

## PT0-001 Dumps

### CompTIA PenTest+ Certification Exam

<https://www.certleader.com/PT0-001-dumps.html>



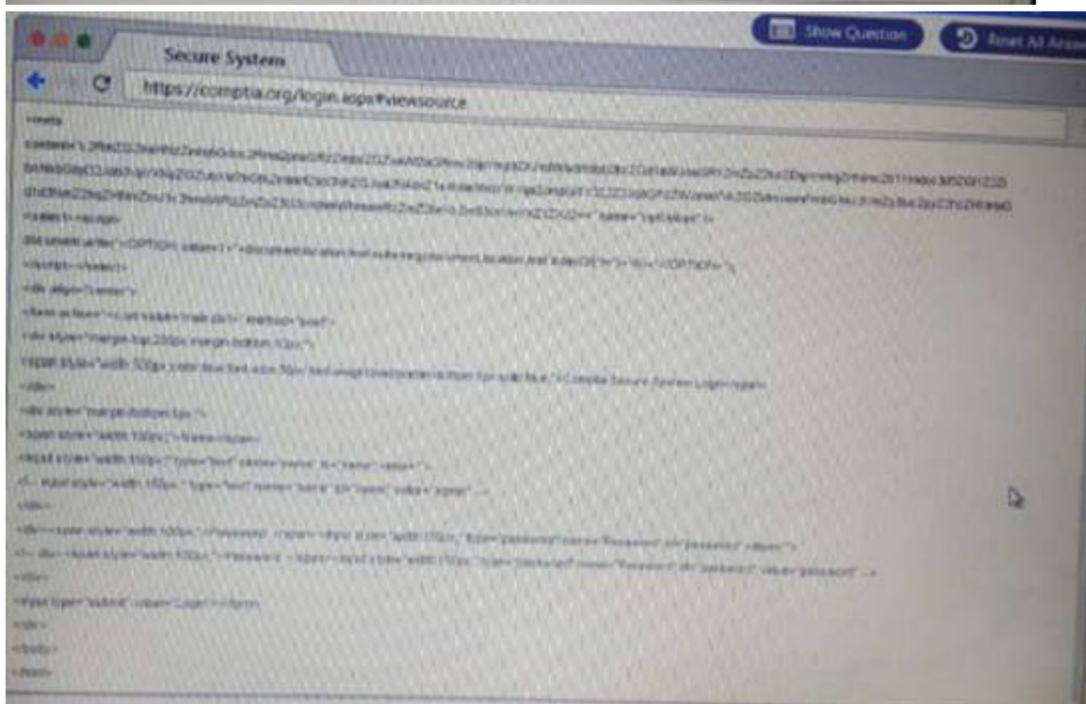
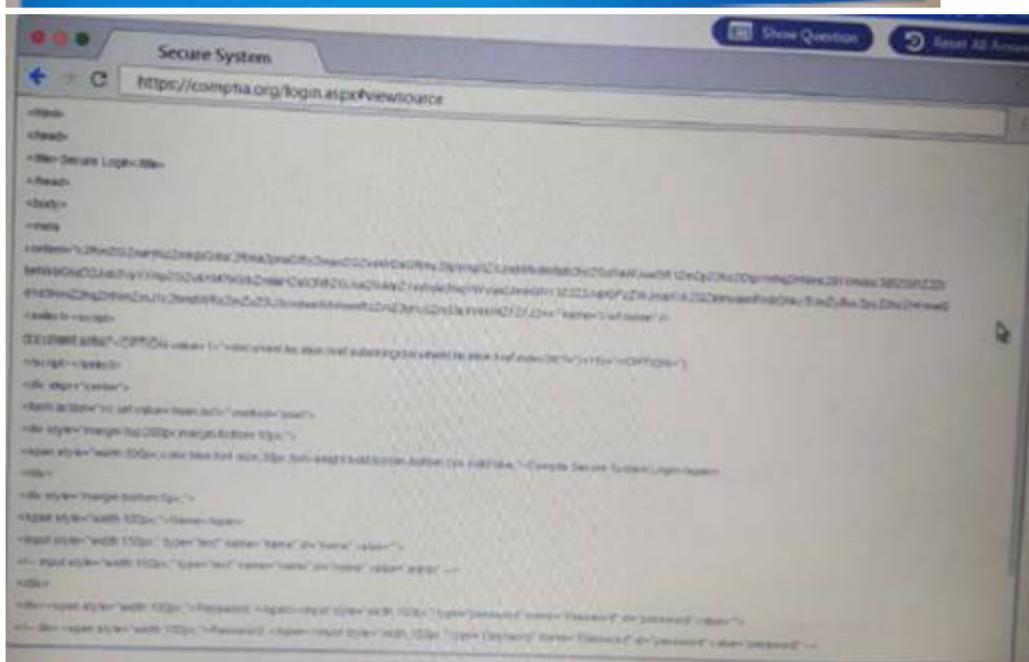
**NEW QUESTION 1**

