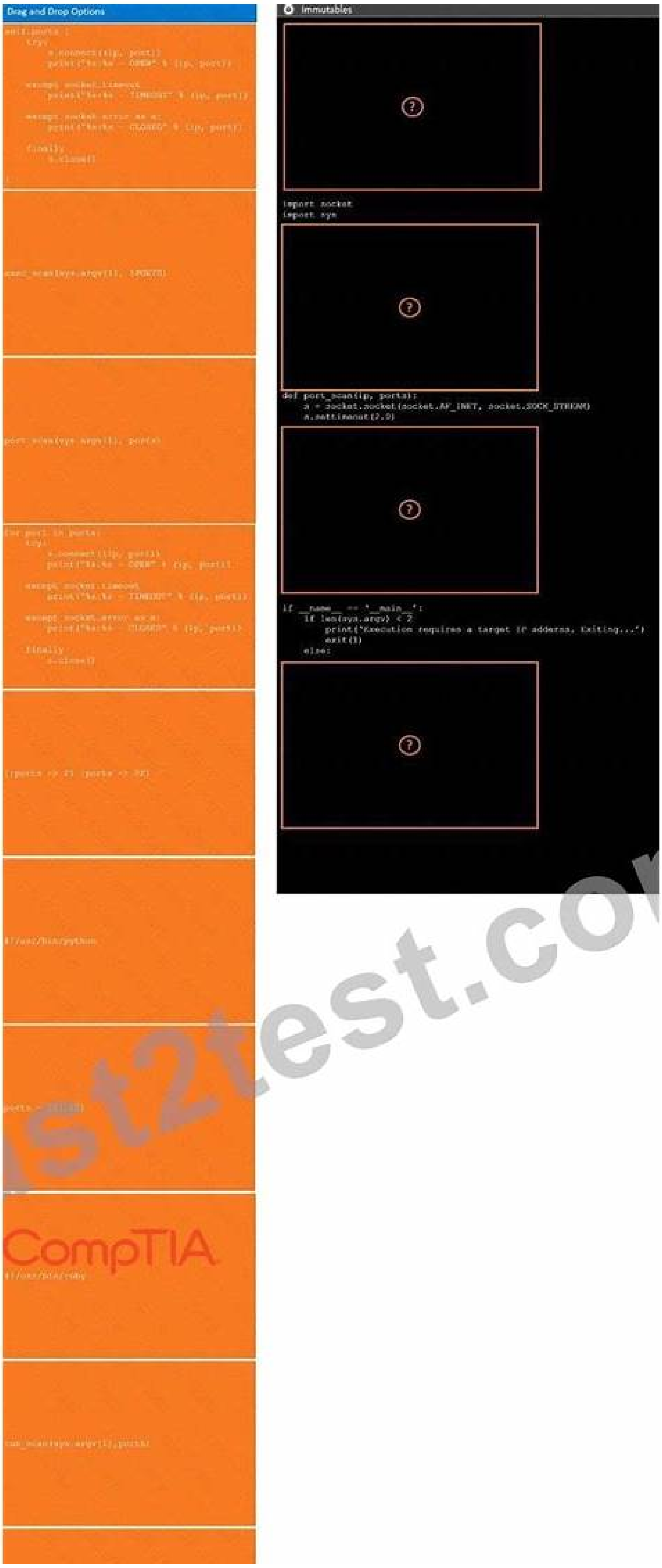
CompTIA - PT0-003–Efficient New Exam Name



```
until(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()
}
```

```
conn_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))

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

    finally:
        s.close()
```

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

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

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

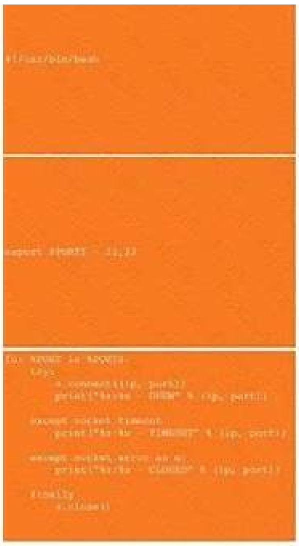
```
#!/usr/bin/ruby
```

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

```
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 adderss. Exiting...')
        exit(1)
    else:
```



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

```
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()
```

BTW, DOWNLOAD part of FreePdfDump PT0-003 dumps from Cloud Storage: https://drive.google.com/open?id=1Y0G2wugavwnZzMOtW-0TjGe9tpLCR3vv

