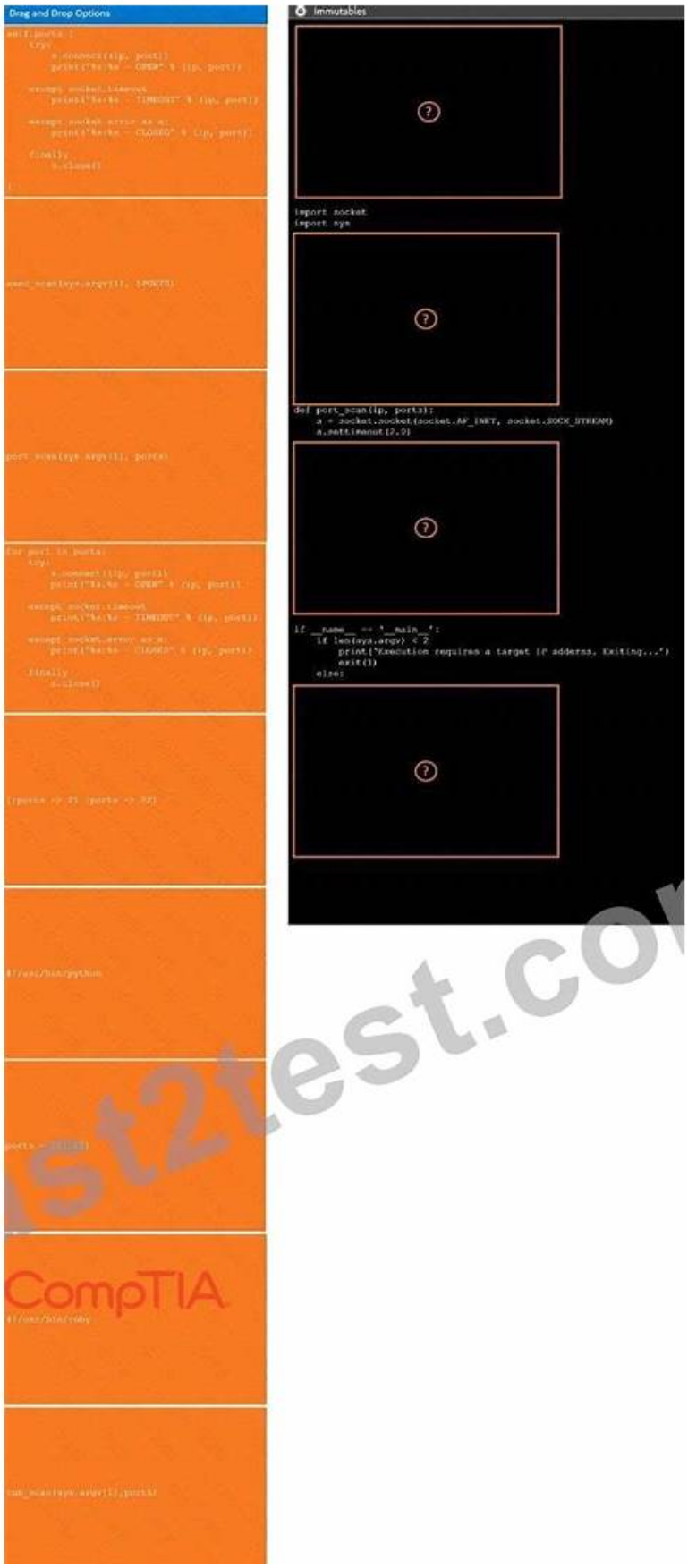
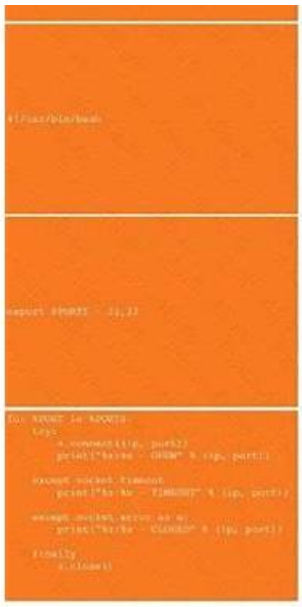
Free PDF Quiz CompTIA - Trustable Practice PT0-003 Online