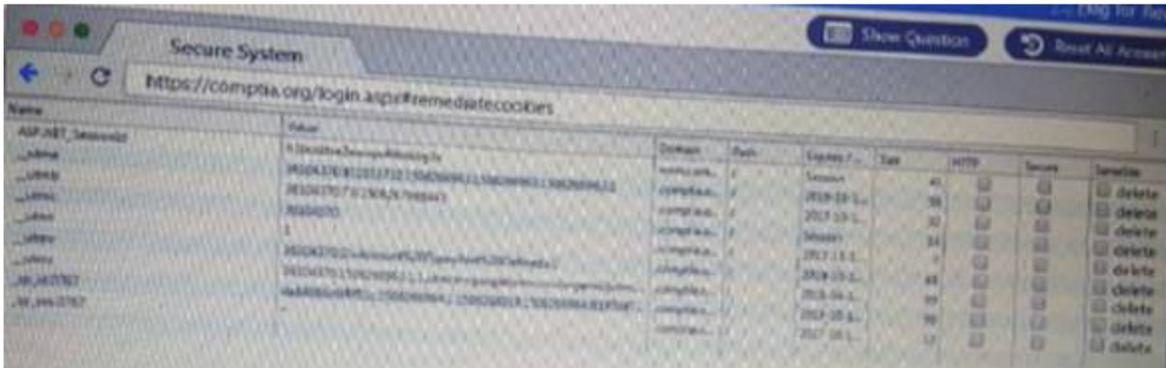
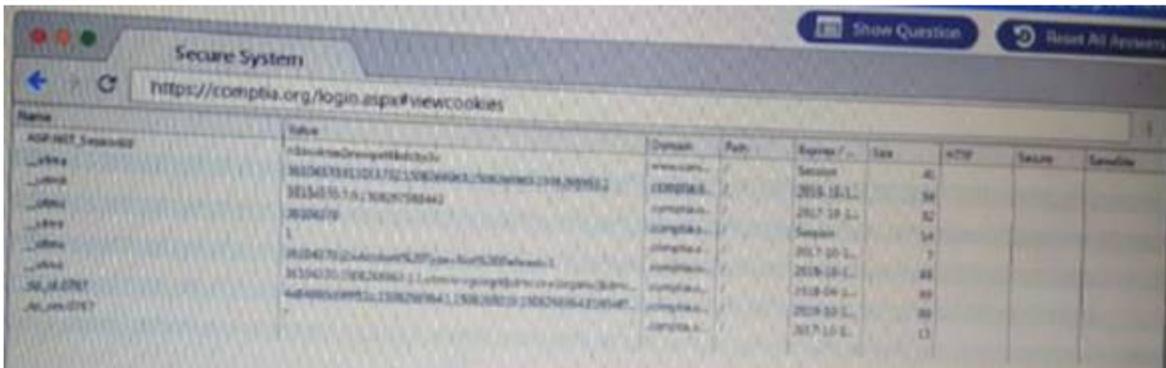
