CS0-001 Q&As

CompTIA Cybersecurity Analyst

Pass CompTIA CS0-001 Exam with 100% Guarantee

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

https://www.passapply.com/cs0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A security analyst is performing a forensic analysis on a machine that was the subject of some historic SIEM alerts. The analyst noticed some network connections utilizing SSL on non-common ports, copies of svchost.exe and cmd.exe in %TEMP% folder, and RDP files that had connected to external IPs. Which of the following threats has the security analyst uncovered?

A. DDoS

B. APT

C. Ransomware

D. Software vulnerability

Correct Answer: B

QUESTION 2

A security analyst is performing ongoing scanning and continuous monitoring of the corporate datacenter. Over time, these scans are repeatedly showing susceptibility to the same vulnerabilities and an increase in new vulnerabilities on a specific group of servers that are clustered to run the same application. Which of the following vulnerability management processes should be implemented?

A. Frequent server scanning

B. Automated report generation

C. Group policy modification

D. Regular patch application

Correct Answer: D

QUESTION 3

During the forensic a phase of a security investigation, it was discovered that an attacker was able to find private keys on a poorly secured team shared drive. The attacker used those keys to intercept and decrypt sensitive traffic on a web server. Which of the following describes this type of exploit and the potential remediation?

A. Session hijacking; network intrusion detection sensors

B. Cross-site scripting; increased encryption key sizes

C. Man-in-the-middle; well-controlled storage of private keys

D. Rootkit; controlled storage of public keys

Correct Answer: C

QUESTION 4

Which of the following has the GREATEST impact to the data retention policies of an organization?

A. The CIA classification matrix assigned to each piece of data

B. The level of sensitivity of the data established by the data owner

C. The regulatory requirements concerning the data set

D. The technical constraints of the technology used to store the data

Correct Answer: D

QUESTION 5

A security analyst has noticed an alert from the SIEM. A workstation is repeatedly trying to connect to port 445 of a file server on the production network. All of the attempts are made with invalid credentials. Which of the following describes what is occurring?

A. Malware has infected the workstation and is beaconing out to the specific IP address of the file server.

B. The file server is attempting to transfer malware to the workstation via SMB.

C. An attacker has gained control of the workstation and is attempting to pivot to the file server by creating an SMB session.

D. An attacker has gained control of the workstation and is port scanning the network.

Correct Answer: C

QUESTION 6

A security analyst performs various types of vulnerability scans.

You must review the vulnerability scan results to determine the type of scan that was executed and determine if a false positive occurred for each device.

Instructions:

Select the drop option for whether the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a

second time.

Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results.

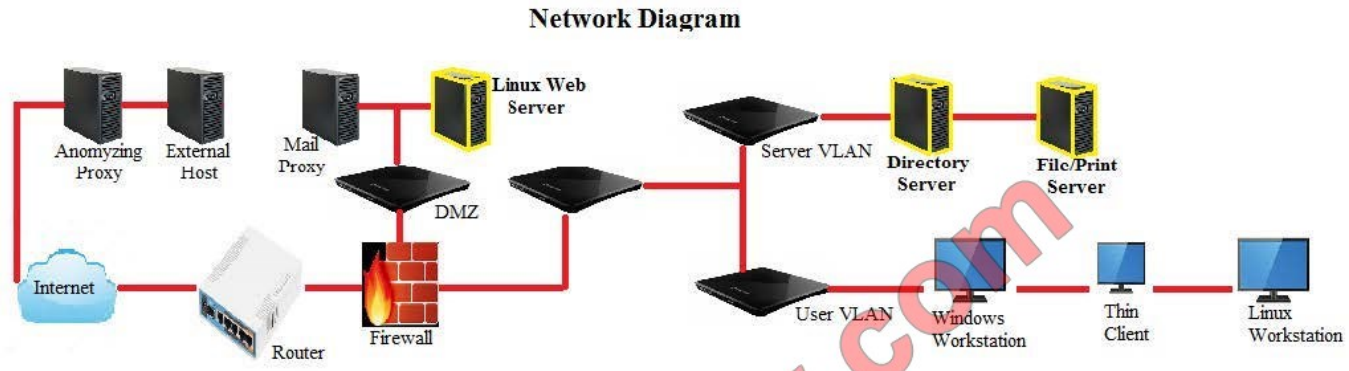
The Linux Web Server, File-Print Server and Directory Server are draggable.

