Free PDF Quiz Marvelous PT0-002 - CompTIA PenTest+ Certification Valid Exam Experience

DOWNLOAD the newest Pass4training PT0-002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1YvY1UBqYzfwo8f3NVjv5ZTk_xRtC_1kH

Our PT0-002 practice materials compiled by the most professional experts can offer you with high quality and accuracy practice materials for your success. Up to now, we have more than tens of thousands of customers around the world supporting our PT0-002 exam torrent. If you are unfamiliar with our PT0-002 Study Materials, please download the PT0-002 free demos for your reference, and to some unlearned exam candidates, you can master necessities by our PT0-002 practice materials quickly. So our PT0-002 materials are elemental materials you cannot miss.

Passing the CompTIA PT0-002 Certification exam is a benchmark measure of the skills and knowledge essential for the individual to perform pre and post-vulnerability analysis of networks, devices, and applications. CompTIA PenTest+ Certification certification validates that you understand the permissible and lawful procedures for penetration testing and is instrumental in accelerating the individual's career in the cybersecurity field. CompTIA PenTest+ Certification certification offers numerous job opportunities, and individuals holding the CompTIA PT0-002 Certification Exam have a high earning potential in the market.

CompTIA PT0-002 certification exam covers various topics related to penetration testing, such as planning and scoping, information gathering and vulnerability identification, attacks, exploitation, and post-exploitation techniques, reporting, and communication skills. PT0-002 Exam also tests the candidate's knowledge of legal and regulatory compliance requirements, standards, and ethical considerations. CompTIA PenTest+ Certification certification exam is vendor-neutral, which means it is not limited to a particular software or hardware vendor. A successful completion of the exam indicates that the candidate possesses the necessary skills and knowledge required to conduct a successful penetration test.

>> PT0-002 Valid Exam Experience <<

100% CompTIA PT0-002 Accuracy & Dumps PT0-002 Reviews

We stand behind all of our customers, so we provide you with the best valid and useful CompTIA PT0-002 exam training. Regular and frequent updates for PT0-002 dumps are necessary, so you can get hold of the PT0-002 updated exam material every time. Besides, we offer the exact questions with correct answers, which can ensure you 100% pass in your CompTIA PT0-002 Actual Test. We have 100% money back guarantee, in case of failure, we will give you full refund.

CompTIA PenTest+ Certification Sample Questions (Q55-Q60):

NEW QUESTION # 55
A penetration tester conducted a vulnerability scan against a client's critical servers and found the following:

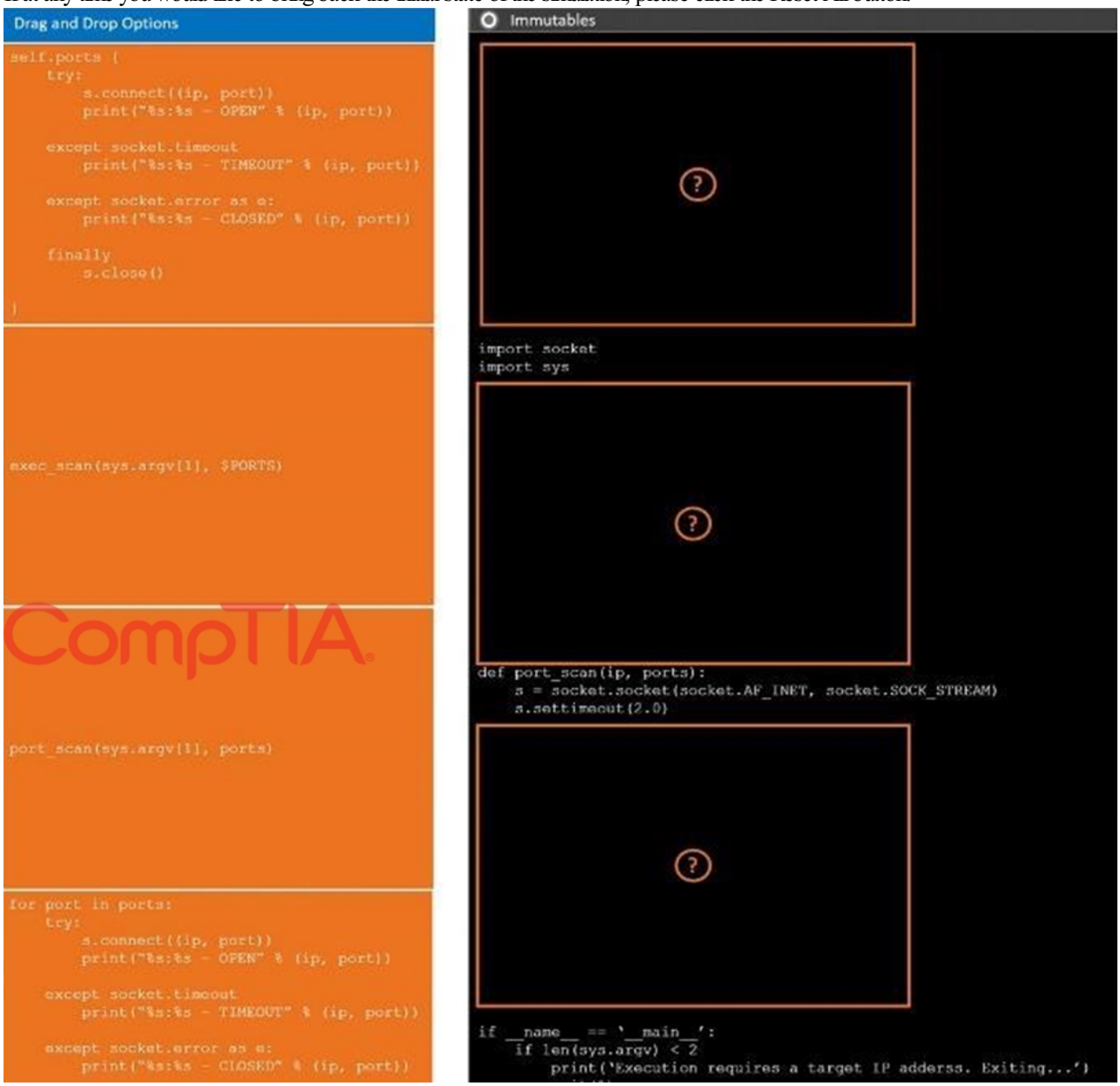
Host name	IP	OS	Security updates
addc01.local	10.1.1.20	Windows Server 2012	KB4581001, KB4585587, KB4586007
addc02.local	10.1.1.21	Windows Server 2012	KB4586007
dnsint.local	10.1.1.22	Windows Server 2012	KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local	10.1.1.23	Windows Server 2012	KB4581001

