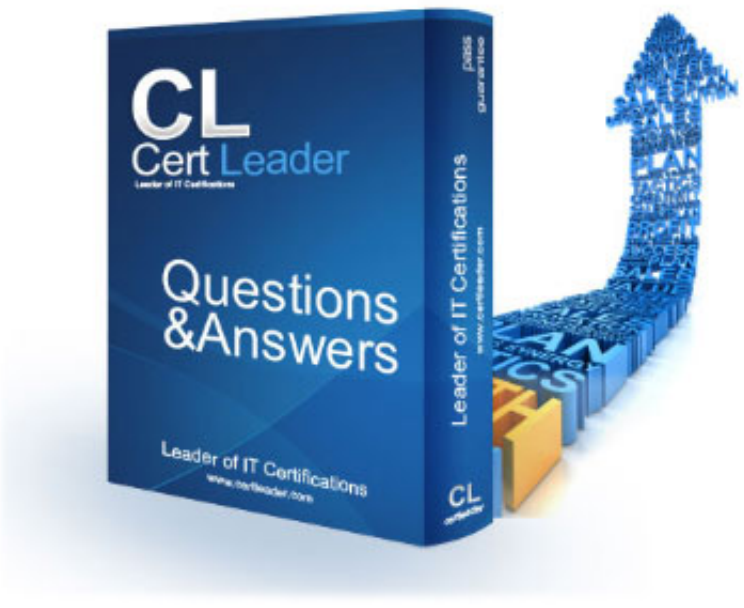
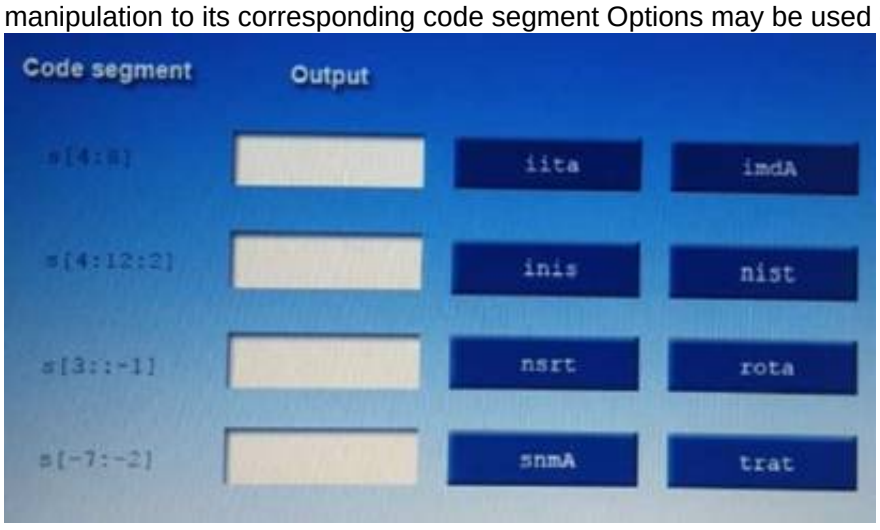
PT0-001 Dumps

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
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 3
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\CcontrolSet002\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 4
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 5
After several attempts, an attacker was able to gain unauthorized access through a biometric sensor using the attacker's actual fingerprint without explogtation. 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 biometnc device duplicated a valid user's fingerpnn

Answer: A

NEW QUESTION 6
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 7
A penetration tester has successfully explogted 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 I clear
C. rm -f ./history
D. history -c

Answer: D

NEW QUESTION 8
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 9
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
A penetration tester notices that the X-Frame-Optjons header on a web application is not set. Which of the following would a malicious actor do to explogt 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 maliciou

Answer: B

NEW QUESTION 10
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 13
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 16
A recently concluded penetration test revealed that a legacy web application is vulnerable lo SQL injection Research indicates that completely remediating the vulnerability would require an architectural change, and the stakeholders are not m a position to risk the availability of the application Under such circumstances, which of the following controls are low-effort, short-term solutions to minimize the SQL injection risk? (Select TWO).

A. Identify and eliminate inline SQL statements from the code.
B. Identify and eliminate dynamic SQL from stored procedures.
C. Identify and sanitize all user inputs.
D. Use a whitelist approach for SQL statements.
E. Use a blacklist approach for SQL statements.
F. Identify the source of malicious input and block the IP addres

Answer: DE

NEW QUESTION 20
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 21
Given the following script:

```
import pyHook, pythoncom, logging, sys

f="f.txt"
def OnKeyboardEvent(event):
        logging.basicConfig(filename=f,level=loggin.DEBUG,format='%(message)')
        chr(event.Ascii)
        logging.log(10,chr(event.Ascii))
        return True

hm = pyHook.HookManager()
hm.KeyDown=OnKeyboardEvent
hm.HookKeyboard()
pythoncom.PumpMessages()
```

Which of the following BEST describes the purpose of this script?