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. Once the simulation is submitted, please select the

Next button to continue.

Hot Area:

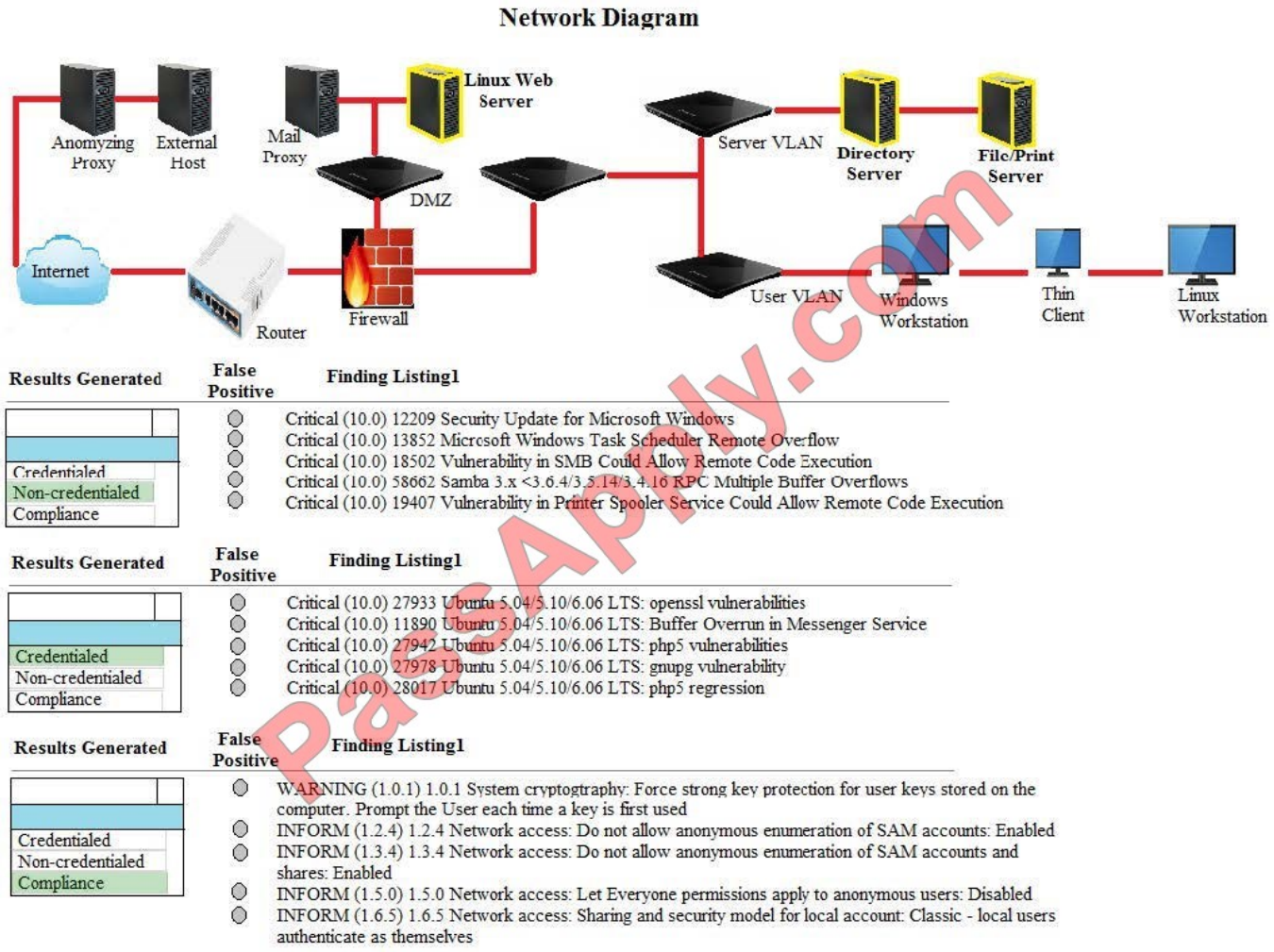


Results Generated	False Positive	Finding Listing1
Credentialed	○	Critical (10.0) 12209 Security Update for Microsoft Windows
Non-credentialed	○	Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow
Compliance	○	Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution
	○	Critical (10.0) 58662 Samba 3.x <3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows
	○	Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution

