CompTIA CSA+ Certification Exam

CompTIA CS0-001

Version Demo

Total Demo Questions: 20

Total Premium Questions: 416

QUESTION NO: 1

Several accounting department users are reporting unusual Internet traffic in the browsing history of their workstations after returning to work and logging in. The building security team informs the IT security team that the cleaning staff was caught using the systems after the accounting department users left for the day. Which of the following steps should the IT security team take to help prevent this from happening again? (Choose two.)

A. Install a web monitor application to track Internet usage after hours.

B. Configure a policy for workstation account timeout at three minutes.

C. Configure NAC to set time-based restrictions on the accounting group to normal business hours.

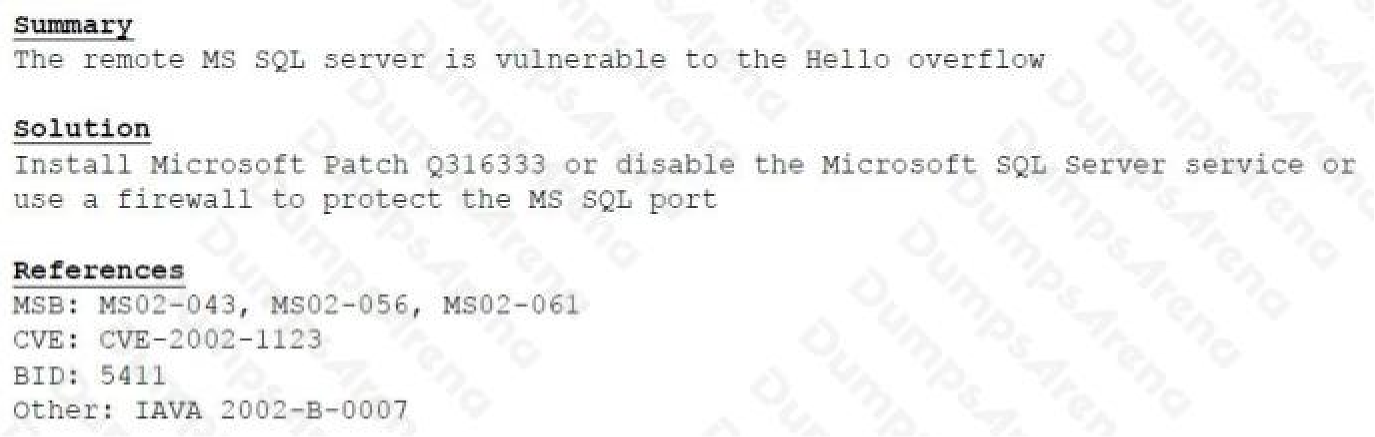
D. Configure mandatory access controls to allow only accounting department users to access the workstations.

E. Set up a camera to monitor the workstations for unauthorized use.

ANSWER: B C

QUESTION NO: 2

A cybersecurity consultant is reviewing the following output from a vulnerability scan against a newly installed MS SQL Server 2012 that is slated to go into production in one week:



```
Summary
The remote MS SQL server is vulnerable to the Hello overflow

Solution
Install Microsoft Patch Q316333 or disable the Microsoft SQL Server service or
use a firewall to protect the MS SQL port

References
MSB: MS02-043, MS02-056, MS02-061
CVE: CVE-2002-1123
BID: 5411
Other: IAVA 2002-B-0007
```

Based on the above information, which of the following should the system administrator do? (Choose two.)

A. Verify the vulnerability using penetration testing tools or proof-of-concept exploits.

B. Review the references to determine if the vulnerability can be remotely exploited.

C. Mark the result as a false positive so it will show in subsequent scans.

D. Configure a network-based ACL at the perimeter firewall to protect the MS SQL port.

E. Implement the proposed solution by installing Microsoft patch Q316333.

ANSWER: D E

QUESTION NO: 3

A security analyst is reviewing output from a CVE-based vulnerability scanner. Before conducting the scan, the analyst was careful to select only Windows-based servers in a specific datacenter. The scan revealed that the datacenter includes 27 machines running Windows 2003 Server Edition (Win2003SE). In 2015, there were 36 new vulnerabilities discovered in the Win2003SE environment. Which of the following statements are MOST likely applicable? (Choose two.)

