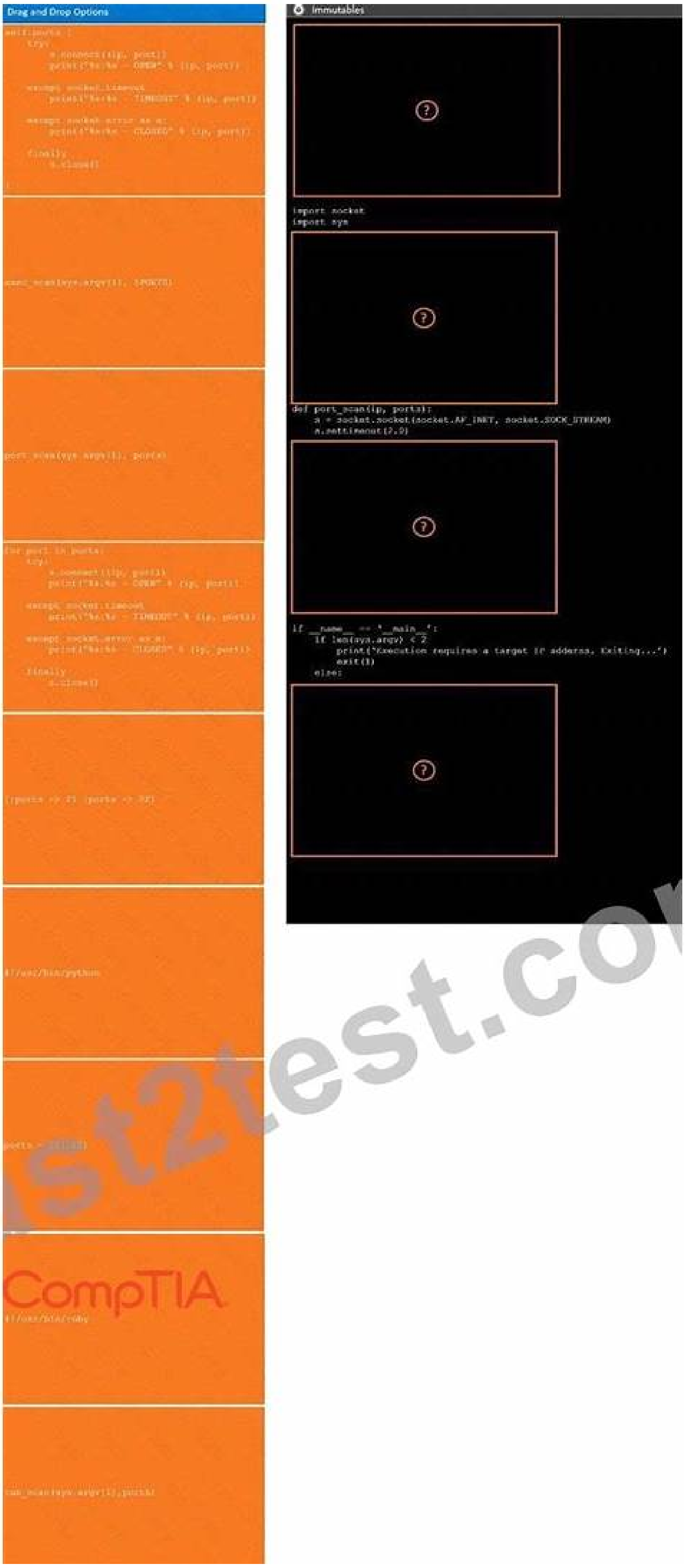
Free PDF Quiz CompTIA - Unparalleled Exam PT0-003 Answers



```
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()
}
```

```
sant_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}
```