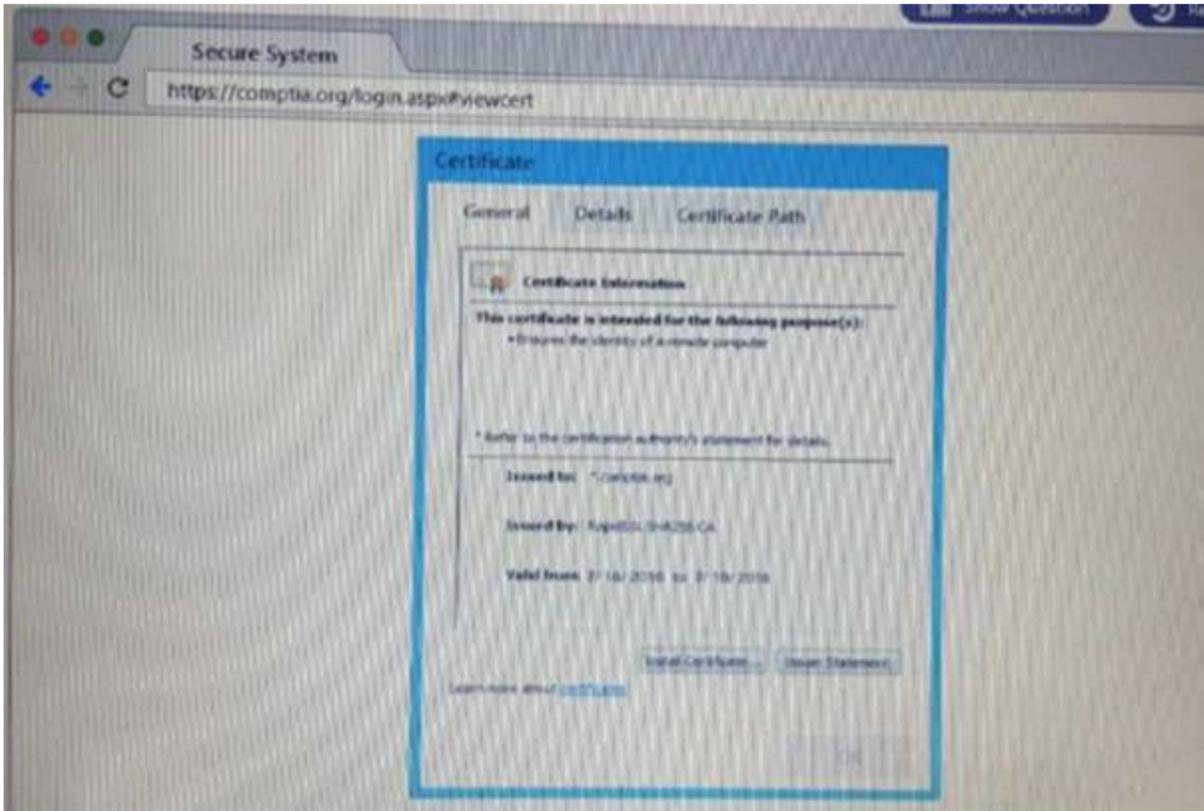
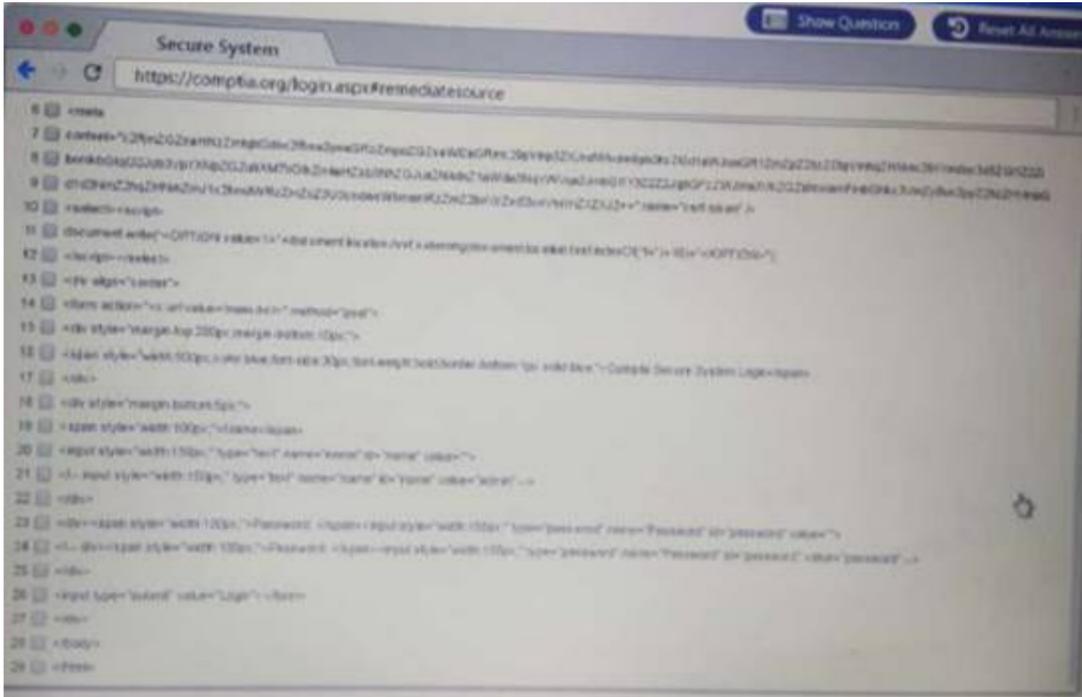
DRAG DROP