A. Remediation is likely to require some form of compensating control.

B. Microsoft’s published schedule for updates and patches for Win2003SE have continued uninterrupted.

C. Third-party vendors have addressed all of the necessary updates and patches required by Win2003SE.

D. The resulting report on the vulnerability scan should include some reference that the scan of the datacenter included 27 Win2003SE machines that should be scheduled for replacement and deactivation.

E. Remediation of all Win2003SE machines requires changes to configuration settings and compensating controls to be made through Microsoft Security Center’s Win2003SE Advanced Configuration Toolkit.

ANSWER: D

QUESTION NO: 4

Alerts have been received from the SIEM, indicating infections on multiple computers. Based on threat characteristics, these files were quarantined by the host-based antivirus program. At the same time, additional alerts in the SIEM show multiple blocked URLs from the address of the infected computers; the URLs were classified as uncategorized. The domain location of the IP address of the URLs that were blocked is checked, and it is registered to an ISP in Russia. Which of the following steps should be taken NEXT?

A. Remove those computers from the network and replace the hard drives. Send the infected hard drives out for investigation.

B. Run a full antivirus scan on all computers and use Splunk to search for any suspicious activity that happened just before the alerts were received in the SIEM.

C. Run a vulnerability scan and patch discovered vulnerabilities on the next pathing cycle. Have the users restart their computers. Create a use case in the SIEM to monitor failed logins on the infected computers.

D. Install a computer with the same settings as the infected computers in the DMZ to use as a honeypot. Permit the URLs classified as uncategorized to and from that host.

ANSWER: B

QUESTION NO: 5

A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website.

During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

A. Transitive access

B. Spoofing

C. Man-in-the-middle

D. Replay

ANSWER: C

QUESTION NO: 6

An administrator has been investigating the way in which an actor had been exfiltrating confidential data from a web server to a foreign host. After a thorough forensic review, the administrator determined the server's BIOS had been modified by rootkit installation. After removing the rootkit and flashing the BIOS to a known good state, which of the following would BEST protect against future adversary access to the BIOS, in case another rootkit is installed?

A. Anti-malware application

B. Host-based IDS

C. TPM data sealing

D. File integrity monitoring

ANSWER: C

QUESTION NO: 7

After an internal audit, it was determined that administrative logins need to use multifactor authentication or a 15-character key with complexity enabled. Which of the following policies should be updates to reflect this change? (Choose two.)

A. Data ownership policy

B. Password policy

C. Data classification policy

D. Data retention policy

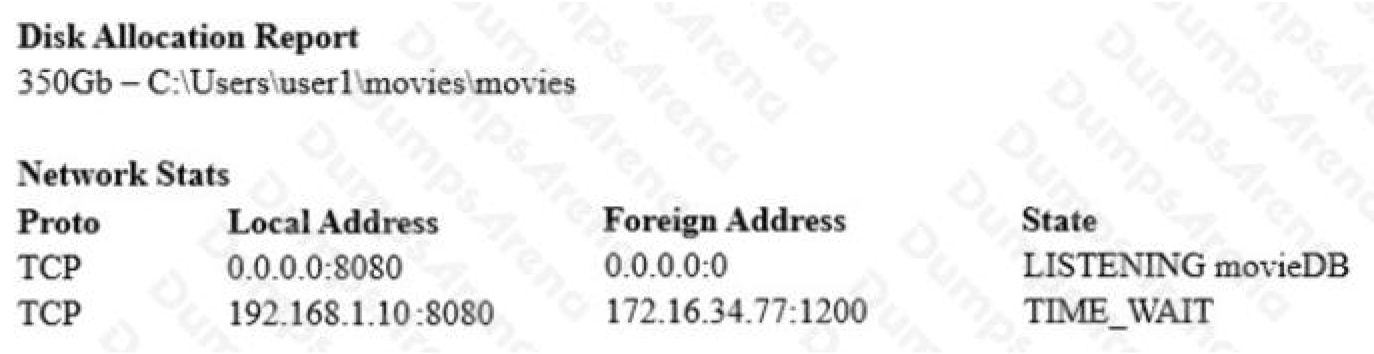
E. Acceptable use policy

F. Account management policy

ANSWER: B F

QUESTION NO: 8

A technician is troubleshooting a desktop computer with low disk space. The technician reviews the following information snippets:



