QUESTION 4**

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 5**

Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain. Which of the following tools would aid her to decipher the network traffic?

A. Vulnerability Scanner

B. NMAP

C. NETSTAT

D. Packet Analyzer

Correct Answer: C


**QUESTION 6**

A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The

bank president thought separation of duties would prevent this from happening.

In order to implement a true separation of duties approach the bank could:

A. Require the use of two different passwords held by two different individuals to open an account

B. Administer account creation on a role based access control approach

C. Require all new accounts to be handled by someone else other than a teller since they have different duties

D. Administer account creation on a rule based access control approach

Correct Answer: C

---

**QUESTION 7**

Which of the following best describes the initial processing phase used in mobile device forensics?

A. The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device

B. The removable data storage cards should be processed first to prevent data alteration when examining the mobile device

C. The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again D. The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.

Correct Answer: D

---

**QUESTION 8**

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 9**

A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.0:6666. Which of the following should the security analyst do to determine if the compromised system still has an active connection?

A. tracert

B. netstat

C. ping

D. nslookup

Correct Answer: B

## QUESTION 10

An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?

A. Find two identical messages with different hashes

B. Find two identical messages with the same hash

C. Find a common has between two specific messages

D. Find a common hash between a specific message and a random message

Correct Answer: A

## QUESTION 11

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 12

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 13**

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 14**

Which of the following are methods to implement HA in a web application server environment? (Select two.)

A. Load balancers

B. Application layer firewalls

C. Reverse proxies

D. VPN concentrators

E. Routers

Correct Answer: AB

**QUESTION 15**

Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

A. War chalking

B. Bluejacking

C. Bluesnarfing

D. Rogue tethering

Correct Answer: B

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

RC0-501 Practice Test                RC0-501 Study Guide                RC0-501 Exam Questions