A. Log collection
B. Event logging
C. Keystroke monitoring
D. Debug message collection

Answer: C

NEW QUESTION 25
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 29
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 33
During an internal network penetration test, a tester recovers the NTLM password hash tor 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 explogtation 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 1Open ports 445, 3389
D. Operating system Windows 8 Open ports 514, 3389

Answer: C

NEW QUESTION 36
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. Hacktivist
D. Organized crime

Answer: A

NEW QUESTION 38
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 43
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 44
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 explogted
C. To report critical findings
D. To report the latest published explogts
E. To update payment information
F. To report a server that becomes unresponsive
G. To update the statement o(work
H. To report a cracked password

Answer: DEF

NEW QUESTION 45
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 48
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 53
Which of the following CPU register does the penetration tester need to overwrite in order to explogt a simple butter overflow?

A. Stack pointer register
B. Index pointer register
C. Stack base pointer
D. Destination index register

Answer: D

NEW QUESTION 57
A penetration test was performed by an on-staff technicians junior technician. During the test, the technician discovered the application could disclose an SQL table with user account and password information. Which of the following is the MOST effective way to notify management of this finding and its importance?

A. Document Ihe findtngs with an executive summary, recommendations, and screenshots of the web apphcation disclosure.
B. Connect to the SQL server using this information and change the password to one or two noncritical accounts to demonstrate a proof-of-concept to management.
C. Notify the development team of the discovery and suggest that input validation be implementedon the web application's SQL query strings.
D. Request that management create an RFP to begin a formal engagement with a professional penetration testing company.

Answer: B

NEW QUESTION 62
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

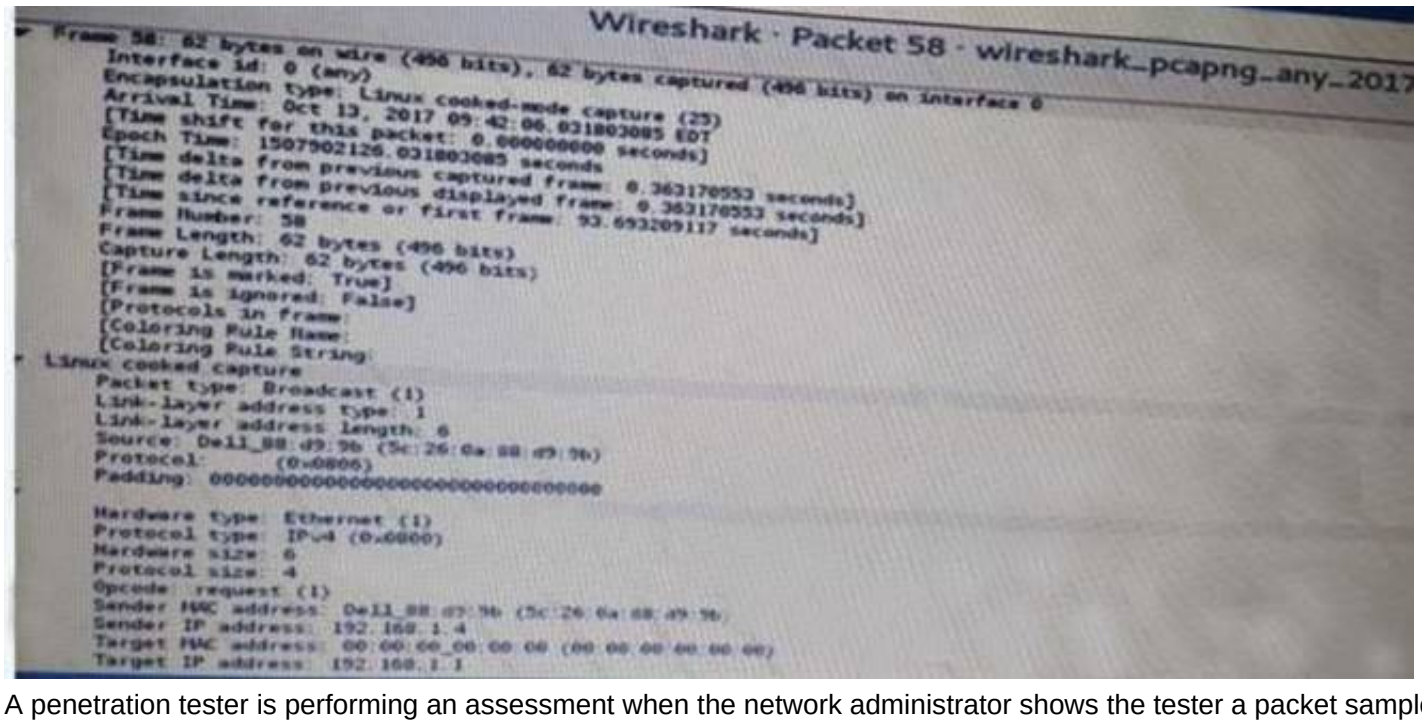
Answer: C

NEW QUESTION 63
A penetration tester has been asked to conduct OS fingerprinting with Nmap using a companyprovide text file that contain a list of IP addresses.
Which of the following are needed to conduct this scan? (Select TWO).