Disk Allocation Report

350Gb – C:\Users\user1\movies\movies

Network Stats

```
Proto     Local Address         Foreign Address       State
TCP       0.0.0.0:8080          0.0.0.0:0             LISTENING movieDB
TCP       192.168.1.10:8080     172.16.34.77:1200     TIME_WAIT
```

Which of the following should the technician do to BEST resolve the issue based on the above information? (Choose two.)

A. Delete the movies/movies directory

B. Disable the movieDB service

C. Enable OS auto updates

D. Install a file integrity tool

E. Defragment the disk

ANSWER: B E

QUESTION NO: 9

A technician recently fixed a computer with several viruses and spyware programs on it and notices the Internet settings were set to redirect all traffic through an unknown proxy. This type of attack is known as which of the following?

A. Phishing

B. Social engineering

C. Man-in-the-middle

D. Shoulder surfing

ANSWER: C

QUESTION NO: 10

There have been several exploits to critical devices within the network. However, there is currently no process to perform vulnerability analysis.

Which of the following should the security analyst implement during production hours to identify critical threats and vulnerabilities?

A. Asset inventory of all critical devices

B. Vulnerability scanning frequency that does not interrupt workflow

C. Daily automated reports of exploited devices

D. Scanning of all types of data regardless of sensitivity levels

ANSWER: B

QUESTION NO: 11

Malicious users utilized brute force to access a system. An analyst is investigating these attacks and recommends methods to management that would help secure the system. Which of the following controls should the analyst recommend? (Choose three.)