You will be able to assess your shortcomings and improve gradually without having anything to lose in the actual CompTIA PenTest+ Exam exam. You will sit through mock exams and solve actual CompTIA PT0-003 dumps. In the end, you will get results that will improve each time you progress and grasp the concepts of your syllabus. The desktop-based CompTIA PT0-003 Practice Exam software is only compatible with Windows.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	• Engagement Management: In this topic, cybersecurity analysts learn about pre-engagement activities, collaboration, and communication in a penetration testing environment. The topic covers testing frameworks, methodologies, and penetration test reports. It also explains how to analyze findings and recommend remediation effectively within reports, crucial for real-world testing scenarios.
Topic 2	• Attacks and Exploits: This extensive topic trains cybersecurity analysts to analyze data and prioritize attacks. Analysts will learn how to conduct network, authentication, host-based, web application, cloud, wireless, and social engineering attacks using appropriate tools. Understanding specialized systems and automating attacks with scripting will also be emphasized.
Topic 3	• Post-exploitation and Lateral Movement: Cybersecurity analysts will gain skills in establishing and maintaining persistence within a system. This topic also covers lateral movement within an environment and introduces concepts of staging and exfiltration. Lastly, it highlights cleanup and restoration activities, ensuring analysts understand the post-exploitation phase's responsibilities.
Topic 4	• Vulnerability Discovery and Analysis: In this section, cybersecurity analysts will learn various techniques to discover vulnerabilities. Analysts will also analyze data from reconnaissance, scanning, and enumeration phases to identify threats. Additionally, it covers physical security concepts, enabling analysts to understand security gaps beyond just the digital landscape.
Topic 5	• Reconnaissance and Enumeration: This topic focuses on applying information gathering and enumeration techniques. Cybersecurity analysts will learn how to modify scripts for reconnaissance and enumeration purposes. They will also understand which tools to use for these stages, essential for gathering crucial information before performing deeper penetration tests.

>> New PT0-003 Exam Name <<

Valid PT0-003 Test Pdf, PT0-003 Certification Exam Dumps

The FreePdfDump aids students in passing the test on their first try by giving them the real questions in three formats, 24/7 support team assistance, free demo, up to 1 year of free updates, and the satisfaction guarantee. As a result of its persistent efforts in providing candidates with actual PT0-003 Exam Questions, FreePdfDump has become one of the best platforms to prepare for the CompTIA PT0-003 exam successfully. One must prepare with FreePdfDump exam questions if one wishes to pass the PT0-003 exam on their first attempt.

CompTIA PenTest+ Exam Sample Questions (Q30-Q35):

NEW QUESTION # 30
A penetration tester established an initial compromise on a host. The tester wants to pivot to other targets and set up an appropriate relay. The tester needs to enumerate through the compromised host as a relay from the tester's machine. Which of the following commands should the tester use to do this task from the tester's host?

- A. attacker_host$ nc -nlp 8000 | nc -n <target_cidr> attacker_host$ nmap -sT 127.0.0.1 8000
- B. attacker_host$ proxychains nmap -sT <target_cidr>
- C. attacker_host$ nmap -sT <target_cidr> | nc -n <compromised_host> 22
- D. attacker_host$ mknod backpipe p attacker_host$ nc -l -p 8000 | 0<backpipe | nc <target_cidr> 80 | tee backpipe

Answer: B

Explanation:
ProxyChains is a tool that allows you to route your traffic through a chain of proxy servers, which can be used to anonymize your network activity. In this context, it is being used to route Nmap scan traffic through the compromised host, allowing the penetration tester to pivot and enumerate other targets within the network.
* Understanding ProxyChains:
* Purpose: ProxyChains allows you to force any TCP connection made by any given application to follow through proxies like TOR, SOCKS4, SOCKS5, and HTTP(S).
* Usage: It's commonly used to anonymize network traffic and perform actions through an intermediate proxy.
* Command Breakdown:
* proxychains nmap -sT <target_cidr>: This command uses ProxyChains to route the Nmap scan traffic through the configured proxies.
* Nmap Scan (-sT): This option specifies a TCP connect scan.
* Setting Up ProxyChains:
* Configuration File: ProxyChains configuration is typically found at /etc/proxychains.conf.
* Adding Proxy: Add the compromised host as a SOCKS proxy.
Step-by-Step Explanationplaintext
Copy code
socks4 127.0.0.1 1080
* Execution:
* Start Proxy Server: On the compromised host, run a SOCKS proxy (e.g., using ssh -D 1080 user@compromised_host).
* Run ProxyChains with Nmap: Execute the command on the attacker's host.
proxychains nmap -sT <target_cidr>
* References from Pentesting Literature:
* ProxyChains is commonly discussed in penetration testing guides for scenarios involving pivoting through a compromised host.
* HTB write-ups frequently illustrate the use of ProxyChains for routing traffic through intermediate systems.