Results Generated	False Positive	Finding Listing1
Credentialed	○	Critical (10.0) 27933 Ubuntu 5.04/5.10/6.06 LTS: openssl vulnerabilities
Non-credentialed	○	Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS: Buffer Overrun in Messenger Service
Compliance	○	Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS: php5 vulnerabilities
	○	Critical (10.0) 27978 Ubuntu 5.04/5.10/6.06 LTS: gnupg vulnerability
	○	Critical (10.0) 28017 Ubuntu 5.04/5.10/6.06 LTS: php5 regression

Results Generated	False Positive	Finding Listing1
Credentialed	○	WARNING (1.0.1) 1.0.1 System cryptography: Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
Non-credentialed	○	INFORM (1.2.4) 1.2.4 Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
Compliance	○	INFORM (1.3.4) 1.3.4 Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
	○	INFORM (1.5.0) 1.5.0 Network access: Let Everyone permissions apply to anonymous users: Disabled
	○	INFORM (1.6.5) 1.6.5 Network access: Sharing and security model for local account: Classic - local users authenticate as themselves

Correct Answer:



QUESTION 7

Given the following code:

```
<SCRIPT type="text/javascript">
var adr = "../evil.php?breadmonster=" +escape{document.cookie};
var query = "SELECT * FROM users WHERE name='smith';
</SCRIPT>
```

Which of the following types of attacks is occurring?

A. MITM

B. Session hijacking

C. XSS

D. Privilege escalation

E. SQL injection

Correct Answer: E

QUESTION 8

A security operations team was alerted to abnormal DNS activity coming from a user\\'s machine. The team performed a forensic investigation and discovered a host had been compromised. Malicious code was using DNS as a tunnel to extract data from the client machine, which had been leaked and transferred to an unsecure public Internet site. Which of the following BEST describes the attack?

A. Phishing

B. Pharming

C. Cache poisoning

D. Data exfiltration

Correct Answer: D

QUESTION 9

An analyst is reviewing the following log from the company web server:

```
15.34.24 GET /directory/listening.php?user=admin&pass=admin1
15.34.27 GET /directory/listening.php?user=admin&pass=admin2
15.34.29 GET /directory/listening.php?user=admin&pass=1admin
15.34.35 GET /directory/listening.php?user=admin&pass=2admin
```

Which of the following is this an example of?

A. Online rainbow table attack

B. Offline brute force attack

C. Offline dictionary attack

D. Online hybrid attack

Correct Answer: B

QUESTION 10

A security analyst received an alert from the antivirus software identifying a complex instance of malware on a company\\'s network. The company does not have the resources to fully analyze the malware and determine its effect on the system. Which of the following is the BEST action to take in the incident recovery and post-incident response process?

A. Wipe hard drives, reimage the systems, and return the affected systems to ready state.

B. Detect and analyze the precursors and indicators; schedule a lessons learned meeting.

C. Remove the malware and inappropriate materials; eradicate the incident.

D. Perform event correlation; create a log retention policy.

Correct Answer: C

QUESTION 11

A cybersecurity analyst was hired to resolve a security issue within a company after it was reported that many employee account passwords had been compromised. Upon investigating the incident, the cybersecurity analyst found that a brute

force attack was launched against the company.

Which of the following remediation actions should the cybersecurity analyst recommend to senior management to address these security issues?

A. Prohibit password reuse using a GPO.

B. Deploy multifactor authentication.

C. Require security awareness training.

D. Implement DLP solution.

Correct Answer: B

QUESTION 12

After implementing and running an automated patching tool, a security administrator ran a vulnerability scan that reported no missing patches found. Which of the following BEST describes why this tool was used?

A. To create a chain of evidence to demonstrate when the servers were patched.

B. To harden the servers against new attacks.

C. To provide validation that the remediation was active.

D. To generate log data for unreleased patches.

Correct Answer: B