A. Multifactor authentication

B. Network segmentation

C. Single sign-on

D. Encryption

E. Complexity policy

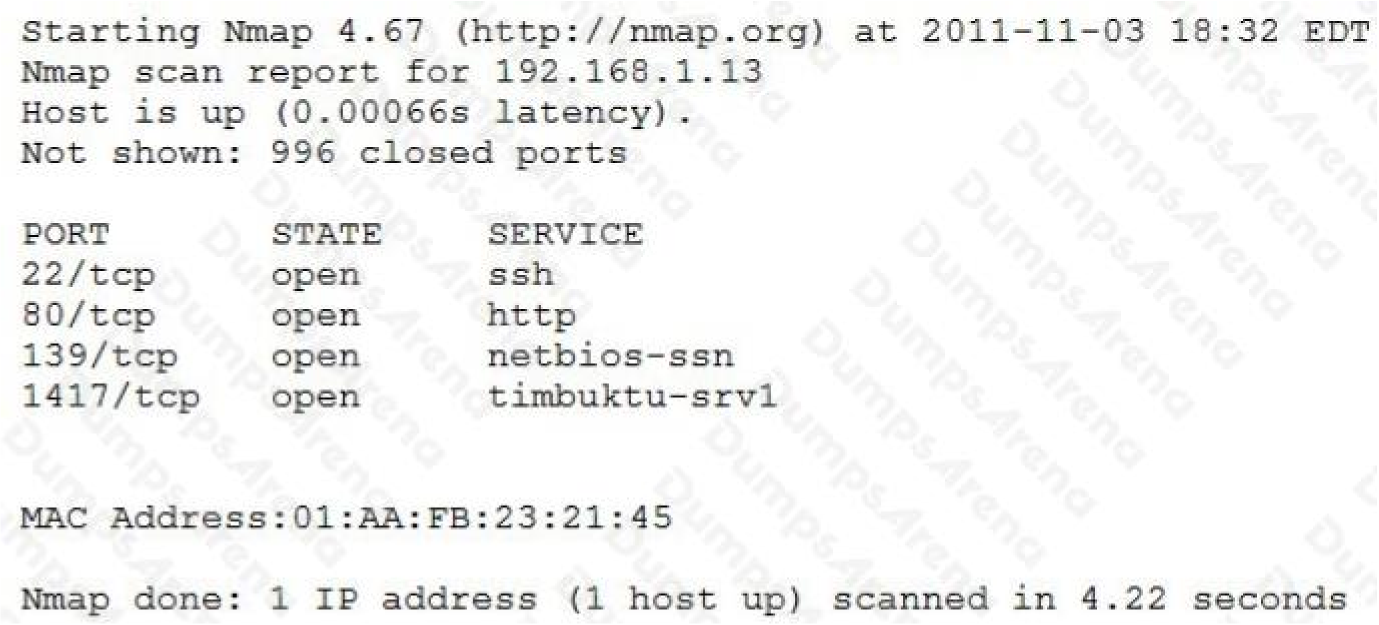
F. Biometrics

G. Obfuscation

ANSWER: A E F

QUESTION NO: 12

An organization is conducting penetration testing to identify possible network vulnerabilities. The penetration tester has received the following output from the latest scan:



```
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: 996 closed ports

PORT        STATE      SERVICE
22/tcp      open       ssh
80/tcp      open       http
139/tcp     open       netbios-ssn
1417/tcp    open       timbuktu-srv1


MAC Address:01:AA:FB:23:21:45

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

The penetration tester knows the organization does not use Timbuktu servers and wants to have Nmap interrogate the ports on the target in more detail. Which of the following commands should the penetration tester use NEXT?

A. nmap –sV 192.168.1.13 –p1417

B. nmap –sS 192.168.1.13 –p1417

C. sudo nmap –sS 192.168.1.13

D. nmap 192.168.1.13 –v

ANSWER: A

QUESTION NO: 13

Various devices are connecting and authenticating to a single evil twin within the network. Which of the following are MOST likely being targeted?

A. Mobile devices

B. All endpoints

C. VPNs

D. Network infrastructure

E. Wired SCADA devices

ANSWER: A

QUESTION NO: 14

A software assurance lab is performing a dynamic assessment on an application by automatically generating and inputting different, random data sets to attempt to cause an error/failure condition. Which of the following software assessment capabilities is the lab performing AND during which phase of the SDLC should this occur? (Choose two.)

A. Fuzzing

B. Behavior modeling

C. Static code analysis

D. Prototyping phase

E. Requirements phase

F. Planning phase

ANSWER: A D

Explanation:

Reference: http://www.brighthub.com/computing/smb-security/articles/9956.aspx

QUESTION NO: 15