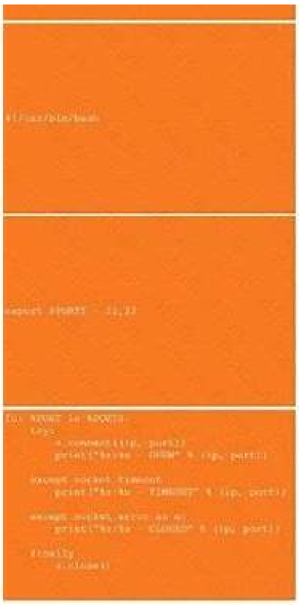
```
#!/usr/bin/python
```

```
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()
```

P.S. Free & New PT0-003 dumps are available on Google Drive shared by TestPassKing: https://drive.google.com/open?id=1uxIxPxT-3LNf0PSgG1CUNdSiboHgmMA4

The curtain of life stage may be opened at any time, the key is that you are willing to show, or choose to avoid. Most of People who can seize the opportunityin front of them are successful. So you have to seize this opportunity of TestPassKing. Only with it can you show your skills. TestPassKing CompTIA PT0-003 Exam Training materials is the most effective way to pass the certification exam. With this certification, you will achieve your dreams, and become successful.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• 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 3	• 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 4	• 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 5	• 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.

CompTIA PT0-003 Exam Collection Pdf & PT0-003 Torrent

With these mock exams, it is easy to track your progress by monitoring your marks each time you go through the PT0-003 practice test. Our PT0-003 practice exams will give you an experience of attempting the PT0-003 original examination. You will be able to deal with the actual exam pressure better when you have already experienced it in our CompTIA PT0-003 practice exams.

CompTIA PenTest+ Exam Sample Questions (Q56-Q61):

NEW QUESTION # 56
During a penetration testing engagement, a tester targets the internet-facing services used by the client. Which of the following describes the type of assessment that should be considered in this scope of work?

- A. Web
- B. Mobile
- C. Segmentation
- D. External

Answer: D

Explanation:
An external assessment focuses on testing the security of internet-facing services.
External Assessment: It involves evaluating the security posture of services exposed to the internet, such as web servers, mail servers, and other public-facing infrastructure. The goal is to identify vulnerabilities that could be exploited by attackers from outside the organization's network.
Segmentation: This type of assessment focuses on ensuring that different parts of a network are appropriately segmented to limit the spread of attacks. It's more relevant to internal network architecture.
Mobile: This assessment targets mobile applications and devices, not general internet-facing services.
Web: While web assessments focus on web applications, the scope of an external assessment is broader and includes all types of internet-facing services.

NEW QUESTION # 57
A company hires a penetration tester to perform an external attack surface review as part of a security engagement. The company informs the tester that the main company domain to investigate is comptia.org.
Which of the following should the tester do to accomplish the assessment objective?

- A. Perform a phishing assessment to try to gain access to more resources and users' computers.
- B. Perform a physical security review to identify vulnerabilities that could affect the company.
- C. Perform information-gathering techniques to review internet-facing assets for the company.
- D. Perform a vulnerability assessment over the main domain address provided by the client.

Answer: C

Explanation:
Comprehensive and Detailed Explanation:
An external attack surface review focuses on identifying publicly accessible assets that an attacker could exploit. The first step in this process is information gathering, which involves enumerating domains, subdomains, public IPs, DNS records, and other internet-facing resources. This is done using passive reconnaissance tools such as Whois, Shodan, Google Dorking, and OSINT techniques.
Option A is correct because it aligns with the assessment goal-finding public-facing systems and their vulnerabilities before an attacker does.
Option B (phishing assessment) is incorrect because it involves social engineering, which is not part of an external attack surface review.
Option C (physical security review) is incorrect as it pertains to physical penetration testing, not an external attack analysis.
Option D (vulnerability assessment) is incorrect because a vulnerability assessment is a later step after reconnaissance. The first step is identifying assets through information gathering.

NEW QUESTION # 58

During a security assessment of a web application, a penetration tester was able to generate the following application response:
Unclosed quotation mark after the character string Incorrect syntax near ''.
Which of the following is the most probable finding?