NEW QUESTION # 31
During a security audit, a penetration tester wants to run a process to gather information about a target network's domain structure and associated IP addresses. Which of the following tools should the tester use?

- A. Netcat
- B. Nmap
- C. Wireshark
- D. Dnsenum

Answer: D

Explanation:

Dnsenum is a tool specifically designed to gather information about DNS, including domain structure and associated IP addresses.
Dnsenum: This tool is used for DNS enumeration and can gather information about a domain's DNS records, subdomains, IP addresses, and other related information. It is highly effective for mapping out a target network's domain structure.
Nmap: While a versatile network scanning tool, Nmap is more focused on port scanning and service detection rather than detailed DNS enumeration.
Netcat: This is a network utility for reading and writing data across network connections, not for DNS enumeration.
Wireshark: This is a network protocol analyzer used for capturing and analyzing network traffic but not specifically for gathering DNS information.

NEW QUESTION # 32
A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?

- A. schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe
- B. crontab -l; echo "@reboot sleep 200 && ncat -lvp 4242 -e /bin/bash") | crontab 2>/dev/null
- C. wmic startup get caption,command
- D. sudo useradd -ou 0 -g 0 user

Answer: A

NEW QUESTION # 33
During an assessment, a penetration tester exploits an SQLi vulnerability. Which of the following commands would allow the penetration tester to enumerate password hashes?

- A. sqlmap -u www.example.com/?id=1 --schema --current-user --current-db
- B. sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred
- C. sqlmap -u www.example.com/?id=1 --search -T user
- D. sqlmap -u www.example.com/?id=1 --tables -D accounts

Answer: B

Explanation:
To enumerate password hashes using an SQL injection vulnerability, the penetration tester needs to extract specific columns from the database that typically contain password hashes. The --dump command in sqlmap is used to dump the contents of the specified database table. Here's a breakdown of the options:
Option A: sqlmap -u www.example.com/?id=1 --search -T user
The --search option is used to search for columns and not to dump data. This would not enumerate password hashes.
Option B: sqlmap -u www.example.com/?id=1 --dump -D accounts -T users -C cred This command uses --dump to extract data from the specified database accounts, table users, and column cred.
This is the correct option to enumerate password hashes, assuming cred is the column containing the password hashes.
Option C: sqlmap -u www.example.com/?id=1 --tables -D accounts
The --tables option lists all tables in the specified database but does not extract data.
Option D: sqlmap -u www.example.com/?id=1 --schema --current-user --current-db The --schema option provides the database schema information, and --current-user and --current-db provide information about the current user and database but do not dump data.
References from Pentest:
Writeup HTB: Demonstrates using sqlmap to dump data from specific tables to retrieve sensitive information, including password hashes.
Luke HTB: Shows the process of exploiting SQL injection to extract user credentials and hashes by dumping specific columns from the database.

NEW QUESTION # 34
Which of the following types of assessments MOST likely focuses on vulnerabilities with the objective to access specific data?

- A. A red-team assessment
- B. An unknown-environment assessment
- C. A known-environment assessment

- D. A compliance-based assessment

Answer: A

Explanation:
A red-team assessment is a type of penetration testing that simulates a real-world attack scenario with the goal of accessing specific data or systems. A red-team assessment is different from an unknown-environment assessment, which does not have a predefined objective and focuses on discovering as much information as possible about the target. A known-environment assessment is a type of penetration testing that involves cooperation and communication with the target organization, and may not focus on specific data or systems.
A compliance-based assessment is a type of penetration testing that aims to meet certain regulatory or industry standards, and may not focus on specific data or systems.

NEW QUESTION # 35
......

If you follow the steps of our PT0-003 exam questions, you can easily and happily learn and ultimately succeed in the ocean of learning. And our PT0-003 exam questions can help you pass the PT0-003 exam for sure. Choosing our PT0-003 exam questions actually means that you will have more opportunities to be promoted in the near future. We are confident that in the future, our PT0-003 Study Tool will be more attractive and the pass rate will be further enhanced. For now, the high pass rate of our PT0-003 exam questions is more than 98%.

Valid PT0-003 Test Pdf: https://www.freepdfdump.top/PT0-003-valid-torrent.html

P.S. Free & New PT0-003 dumps are available on Google Drive shared by FreePdfDump: https://drive.google.com/open?id=1Y0G2wugavwnZzMOtW-0TjGe9tpLCR3vv