A security analyst is concerned that employees may attempt to exfiltrate data prior to tendering their resignations. Unfortunately, the company cannot afford to purchase a data loss prevention system. Which of the following recommendations should the security analyst make to provide defense-in-depth against data loss? (Choose three.)

A. Prevent users from accessing personal email and file-sharing sites via web proxy

B. Prevent flash drives from connecting to USB ports using Group Policy

C. Prevent users from copying data from workstation to workstation

D. Prevent users from using roaming profiles when changing workstations

E. Prevent Internet access on laptops unless connected to the network in the office or via VPN

F. Prevent users from being able to use the copy and paste functions

ANSWER: A B E

QUESTION NO: 16

A business-critical application is unable to support the requirements in the current password policy because it does not allow the use of special characters. Management does not want to accept the risk of a possible security incident due to weak password standards. Which of the following is an appropriate means to limit the risks related to the application?

A. A compensating control

B. Altering the password policy

C. Creating new account management procedures

D. Encrypting authentication traffic

ANSWER: D

QUESTION NO: 17 - (HOTSPOT)

HOTSPOT

A security analyst performs various types of vulnerability scans.

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

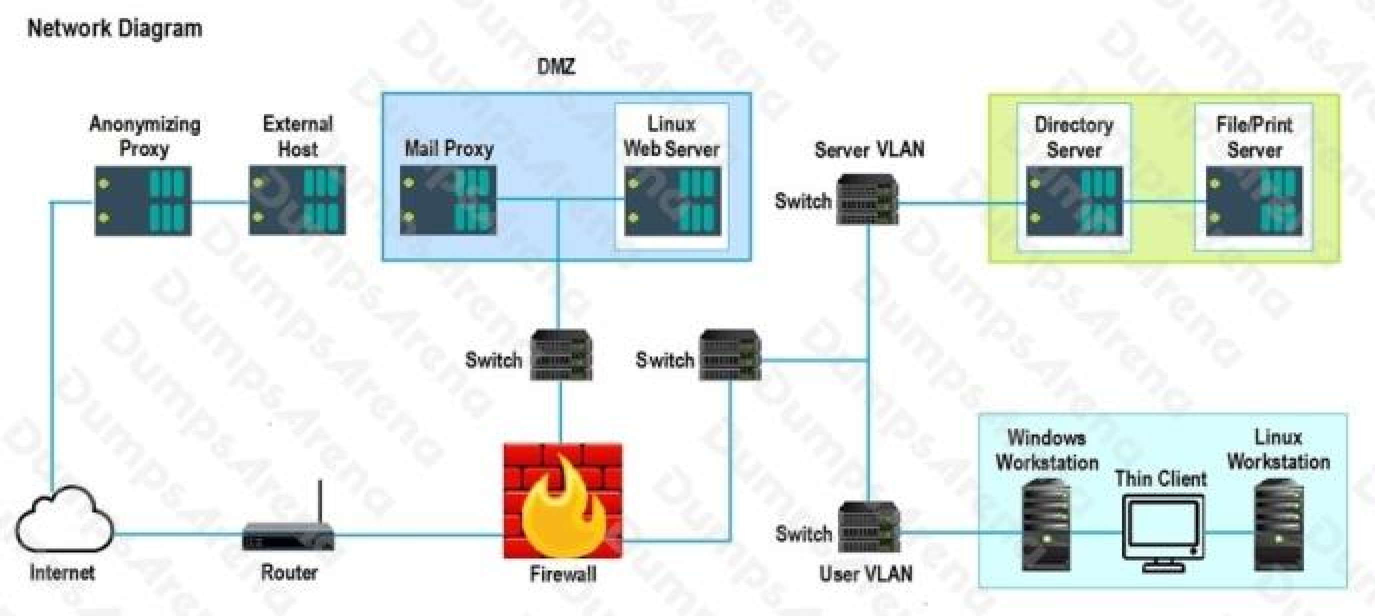
Instructions:

Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.

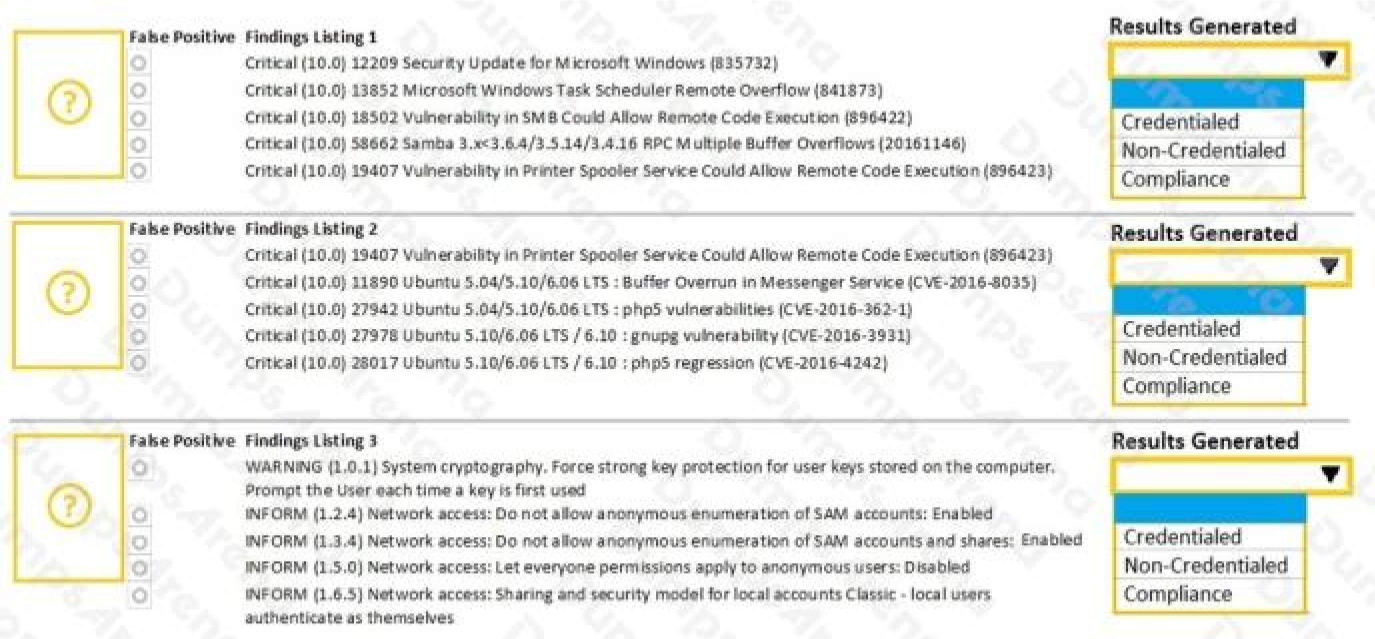
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.

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 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.



Hot Area:



False Positive Findings Listing 1

○ Critical (10.0) 12209 Security Update for Microsoft Windows (835732)
○ Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
○ Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
○ Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated ▼
- Credentialed
- Non-Credentialed
- Compliance

False Positive Findings Listing 2

○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
○ Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)
○ Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
○ Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)
○ Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

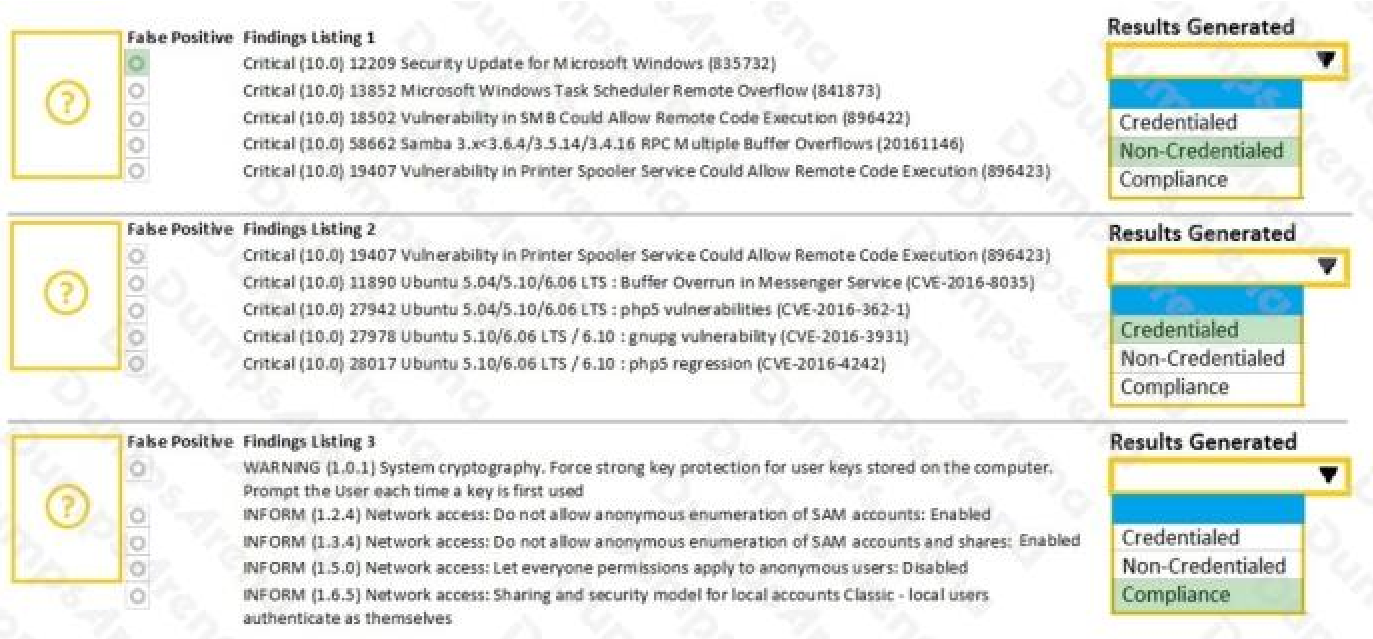
Results Generated ▼
- Credentialed
- Non-Credentialed
- Compliance

False Positive Findings Listing 3

○ WARNING (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
○ INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
○ INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
○ INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled
○ INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

Results Generated ▼
- Credentialed
- Non-Credentialed
- Compliance

ANSWER:



False Positive Findings Listing 1

● Critical (10.0) 12209 Security Update for Microsoft Windows (835732)
○ Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
○ Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
○ Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated: Credentialed [✓ Non-Credentialed] Compliance

False Positive Findings Listing 2

○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
○ Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)
○ Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
○ Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)
○ Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

Results Generated: [✓ Credentialed] Non-Credentialed Compliance

False Positive Findings Listing 3

○ WARNING (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
○ INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
○ INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
○ INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled
○ INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