A. -O
B. _iL
C. _sV
D. -sS
E. -oN
F. -oX

Answer: EF

NEW QUESTION 64
Click the exhibit button.



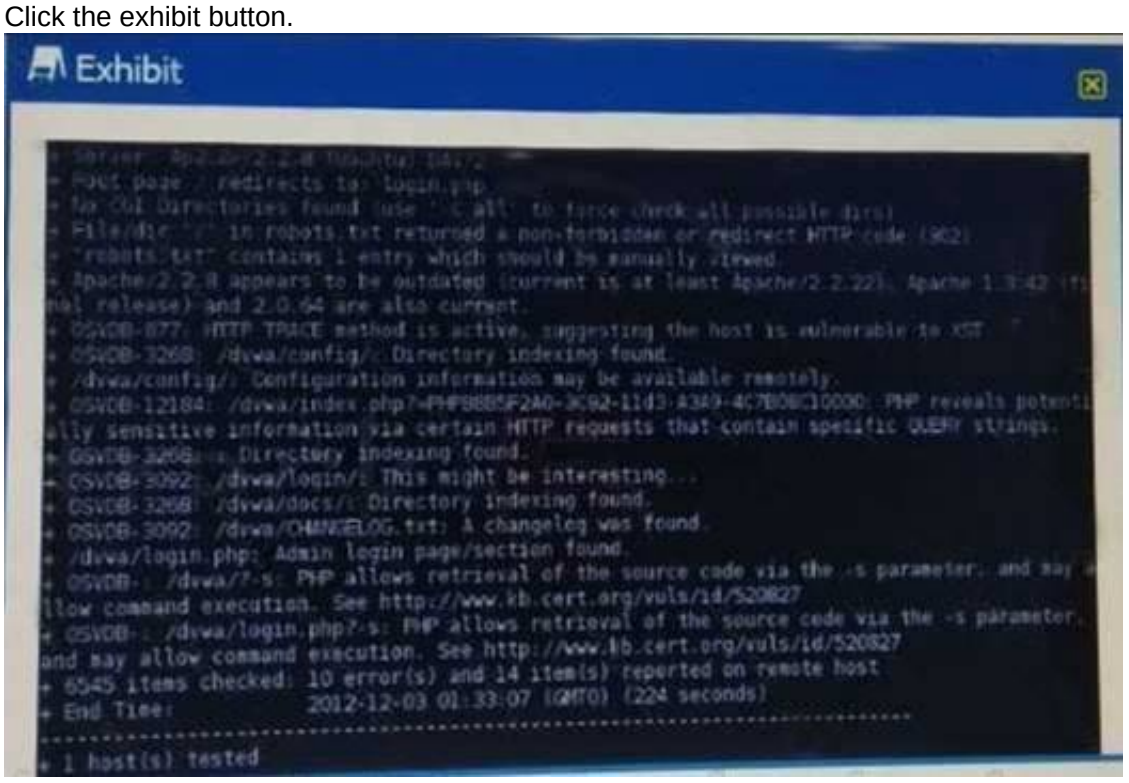
A penetration tester is performing an assessment when the network administrator shows the tester a packet sample that is causing trouble on the network Which of the following types of attacks should the tester stop?

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

D. SMTP relay

Answer: B

NEW QUESTION 68
Click the exhibit button.



Given the Nikto vulnerability scan output shown in the exhibit, which of the following explogtation techniques might be used to explogt the target system? (Select TWO)

A. Arbitrary code execution
B. Session hijacking
C. SQL injection
D. Login credential brute-forcing
E. Cross-site request forgery

Answer: CE

NEW QUESTION 73
Which of Ihe following commands would allow a penetration tester to access a private network from the Internet in Metasplogt?

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/servet/aocka^a

Answer: D

NEW QUESTION 78
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 82
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::::::1
```

D)

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

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

Answer: D

NEW QUESTION 86
A penetration tester is preparing to conduct API testing Which of the following would be MOST helpful in preparing for this engagement?

A. NiktO
B. WAR
C. W3AF
D. Swagger

Answer: A

NEW QUESTION 90
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 91
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 93
.....

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