Performance based

You are a penetration Inter reviewing a client's website through a web browser. Instructions:

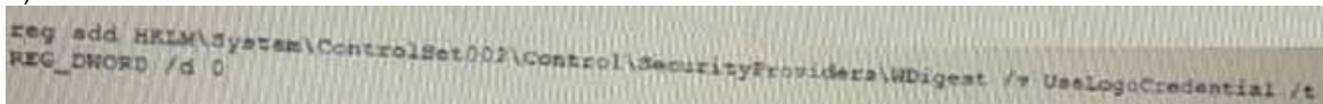
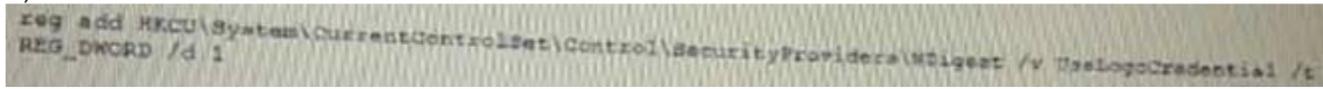
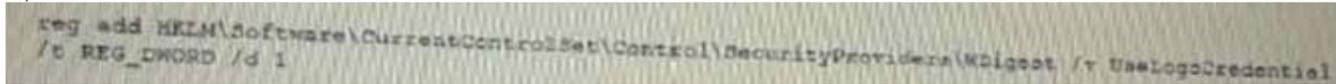
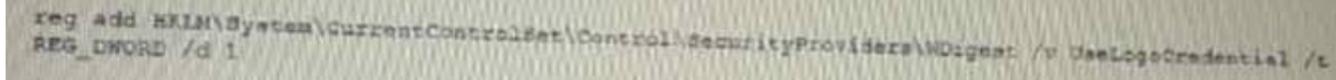
Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate source or cookies.







credential harvesting with Mimikatz. Which of the following registry changes would allow for credential caching in memory?

- A) 
- B) 
- C) 
- D) 

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: D**

**NEW QUESTION 5**

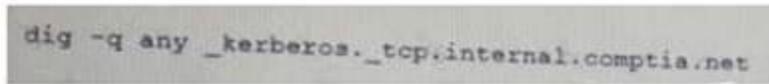
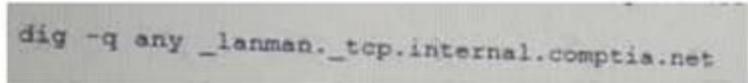
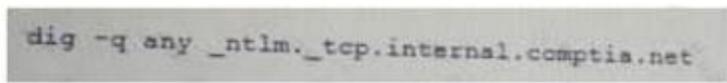
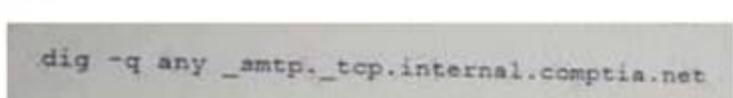
A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack Which of the following remediation steps should be recommended? (Select THREE)

- A. Mandate all employees take security awareness training
- B. Implement two-factor authentication for remote access
- C. Install an intrusion prevention system
- D. Increase password complexity requirements
- E. Install a security information event monitoring solution.
- F. Prevent members of the IT department from interactively logging in as administrators
- G. Upgrade the cipher suite used for the VPN solution

**Answer: BDG**

**NEW QUESTION 6**

An assessor begins an internal security test of the Windows domain internal.comptia.net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

- A) 
- B) 
- C) 
- D) 

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: A**

**NEW QUESTION 7**

After several attempts, an attacker was able to gain unauthorized access through a biometric sensor using the attacker's actual fingerprint without exploitation. Which of the following is the MOST likely explanation of what happened?