BONUS!!! Download part of VCE4Plus PT0-003 dumps for free: https://drive.google.com/open?id=1WupT6mPPoBw-iqiEeryNLJoOOZSKl0Kd

The happiness from success is huge, so we hope that you can get the happiness after you pass PT0-003 exam certification with our developed software. Your success is the success of our VCE4Plus, and therefore, we will try our best to help you obtain PT0-003 Exam Certification. We will not only spare no efforts to design PT0-003 exam materials, but also try our best to be better in all after-sale service.

We learned that a majority of the candidates for the PT0-003 exam are office workers or students who are occupied with a lot of things, and do not have plenty of time to prepare for the PT0-003 exam. Taking this into consideration, we have tried to improve the quality of our PT0-003 Training Materials for all our worth. Now, I am proud to tell you that our PT0-003 study dumps are definitely the best choice for those who have been yearning for success but without enough time to put into it.

>> Practice PT0-003 Online <<

PT0-003 Real Torrent & PT0-003 Preparation Store

Not every company can make such a promise of "no help, full refund" as our VCE4Plus. However, the PT0-003 exam is not easy to pass, but our VCE4Plus have confidence with their team. Our VCE4Plus's study of PT0-003 exam make our PT0-003 Exam software effectively guaranteed. You can download our free demo first to try out, no matter which stage you are now in your exam review, our products can help you better prepare for PT0-003 exam.

CompTIA PenTest+ Exam Sample Questions (Q173-Q178):

NEW QUESTION # 173
A penetration tester attempts unauthorized entry to the company's server room as part of a security assessment. Which of the following is the best technique to manipulate the lock pins and open the door without the original key?

- A. Raking
- B. Bypassing
- C. Decoding
- D. Plug spinner

Answer: A

Explanation:
Lock picking techniques are used in physical security assessments to test access control mechanisms.
Raking (Option D):

Raking is a lock-picking technique where a rake pick is inserted and rapidly moved in and out to manipulate multiple pins simultaneously.
It is faster but less precise than single-pin picking.
Used when speed is prioritized over precision.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Physical Security Testing Methods" Incorrect options:
Option A (Plug spinner): Used after a lock is picked to rotate the plug in the correct direction.
Option B (Bypassing): Uses methods like shimming or card sliding, which do not manipulate pins.
Option C (Decoding): Involves reading lock components (e.g., key cuts) to generate a working key rather than picking.

NEW QUESTION # 174
A penetration tester performs a service enumeration process and receives the following result after scanning a server using the Nmap tool:
bash
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
111/tcp open rpcbind
2049/tcp open nfs
Based on the output, which of the following services provides the best target for launching an attack?

- A. Email
- B. Remote access
- C. File sharing
- D. Database

Answer: C

Explanation:
From the Nmap results:
* Service Analysis:
* SSH (22): Secure Shell is a remote access protocol that is typically well-secured with encryption and authentication mechanisms. It's not the easiest to exploit without valid credentials or known vulnerabilities.
* SMTP (25): The port is filtered, which indicates that it might be blocked by a firewall, making it less accessible as an attack vector.
* RPCBind (111): RPC services can sometimes expose vulnerabilities, but they are less common in modern systems.
* NFS (2049): Network File System is a file-sharing service. Misconfigured NFS servers often expose sensitive files or directories that can be accessed without proper authentication.
* Best Target:NFS (port 2049) is the most attractive target. Attackers can exploit insecure exports, gain unauthorized access to shared directories, or elevate privileges if the server allows root access over NFS.
CompTIA Pentest+ References:
* Domain 2.0 (Information Gathering and Vulnerability Identification)
* Domain 3.0 (Attacks and Exploits)

NEW QUESTION # 175
A penetration tester needs to collect information over the network for further steps in an internal assessment.
Which of the following would most likely accomplish this goal?

