CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.pass4itsure.com/cs0-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A medical organization recently started accepting payments over the phone. The manager is concerned about the impact of the storage of different types of data. Which of the following types of data incurs the highest regulatory constraints?

A. PHI

B. PCI

C. PII

D. IP

Correct Answer: B

QUESTION 2

A company just chose a global software company based in Europe to implement a new supply chain management solution. Which of the following would be the MAIN concern of the company?

A. Violating national security policy

B. Packet injection

C. Loss of intellectual property

D. International labor laws

Correct Answer: A

QUESTION 3

Which of the following could be directly impacted by an unpatched vulnerability in vSphere ESXi?

A. The organization\\'s physical routers

B. The organization\\'s mobile devices

C. The organization\\'s virtual infrastructure

D. The organization\\'s VPN

Correct Answer: C

QUESTION 4

The SFTP server logs show thousands of failed login attempts from hundreds of IP addresses worldwide. Which of the following controls would BEST protect the service?

A. Whitelisting authorized IP addresses

B. Blacklisting unauthorized IP addresses

C. Enforcing more complex password requirements

D. Establishing a sinkhole service

Correct Answer: A

QUESTION 5

A nuclear facility manager determined the need to monitor utilization of water within the facility. A startup company just announced a state-of-the-art solution to address the need for integrating the business and ICS network. The solution requires a very small agent to be installed on the ICS equipment. Which of the following is the MOST important security control for the manager to invest in to protect the facility?

A. Run a penetration test on the installed agent.

B. Require that the solution provider make the agent source code available for analysis.

C. Require through guides for administrator and users.

D. Install the agent for a week on a test system and monitor the activities.

Correct Answer: D

QUESTION 6

An organization has recently found some of its sensitive information posted to a social media site. An investigation has identified large volumes of data leaving the network with the source traced back to host 192.168.1.13. An analyst performed a targeted Nmap scan of this host with the results shown below:

```
Starting Nmap 4.67 (http://nmap.org) at 2011-11-03 18:32 EDT
Nmap scan report for 192.168.1.13
Host is up (0.00066s latency).
Not shown: 990 closed ports
PORT            STATE           SERVICE
22/tcp          open            ssh
80/tcp          open            http
111/tcp         open            rpcbind
139/tcp         open            netbios-ssn
1417/tcp        open            timbuktu-srv1
3306/tcp        open            mysql
27573/tcp       open            winHelper

MAC Address:01:AA:FB:23:21:15

Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds
```

Subsequent investigation has allowed the organization to conclude that all of the well-known, standard ports are secure. Which of the following services is the problem?

A. winHelper

B. ssh

C. rpcbind

D. timbuktu-serv1

E. mysql

Correct Answer: D

QUESTION 7

Which of the following policies would slate an employee should not disable security safeguards, such as host firewalls and antivirus on company systems?

A. Code of conduct policy

B. Account management policy

C. Password policy

D. Acceptable use policy

Correct Answer: D

QUESTION 8

A security analyst is reviewing the following web server log: GET %2f..%2f..%2f.. %2f.. %2f.. %2f.. %2f../etc/passwd
Which of the following BEST describes the issue?

A. Directory traversal exploit

B. Cross-site scripting

C. SQL injection

D. Cross-site request forgery

Correct Answer: A

QUESTION 9

An organization has the following risk mitigation policies

Risks without compensating controls will be mitigated first if the risk value is greater than $50,000.

Other risk mitigation will be prioritized based on risk value.

The following risks have been identified:

Risk	Probability	Impact	Compensating control?
A	80%	$100,000	Y
B	20%	$500,000	Y
C	50%	$120,000	N
D	40%	$80,000	N

Which of the following is the order of priority for risk mitigation from highest to lowest?

A. A, C, D, B

B. B, C, D, A

C. C, B, A, D

D. C. D, A, B

E. D, C, B, A

Correct Answer: C

QUESTION 10

SIMULATION

Malware is suspected on a server in the environment.

The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.

INSTRUCTIONS

Servers 1, 2, and 4 are clickable. Select the Server and the process that host the malware.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All 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.