- A. The biometric device is tuned more toward false positives
- B. The biometric device is configured more toward true negatives
- C. The biometric device is set to fail closed
- D. The biometric device duplicated a valid user's fingerprint

**Answer:** A

**NEW QUESTION 8**

The results of a basic compliance scan show a subset of assets on a network. This data differs from what is shown on the network architecture diagram, which was supplied at the beginning of the test. Which of the following are the MOST likely causes for this difference? (Select TWO)

- A. Storage access
- B. Limited network access
- C. Misconfigured DHCP server
- D. Incorrect credentials
- E. Network access controls

**Answer:** A

**NEW QUESTION 9**

A penetration tester has successfully exploited an application vulnerability and wants to remove the command history from the Linux session. Which of the following will accomplish this successfully?

- A. `history --remove`
- B. `cat history | clear`
- C. `rm -f ./history`
- D. `history -c`

**Answer:** D

**NEW QUESTION 10**

When performing compliance-based assessments, which of the following is the MOST important Key consideration?

- A. Additional rate
- B. Company policy
- C. Impact tolerance
- D. Industry type

**Answer:** A

**NEW QUESTION 10**

A penetration tester notices that the X-Frame-Options header on a web application is not set. Which of the following would a malicious actor do to exploit this configuration setting?

- A. Use path modification to escape the application's framework.
- B. Create a frame that overlays the application.
- C. Inject a malicious iframe containing JavaScript.
- D. Pass an iframe attribute that is malicious

**Answer:** B

**NEW QUESTION 15**

A penetration tester is required to perform OSINT on staff at a target company after completing the infrastructure aspect. Which of the following would be the BEST step for the penetration tester to take?

- A. Obtain staff information by calling the company and using social engineering techniques.
- B. Visit the client and use impersonation to obtain information from staff.
- C. Send spoofed emails to staff to see if staff will respond with sensitive information.
- D. Search the Internet for information on staff such as social networking site

**Answer:** C

**NEW QUESTION 16**

Which of the following is the reason why a penetration tester would run the `chkconfig --del servicename` command at the end of an engagement?

- A. To remove the persistence
- B. To enable persistence
- C. To report persistence
- D. To check for persistence

**Answer:** A

**NEW QUESTION 21**

A penetration tester is checking a script to determine why some basic persisting. The expected result was the program outputting "True."

```

root:~# cat ./test.sh
#!/bin/bash
source=10
let dest=5+5

if [ 'source' = 'dest' ]; then
    echo "True"
else
    echo "False"
fi
#End of File
root:~# ./test.sh
False
    
```

Given the output from the console above, which of the following explains how to correct the errors in the script? (Select TWO)

- A. Change 'fi' to 'Endlf'
- B. Remove the 'let' in front of 'dest=5+5'.
- C. Change the '=' to '-eq'.
- D. Change 'source' and 'dest' to "Ssource" and "Sdest"
- E. Change 'else' to 'eli'

**Answer:** BC

**NEW QUESTION 25**

A penetration tester runs the following from a compromised box 'python -c -import pty;Pty.sPawn( "/bin/bash").' Which of the following actions is the tester taking?

- A. Removing the Bash history
- B. Upgrading the shell
- C. Creating a sandbox
- D. Capturing credentials

**Answer:** A

**NEW QUESTION 30**

During an internal network penetration test, a tester recovers the NTLM password hash for a user known to have full administrator privileges on a number of target systems. Efforts to crack the hash and recover the plaintext password have been unsuccessful. Which of the following would be the BEST target for continued exploitation efforts?

- A. Operating system Windows 7 Open ports: 23, 161
- B. Operating system Windows Server 2016 Open ports: 53, 5900
- C. Operating system Windows 8 1 Open ports 445, 3389
- D. Operating system Windows 8 Open ports 514, 3389

**Answer:** C

**NEW QUESTION 32**

A client requests that a penetration tester emulate a help desk technician who was recently laid off. Which of the following BEST describes the abilities of the threat actor?

- A. Advanced persistent threat
- B. Script kiddie
- C. Hactivist
- D. Organized crime

**Answer:** A

**NEW QUESTION 36**

Which of the following types of physical security attacks does a mantrap mitigate-?

