PT0-002 Q&As

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

CORRECT TEXT SIMULATION Using the output, identify potential attack vectors that should be further investigated.

Weak Apache Tomcat Credentials

Null session enumeration

Weak SMB file permissions

Webdav file upload

ARP spoofing

SNMP enumeration

Fragmentation attack

FTP anonymous login

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```

-Pn

-sV

-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

-sL

-sU

-O

192.168.2.2

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```

ports – [21, 22]

{:ports => 21:ports => 22}

#!/usr/bin/python

```
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()
```

export $PORTS = 21,22

#!/usr/bin/ruby

#!/usr/bin/bash

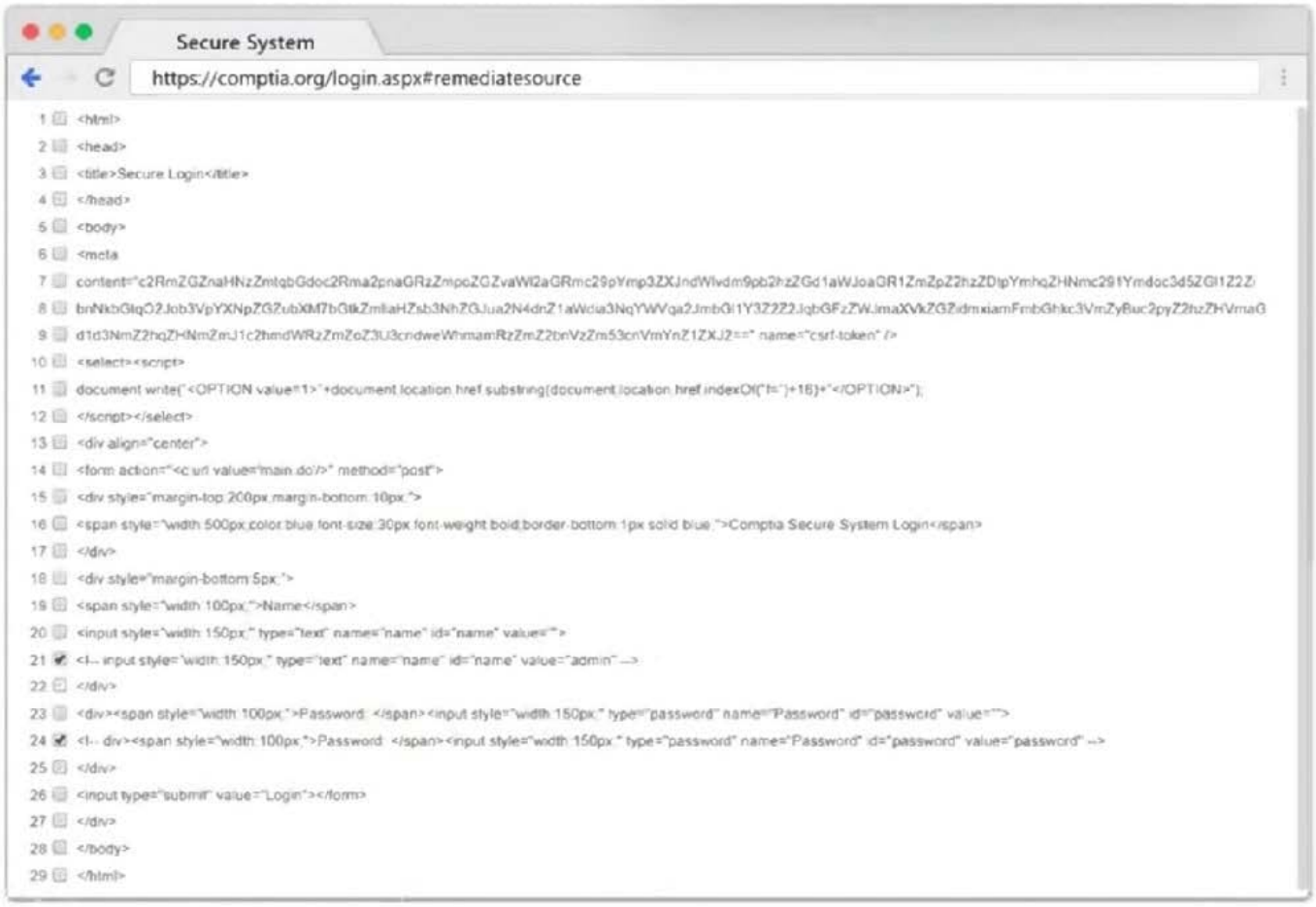
for port in ports:

Immutables

```
import socket
import sys

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

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



Correct Answer: Answer: See explanation below.

1: Null session enumeration

Weak SMB file permissions

Fragmentation attack

2: nmap

-sV

-p 1-1023

192.168.2.2

3: #!/usr/bin/python

export $PORTS = 21,22

for $PORT in $PORTS:

try:

s.connect((ip, port))

print("%s:%s ?OPEN" % (ip, port))

except socket.timeout

print("%:%s ?TIMEOUT" % (ip, port))

except socket.error as e:

print("%:%s ?CLOSED" % (ip, port))

finally

s.close()

port_scan(sys.argv[1], ports)

QUESTION 2

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

A. Acceptance by the client and sign-off on the final report

B. Scheduling of follow-up actions and retesting

C. Attestation of findings and delivery of the report

D. Review of the lessons learned during the engagement

Correct Answer: C

QUESTION 3

A company becomes concerned when the security alarms are triggered during a penetration test. Which of the following should the company do NEXT?

A. Halt the penetration test.

B. Contact law enforcement.

C. Deconflict with the penetration tester.

D. Assume the alert is from the penetration test.

Correct Answer: B

QUESTION 4

A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

A. Multiple handshakes

B. IP addresses

C. Encrypted file transfers

D. User hashes sent over SMB

Correct Answer: B

QUESTION 5

A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP. Which of the following steps should the tester take NEXT?

A. Send deauthentication frames to the stations.

B. Perform jamming on all 2.4GHz and 5GHz channels.

C. Set the malicious AP to broadcast within dynamic frequency selection channels.

D. Modify the malicious AP configuration to not use a pre-shared key.

Correct Answer: A

https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless- networks-with-wifislax