Results Generated: Credentialed Non-Credentialed [✓ Compliance]

Explanation:

1. non-credentialed scan - File Print Server: False positive is first bullet point.

2. credentialed scan – Linux Web Server: No False positives.

3. Compliance scan - Directory Server

QUESTION NO: 18

Which of the following are essential components within the rules of engagement for a penetration test? (Choose two.)

A. Schedule

B. Authorization

C. List of system administrators

D. Payment terms

E. Business justification

ANSWER: A B

QUESTION NO: 19

A security administrator determines several months after the first instance that a local privileged user has been routinely logging into a server interactively as “root” and browsing the Internet. The administrator determines this by performing an annual review of the security logs on that server. For which of the following security architecture areas should the administrator recommend review and modification? (Choose two.)

A. Log aggregation and analysis

B. Software assurance

C. Encryption

D. Acceptable use policies

E. Password complexity

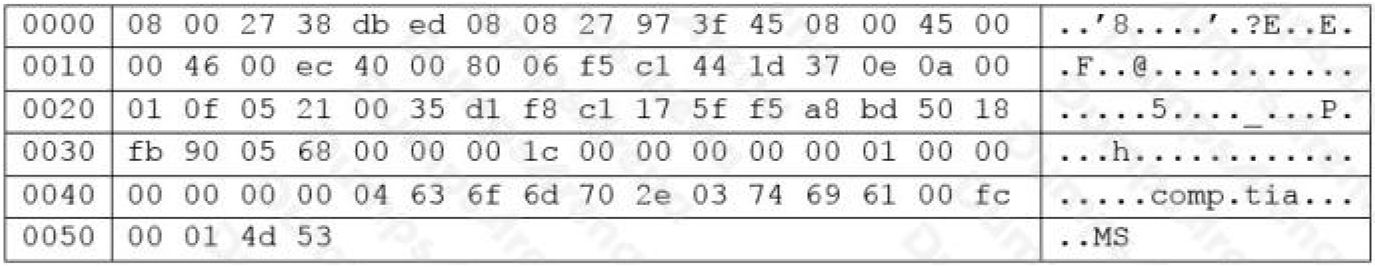
F. Network isolation and separation

ANSWER: A D

QUESTION NO: 20

A security analyst is reviewing packet captures to determine the extent of success during an attacker’s reconnaissance phase following a recent incident.

The following is a hex and ASCII dump of one such packet:



```
0000  08 00 27 38 db ed 08 08 27 97 3f 45 08 00 45 00   ..'8....'.?E..E.
0010  00 46 00 ec 40 00 80 06 f5 c1 44 1d 37 0e 0a 00   .F..@...........
0020  01 0f 05 21 00 35 d1 f8 c1 17 5f f5 a8 bd 50 18   .....5...._...P.
0030  fb 90 05 68 00 00 00 1c 00 00 00 00 00 01 00 00   ...h............
0040  00 00 00 00 04 63 6f 6d 70 2e 03 74 69 61 00 fc   .....comp.tia...
0050  00 01 4d 53                                       ..MS
```

Which of the following BEST describes this packet?

A. DNS BIND version request

B. DNS over UDP standard query

C. DNS over TCP server status query

D. DNS zone transfer request

ANSWER: A