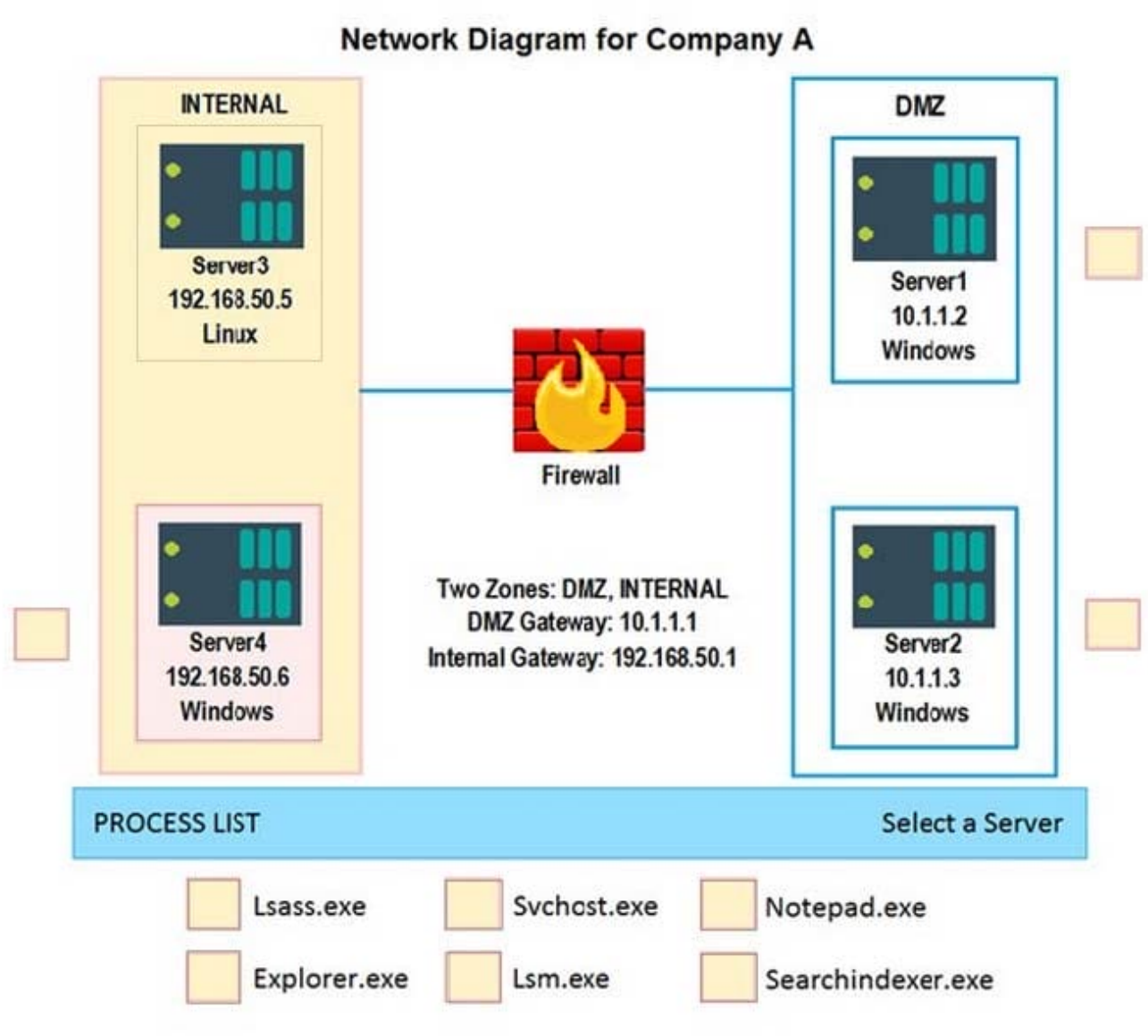
Server1 Log

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	1,340 K
smss.exe	300	Services	0	884 K
csrss.exe	384	Services	0	3,048 K
wininit.exe	432	Services	0	3,284 K
services.exe	532	Services	0	7,832 K
lsass.exe	540	Services	0	9,776 K
lsm.exe	560	Services	0	5,164 K
svchost.exe	884	Services	0	22,528 K
svchost.exe	276	Services	0	9,860 K
svchost.exe	348	Services	0	12,136 K
spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
notepad.exe	1276	Services	0	4,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K