- A. Business logic flaw
- B. SQL injection
- C. Cross-site scripting
- D. Race condition

Answer: B

Explanation:
The error message "Unclosed quotation mark after the character string Incorrect syntax near '.'" suggests that the application is vulnerable to SQL Injection (A). This type of vulnerability occurs when an attacker is able to inject malicious SQL queries into an application's database query. The error message indicates that the application's input handling allows for the manipulation of the underlying SQL queries, which can lead to unauthorized data access, data modification, and other database-related attacks.

NEW QUESTION # 59

A penetration tester needs to launch an Nmap scan to find the state of the port for both TCP and UDP services. Which of the following commands should the tester use?

- A. nmap -sU -sY -p 1-65535 example.com
- B. nmap -sU -sW -p 1-65535 example.com
- C. nmap -sU -sN -p 1-65535 example.com
- D. nmap -sU -sT -p 1-65535 example.com

Answer: D

Explanation:
To find the state of both TCP and UDP ports using Nmap, the appropriate command should combine both TCP and UDP scan options:
Understanding the Options:
-sU: Performs a UDP scan.
-sT: Performs a TCP connect scan.
Command Explanation:
Command: nmap -sU -sT -p 1-65535 example.comExplanation: This command will scan both TCP and UDP ports from 1 to 65535 on the target example.com. Combining -sU and -sT ensures that both types of services are scanned.

NEW QUESTION # 60

A penetration tester is testing a power plant's network and needs to avoid disruption to the grid. Which of the following methods is most appropriate to identify vulnerabilities in the network?

- A. Run a network mapper tool to get an understanding of the devices.
- B. Configure a network scanner engine and execute the scan.
- C. Execute a testing framework to validate vulnerabilities on the devices.
- D. Configure a port mirror and review the network traffic.

Answer: D

Explanation:
When testing a power plant's network and needing to avoid disruption to the grid, configuring a port mirror and reviewing the network traffic is the most appropriate method to identify vulnerabilities without causing disruptions.
* Port Mirroring:
* Definition: Port mirroring (SPAN - Switched Port Analyzer) is a method of monitoring network traffic by duplicating packets from one or more switch ports to another port where a monitoring device is connected.
* Purpose: Allows passive monitoring of network traffic without impacting network operations or device performance.
* Avoiding Disruption:
* Non-Intrusive: Port mirroring is non-intrusive and does not generate additional traffic or load on the network devices, making it

suitable for sensitive environments like power plants where disruption is not acceptable.
* Other Options:
* Network Scanner Engine: Active scanning might disrupt network operations or devices, which is not suitable for critical infrastructure.
* Testing Framework: Validating vulnerabilities on devices might involve active testing, which can be disruptive.
* Network Mapper Tool: Running a network mapper tool (like Nmap) actively scans the network and might disrupt services.
Pentest References:
* Passive Monitoring: Passive techniques such as port mirroring are essential in environments where maintaining operational integrity is critical.
* Critical Infrastructure Security: Understanding the need for non-disruptive methods in critical infrastructure penetration testing to ensure continuous operations.
By configuring a port mirror and reviewing network traffic, the penetration tester can identify vulnerabilities in the power plant's network without risking disruption to the grid.

NEW QUESTION # 61

......

The CompTIA PenTest+ Exam (PT0-003) web-based practice test works on all major browsers such as Safari, Chrome, MS Edge, Opera, IE, and Firefox. Users do not have to install any excessive software because this PT0-003 practice test is web-based. It can be accessed through any operating system like Windows, Linux, iOS, Android, or Mac. Another format of the practice test is the desktop software. It works offline only on Windows. Our CompTIA PenTest+ Exam (PT0-003) desktop-based practice exam software comes with all specifications of the web-based version.

PT0-003 Exam Collection Pdf: https://www.testpassking.com/PT0-003-exam-testking-pass.html