- A. Lock picking
- B. Impersonation
- C. Shoulder surfing
- D. Tailgating

**Answer:** D

**NEW QUESTION 41**

Which of the following reasons does penetration tester needs to have a customer's point-of -contact information available at all time? (Select THREE).

- A. To report indicators of compromise
- B. To report findings that cannot be exploited
- C. To report critical findings
- D. To report the latest published exploits
- E. To update payment information
- F. To report a server that becomes unresponsive
- G. To update the statement of work
- H. To report a cracked password

**Answer:** DEF

**NEW QUESTION 43**

While engaging clients for a penetration test from highly regulated industries, which of the following is usually the MOST important to the clients from a business perspective?

- A. Letter of engagement and attestation of findings
- B. NDA and MSA
- C. SOW and final report
- D. Risk summary and executive summary

**Answer:** D

**NEW QUESTION 44**

During an internal penetration test, several multicast and broadcast name resolution requests are observed traversing the network. Which of the following tools could be used to impersonate network resources and collect authentication requests?

- A. Ettercap
- B. Tcpdump
- C. Responder
- D. Medusa

**Answer:** D

**NEW QUESTION 47**

A penetration tester is performing a remote scan to determine if the server farm is compliant with the company's software baseline . Which of the following should the penetration tester perform to verify compliance with the baseline?

- A. Discovery scan
- B. Stealth scan
- C. Full scan
- D. Credentialed scan

**Answer:** A

**NEW QUESTION 49**

A penetration tester is utilizing social media to gather information about employees at a company. The tester has created a list of popular words used in employee profiles. For which of the following types of attack would this information be used?

- A. Exploit chaining
- B. Session hijacking
- C. Dictionary
- D. Karma

**Answer:** B

**NEW QUESTION 50**

A client has voiced concern about the number of companies being branched by remote attackers, who are looking for trade secrets. Which of following BEST describes the types of adversaries this would identify?

- A. Script kiddies
- B. APT actors
- C. Insider threats
- D. Hacktivist groups

**Answer:** B

**NEW QUESTION 52**

Which of the following commands would allow a penetration tester to access a private network from the Internet in Metasploit?

- A. set rhost 192.168.1.10
- B. run autoroute -a 192.168.1.0/24
- C. db\_nm«p -iL /tmp/privatehoots . txt
- D. use auxiliary/servlet/aocka^a

**Answer:** D

**NEW QUESTION 53**

A tester has captured a NetNTLMv2 hash using Responder Which of the following commands will allow the tester to crack the hash using a mask attack?

- A. hashcat -m 5600 -r rulea/beat64.rule hash.txt wordliat.txt
- B. hashcax -m 5€00 hash.txt
- C. hashc&t -m 5600 -a 3 haah.txt ?a?a?a?a?a?a?a
- D. hashcat -m 5600 -o reaulta.txt hash.txt wordliat.txt

**Answer:** A

**NEW QUESTION 58**

A tester has determined that null sessions are enabled on a domain controller. Which of the following attacks can be performed to leverage this vulnerability?

- A. RID cycling to enumerate users and groups
- B. Pass the hash to relay credentials
- C. Password brute forcing to log into the host
- D. Session hijacking to impersonate a system account

**Answer:** C

**NEW QUESTION 60**

In a physical penetration testing scenario, the penetration tester obtains physical access to a laptop following .s a potential NEXT step to extract credentials from the device?

- A. Brute force the user's password.
- B. Perform an ARP spoofing attack.
- C. Leverage the BeEF framework to capture credentials.
- D. Conduct LLMNR/NETBIOS-ns poisonin

**Answer:** D

**NEW QUESTION 65**

A penetration tester is perform initial intelligence gathering on some remote hosts prior to conducting a vulnerability < The tester runs the following command  
nmap -D 192.168.1.1,192.168.1.2,192.168.1.3 -sV -o —max rate 2 192. 168.130  
Which of the following BEST describes why multiple IP addresses are specified?

- A. The network is submitted as a /25 or greater and the tester needed to access hosts on two different subnets
- B. The tester is trying to perform a more stealthy scan by including several bogus addresses
- C. The scanning machine has several interfaces to balance the scan request across at the specified rate
- D. A discovery scan is run on the first set of addresses, whereas a deeper, more aggressive scan is run against the latter host.

**Answer:** C

**NEW QUESTION 66**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your PT0-001 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/PT0-001-dumps.html>