Which of the following would be a recommendation for remediation?

- A. Utilize the secure software development life cycle
- B. Deploy a user training program
- C. Implement a patch management plan
- D. Configure access controls on each of the servers

Answer: C

NEW QUESTION # 56
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.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



```
    finally
        s.close()
```

```
(:ports => 21 :ports => 22)
```

```
#!/usr/bin/python
```

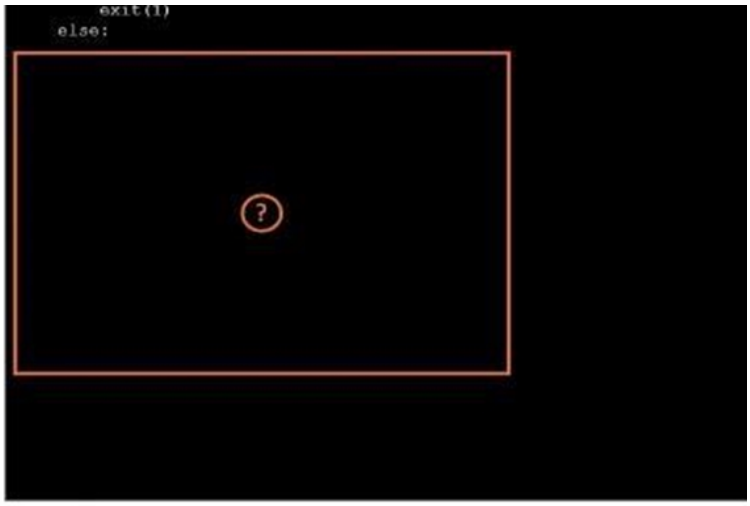
```
ports = [21,22]
```

```
#!/usr/bin/ruby
```

```
run_scan(sys.argv[1],ports)
```

```
#!/usr/bin/bash
```

```
        exit(1)
    else:
```



```
export $PORTS = 21,22
```

```
for %PORT in %PORTS:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()
```

Answer:

Explanation:

Drag and Drop Options

```
self.ports (
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()
)
```

```
exec_scan(sys.argv[1], $PORTS)
```

```
port_scan(sys.argv[1], ports)
```

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))
```

Immutables

```
#!/usr/bin/python
```

```
import socket
import sys
```

```
ports = [21,22]
```

```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()
```

```
    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()
```

```
:ports => 21 :ports => 22)
```

```
#!/usr/bin/python
```

```
orts = [21,22]
```

```
#!/usr/bin/ruby
```

```
un_scan(sys.argv[1],ports)
```

```
#!/usr/bin/bash
```

```
if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP adderss. Exiting...')
        exit(1)
    else:
```