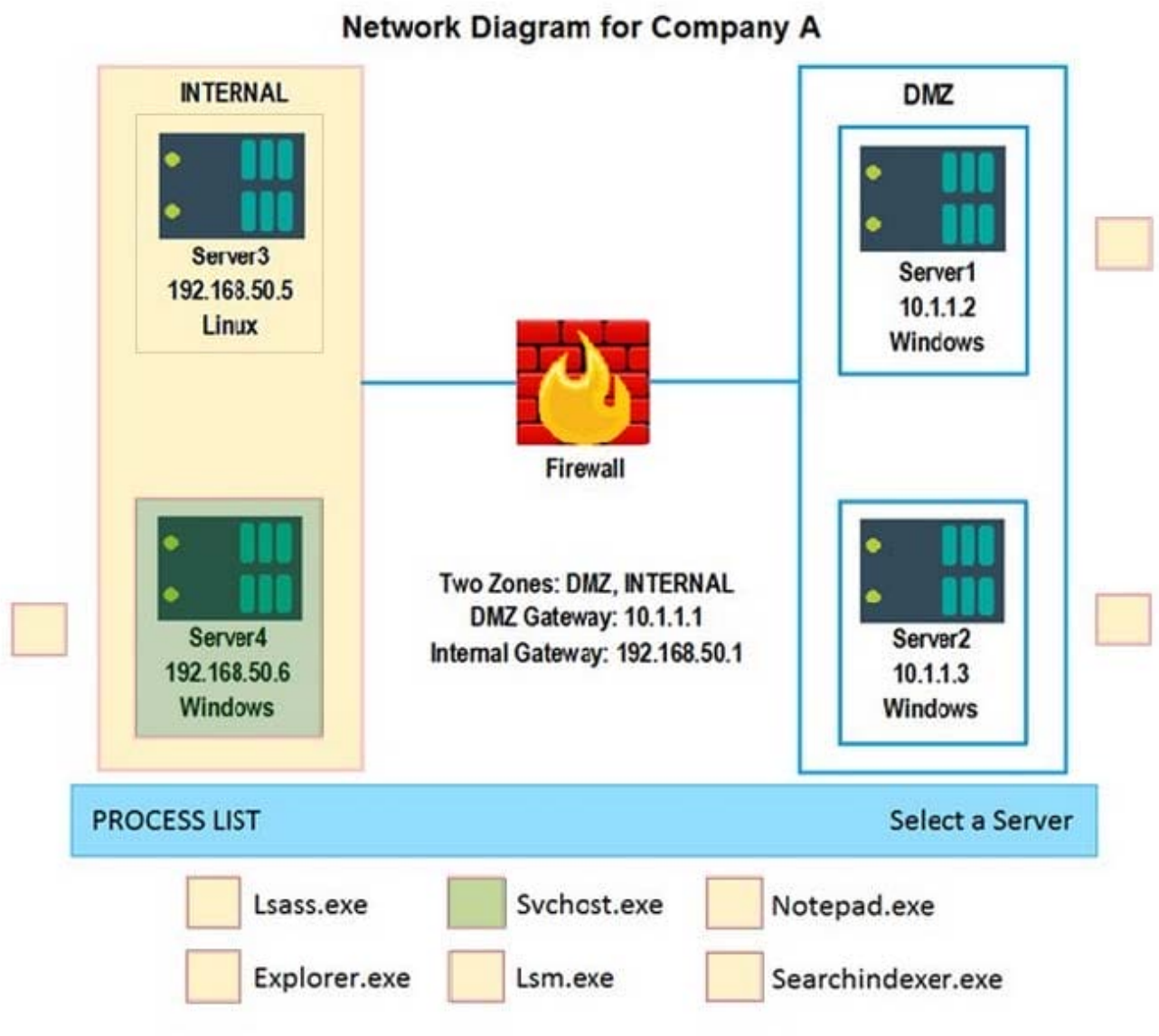
Server4 Log

spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K
explorer.exe	2500	RDP-Tcp#0	1	66,444 K
splwow64.exe	2960	RDP-Tcp#0	1	4,152 K
cmd.exe	1260	RDP-Tcp#0	1	2,652 K
conhost.exe	2616	RDP-Tcp#0	1	5,256 K
audiodg.exe	980	Services	0	13,256 K
csrss.exe	2400	Console	3	3,512 K
winlogon.exe	2492	Console	3	5,772 K
LogonUI.exe	2864	Console	3	17,056 K
taskhost.exe	2812	Services	0	9,540 K
tasklist.exe	1208	RDP-Tcp#0	1	5,196 K
WmiPrvSE.exe	1276	Services	0	5,776 K

Hot Area:



Correct Answer:



Server 4, svchost.exe

QUESTION 11

A threat intelligence analyst who works for a technology firm received this report from a vendor.

"There has been an intellectual property theft campaign executed against organizations in the technology industry. Indicators for this activity are unique to each intrusion. The information that appears to be targeted is RandD data. The data exfiltration appears to occur over months via uniform TTPs. Please execute a defensive operation regarding this attack vector."

Which of the following combinations suggests how the threat should MOST likely be classified and the type of analysis that would be MOST helpful in protecting against this activity?

A. Polymorphic malware and secure code analysis

B. Insider threat and indicator analysis

C. APT and behavioral analysis

D. Ransomware and encryption

Correct Answer: C

QUESTION 12

A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO) asking the employee to perform a wife transfer Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?

A. Implementing a sandboxing solution for viewing emails and attachments

B. Limiting email from the finance department to recipients on a pre-approved whitelist

C. Configuring email client settings to display all messages in plaintext when read

D. Adding a banner to incoming messages that identifies the messages as external

Correct Answer: D

QUESTION 13

An analyst received a forensically sound copy of an employee\\'s hard drive. The employee\\'s manager suspects inappropriate images may have been deleted from the hard drive. Which of the following could help the analyst recover the deleted evidence?

A. File hashing utility

B. File timestamps

C. File carving tool

D. File analysis tool

Correct Answer: C

QUESTION 14

A digital forensics investigator works from duplicate images to preserve the integrity of the original evidence. Which of the following types of media are MOST volatile and should be preserved? (Choose two.)

A. Memory cache

B. Registry file

C. SSD storage

D. Temporary filesystems

E. Packet decoding

F. Swap volume

Correct Answer: AD

QUESTION 15

A security analyst sees the following OWASP ZAP output from a scan that was performed against a modern version of Windows while testing for client-side vulnerabilities:

Alert Detail Low (Medium) Web Browser XSS Protection not enabled Description: Web browser XSS protection not enabled, or disabled by the configuration of the HTTP Response header

URL: https://domain.com/sun/ray

Which of the following is the MOST likely solution to the listed vulnerability?

A. Enable the browser\\'s XSS filter.

B. Enable Windows XSS protection

C. Enable the browser\\'s protected pages mode

D. Enable server-side XSS protection

Correct Answer: A