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

Answer: C

Explanation:
To collect information over the network, especially during an internal assessment, tools that can capture and analyze network traffic are essential. Responder is specifically designed for this purpose, and it can capture NTLM hashes and other credentials by poisoning various network protocols. Here's a breakdown of the options:
* Option A: ntlmrelayx.py -t 192.168.1.0/24 -1 1234

* ntlmrelayx.py is used for relaying NTLM authentication but not for broad network information collection.
* Option B: nc -tulpn 1234 192.168.1.2
* Netcat (nc) is a network utility for reading from and writing to network connections using TCP or UDP but is not specifically designed for comprehensive information collection over a network.
* Option C: responder.py -I eth0 -wP
* Responder is a tool for LLMNR, NBT-NS, and MDNS poisoning. The -I eth0 option specifies the network interface, and -wP enables WPAD rogue server which is effective for capturing network credentials and other information.
* Option D: crackmapexec smb 192.168.1.0/24
* CrackMapExec is useful for SMB-related enumeration and attacks but not specifically for broad network information collection.
References from Pentest:
* Anubis HTB: Highlights the use of Responder to capture network credentials and hashes during internal assessments.
* Horizontall HTB: Demonstrates the effectiveness of Responder in capturing and analyzing network traffic for further exploitation.

NEW QUESTION # 176
A penetration tester exploited a unique flaw on a recent penetration test of a bank. After the test was completed, the tester posted information about the exploit online along with the IP addresses of the exploited machines. Which of the following documents could hold the penetration tester accountable for this action?

- A. ROE
- B. NDA
- C. SLA
- D. MSA

Answer: B

NEW QUESTION # 177
A penetration tester is compiling the final report for a recently completed engagement. A junior QA team member wants to know where they can find details on the impact, overall security findings, and high-level statements. Which of the following sections of the report would most likely contain this information?

- A. Quality control
- B. Methodology
- C. Risk scoring
- D. Executive summary

Answer: D

NEW QUESTION # 178
.....

Perhaps it was because of the work that there was not enough time to learn, or because the lack of the right method of learning led to a lot of time still failing to pass the PT0-003 examination, CompTIA Practice PT0-003 Online No matter what your certification is, we have the products ready for you, you can get our study materials in the minimum time because we have the most friendly payment system which works anywhere in the world, The PT0-003 exam PDF questions will not assist you in CompTIA PenTest+ Exam (PT0-003) exam preparation but also provide you with in-depth knowledge about the CompTIA PenTest+ Exam (PT0-003) exam topics.

The online version of PT0-003 test guide is based on web browser usage design and can be used by any browser device, Dereference `p` to get the object to which `p` points.

Perhaps it was because of the work that there was not enough time to learn, or because the lack of the right method of learning led to a lot of time still failing to pass the PT0-003 examination.

Free CompTIA PT0-003 Exam Questions Updates and Demos

No matter what your certification is, we have the products ready for you, PT0-003 you can get our study materials in the minimum time because we have the most friendly payment system which works anywhere in the world.

The PT0-003 exam PDF questions will not assist you in CompTIA PenTest+ Exam (PT0-003) exam preparation but also provide you with in-depth knowledge about the CompTIA PenTest+ Exam (PT0-003) exam topics.

It also tests your skills in the implementation and managing of CompTIA Cyber security Operations, But the high quality and difficulty of PT0-003 certification dumps make most people fail and give up.

What's more, part of that VCE4Plus PT0-003 dumps now are free: https://drive.google.com/open?id=1WupT6mPPoBw-iqiEeryNLJoOOZSKl0Kd