```
run_scan(sys.argv[1],ports)
```

```
export $PORTS = 21,22
```

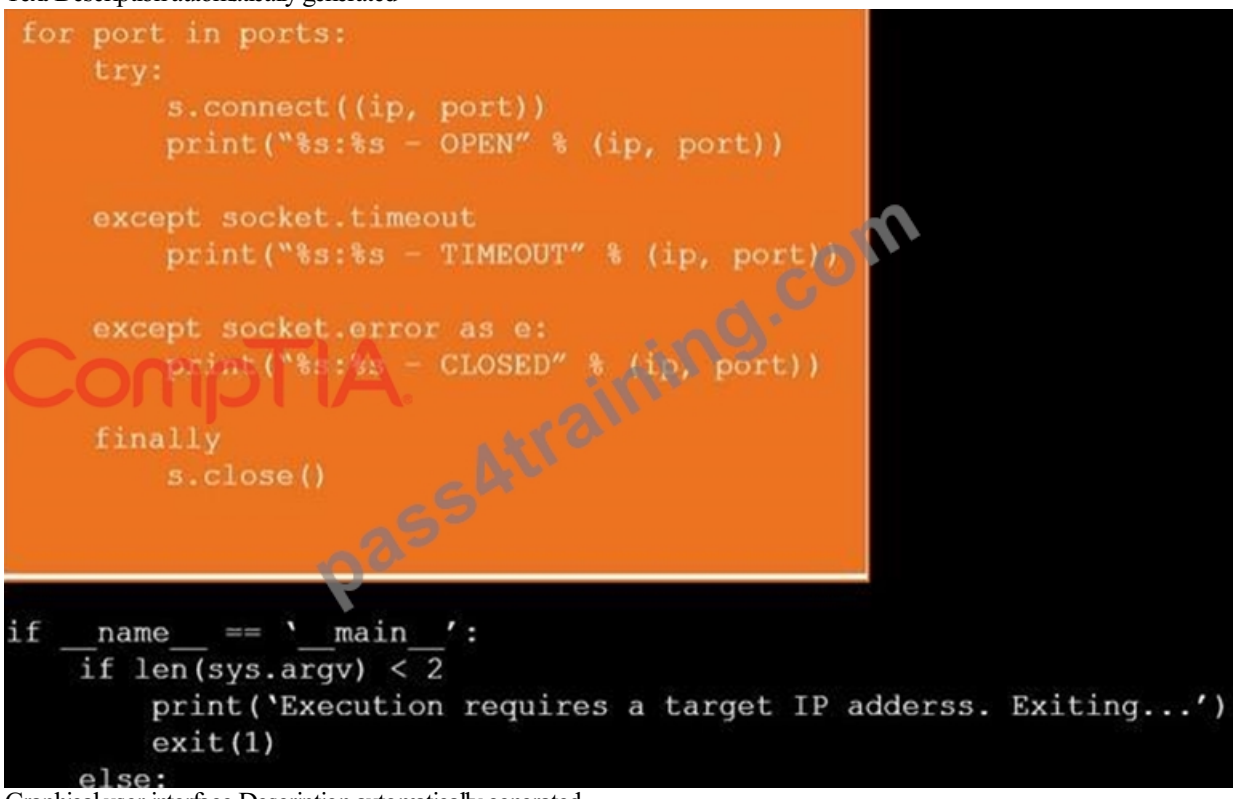
```
for %PORT in %PORTS:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()
```

Explanation

A picture containing shape Description automatically generated

A picture containing treemap chart Description automatically generated

Text Description automatically generated



Graphical user interface Description automatically generated

NEW QUESTION # 57
A penetration tester is looking for a particular type of service and obtains the output below:
I Target is synchronized with 127.127.38.0 (reference clock)
I Alternative Target Interfaces:
I 10.17.4.20
I Private Servers (0)
I Public Servers (0)
I Private Peers (0)
I Public Peers (0)
I Private Clients (2)
I 10.20.8.69 169.254.138.63
I Public Clients (597)
I 4.79.17.248 68.70.72.194 74.247.37.194 99.190.119.152
I 12.10.160.20 68.80.36.133 75.1.39.42 108.7.58.118
I 68.56.205.98
I 2001:1400:0:0:0:0:0:1 2001:16d8:ddOO:38:0:0:0:2
I 2002:db5a:bccd:l:21d:e0ff:feb7:b96f 2002:b6ef:81c4:0:0:1145:59c5:3682 I Other Associations (1)
|_ 127.0.0.1 seen 1949869 times, last tx was unicast v2 mode 7
Which of the following commands was executed by the tester?

- A. nmap-sU-pU:161-Pn-n-script=voldemort-info <target>
- B. nmap-sU-pU:517-Pn-n-script=supermicro-ipmi-config<target>
- C. nmap-sU-pU:123-Pn-n-script=ntp-monlist <target>
- D. nmap-sU-pU:37 -Pn -n -script=icap-info <target>

Answer: C

Explanation:
The output provided indicates the use of the NTP protocol (Network Time Protocol) for querying a target system. The reference to "Public Clients" and the specific IP addresses listed, along with the mention of
"Other Associations" and the use of NTP version 2, points towards the execution of an NTP monlist request.
The monlist feature in NTP servers can be used to obtain a list of the last 600 hosts that have interacted with the NTP server. The command nmap -sU -pU:123 -Pn -n -script=ntp-monlist <target> specifically targets NTP servers on UDP port 123 to retrieve this information, making it the correct choice based on the output shown.

NEW QUESTION # 58
A penetration tester recently performed a social-engineering attack in which the tester found an employee of the target company at a local coffee shop and over time built a relationship with the employee. On the employee's birthday, the tester gave the employee an external hard drive as a gift. Which of the following social-engineering attacks was the tester utilizing?

- A. Tailgating
- B. Phishing

- C. Shoulder surfing
- D. Baiting

Answer: D

NEW QUESTION # 59
A consultant is reviewing the following output after reports of intermittent connectivity issues:
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]
? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]
? (192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet]
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet] Which of the following is MOST likely to be reported by the consultant?

- A. A device on the network has an IP address in the wrong subnet.
- B. An ARP flooding attack is using the broadcast address to perform DDoS.
- C. A device on the network has poisoned the ARP cache.
- D. A multicast session was initiated using the wrong multicast group.

Answer: C

Explanation:
Explanation
The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine (192.168.1.136) also claims to be on the same MAC address. With this on the same network, intermittent connectivity will be inevitable as along as the gateway remains unreachable on the IP known by the others machines on the network, and given that the new machine claiming to be the gateway has not been configured to route traffic.
The output shows an ARP table that contains entries for IP addresses and their corresponding MAC addresses on a local network interface (en0). ARP stands for Address Resolution Protocol and is used to map IP addresses to MAC addresses on a network. However, one entry in the table is suspicious:
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
This entry has the same MAC address as another entry:
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
This indicates that a device on the network has poisoned the ARP cache by sending false ARP replies that associate its MAC address with multiple IP addresses, including 192.168.1.136 and 192.168.1.1 (which is likely the gateway address). This allows the device to intercept or redirect traffic intended for those IP addresses.

NEW QUESTION # 60
.....

- Valid CompTIA PenTest+ Certification braindumps pdf - PT0-002 valid dumps □ Immediately open 《 www.pdfvce.com 》 and search for ➡ PT0-002 □□□ to obtain a free download □Latest PT0-002 Test Fee
- New PT0-002 Exam Test □ Latest PT0-002 Test Fee □ PT0-002 Exam Simulator Fee □ Search for ➥ PT0-002 □ □ on □ www.examsreviews.com □ immediately to obtain a free download □Valid PT0-002 Braindumps
- PT0-002 Test Discount □ New PT0-002 Exam Test □ Valid PT0-002 Braindumps □ Download 【 PT0-002 】 for free by simply searching on ✔ www.pdfvce.com □✔□ □PT0-002 Valid Exam Cram
- 100% Pass Quiz 2025 CompTIA PT0-002: CompTIA PenTest+ Certification Authoritative Valid Exam Experience □ Download ▹ PT0-002 ◃ for free by simply entering □ www.examcollectionpass.com □ website □PT0-002 Pass Rate
- Valid CompTIA PenTest+ Certification braindumps pdf - PT0-002 valid dumps □ Open website 《 www.pdfvce.com 》 and search for □ PT0-002 □ for free download □Exam PT0-002 Papers
- PT0-002 - Newest CompTIA PenTest+ Certification Valid Exam Experience □ Search for " PT0-002 " and download it for free immediately on [www.examcollectionpass.com] □PT0-002 Reliable Test Review
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, motionentrance.edu.np, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, study.stcs.edu.np, www.rohitgaikwad.com, www.stes.tyc.edu.tw, prepelite.in, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New PT0-002 dumps are available on Google Drive shared by Pass4training: https://drive.google.com/open?id=1YvY1UBqYzfwo8f3NVjv5ZTk_xRtC_1kH