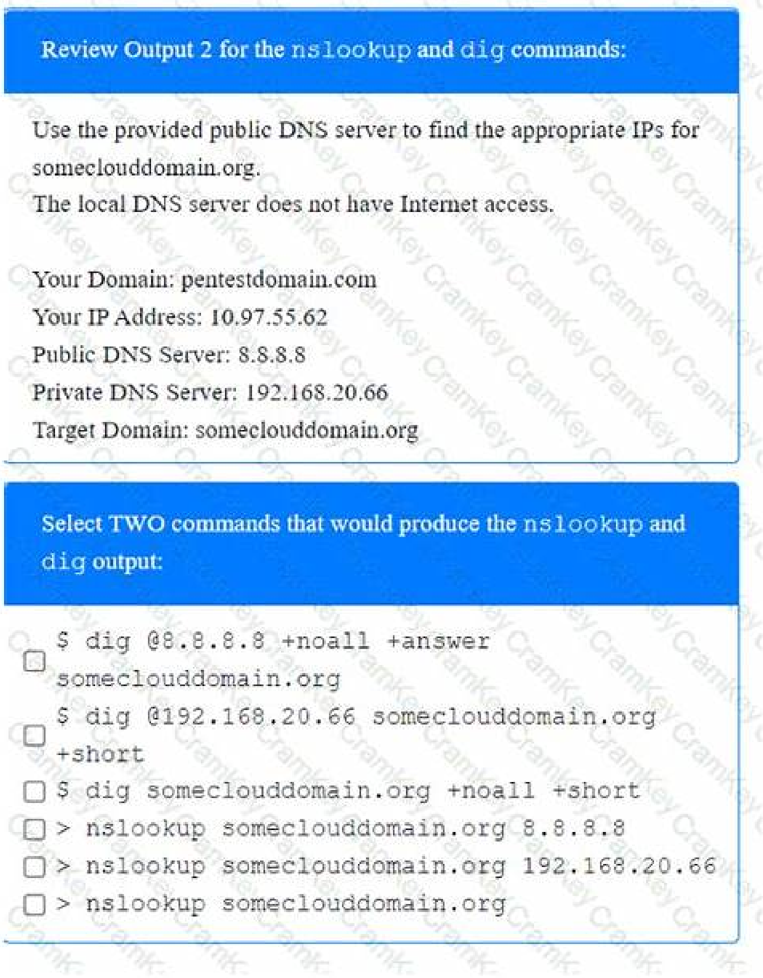
CompTIA PT0-003 Pdf Exam Dump - Dumps PT0-003 Questions



Review Output 2 for the `nslookup` and `dig` commands:

Use the provided public DNS server to find the appropriate IPs for someclouddomain.org.
The local DNS server does not have Internet access.

Your Domain: pentestdomain.com
Your IP Address: 10.97.55.62
Public DNS Server: 8.8.8.8
Private DNS Server: 192.168.20.66
Target Domain: someclouddomain.org

Select TWO commands that would produce the `nslookup` and `dig` output:

```
□ $ dig @8.8.8.8 +noall +answer
  someclouddomain.org
□ $ dig @192.168.20.66 someclouddomain.org
  +short
□ $ dig someclouddomain.org +noall +short
□ > nslookup someclouddomain.org 8.8.8.8
□ > nslookup someclouddomain.org 192.168.20.66
□ > nslookup someclouddomain.org
```

DOWNLOAD the newest TopExamCollection PT0-003 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1Hc0M5FEoZGdvCg1P6xXxmxMG4OJ3ZhK4

You can trust TopExamCollection PT0-003 exam questions and start this journey with complete peace of mind and satisfaction. The TopExamCollection PT0-003 practice questions are designed and verified by experienced and qualified PT0-003 exam experts. They work collectively and put their expertise to ensure the top standard of TopExamCollection CompTIA PT0-003 Exam Dumps. So we can say that with the TopExamCollection CompTIA PT0-003 exam questions, you will get everything that you need to learn, prepare and pass the difficult CompTIA PenTest+ Exam certification exam with good scores.

CompTIA PT0-003 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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 Pdf Exam Dump <<

Dumps PT0-003 Questions | Exam PT0-003 Overviews

Similarly, this desktop CompTIA PenTest+ Exam (PT0-003) practice exam software of TopExamCollection is compatible with all Windows-based computers. You need no internet connection for it to function. The Internet is only required at the time of product license validation. TopExamCollection provides 24/7 customer support to answer any of your queries or concerns regarding the CompTIA PenTest+ Exam (PT0-003) certification exam. They have a team of highly skilled and experienced professionals who have a thorough knowledge of the CompTIA PenTest+ Exam (PT0-003) exam questions and format.

CompTIA PenTest+ Exam Sample Questions (Q29-Q34):

NEW QUESTION # 29
Given the following script:
Which of the following BEST characterizes the function performed by lines 5 and 6?

- A. Performs a single DNS query for www.comptia.org and prints the raw data output
- B. Loops through variable b to count the results returned for the DNS query and prints that count to screen
- C. Prints each DNS query result already stored in variable b
- D. Retrieves the start-of-authority information for the zone on DNS server 10.10.10.10

Answer: C

Explanation:
The script is using the scapy library to perform a DNS query for www.comptia.org and store the response in variable b. Lines 5 and 6 are using a for loop to iterate over each answer in variable b and print its summary to the screen. This can help the penetration tester to view the DNS records returned by the query.

NEW QUESTION # 30
A client warns the assessment team that an ICS application is maintained by the manufacturer. Any tampering of the host could void the enterprise support terms of use. Which of the following techniques would be most effective to validate whether the application encrypts communications in transit?

- A. Requesting that certificate pinning be disabled
- B. Utilizing port mirroring on a firewall appliance
- C. Reconfiguring the application to use a proxy
- D. Installing packet capture software on the server

Answer: B

Explanation:

Using port mirroring on a firewall appliance is the safest and most non-intrusive way to validate if the application encrypts data in transit.
* Why Port Mirroring?
* Port mirroring (SPAN) enables traffic from the ICS system to be copied and sent to a monitoring device without affecting the host system.
* This avoids any tampering with the application or host, preserving enterprise support terms.
* Other Options:
* B (Installing packet capture software): Installing software on the server would violate the terms of use and tamper with the host.
* C (Reconfiguring the application): Reconfiguring the application to use a proxy would require modification, violating the terms of use.
* D (Requesting that certificate pinning be disabled): This would involve modifying the application configuration, which is against the terms of use.
CompTIA Pentest+ References:
* Domain 2.0 (Information Gathering and Vulnerability Identification)
* ICS and SCADA Security Guidelines

NEW QUESTION # 31
A penetration tester has found a web application that is running on a cloud virtual machine instance.
Vulnerability scans show a potential SSRF for the same application URL path with an injectable parameter.
Which of the following commands should the tester run to successfully test for secrets exposure exploitability?

- A. curl <url>?param=http://127.0.0.1/
- B. curl '<url>?param=http://127.0.0.1/etc/passwd'
- C. curl <url>?param=http://169.254.169.254/latest/meta-data/
- D. curl '<url>?param=<script>alert(1)<script>/'

Answer: C

Explanation:
In a cloud environment, testing for Server-Side Request Forgery (SSRF) vulnerabilities involves attempting to access metadata services. Here's why the specified command is appropriate:
* Accessing Cloud Metadata Service:
* URL:
http://169.254.169.254/latest/meta-data/ is a well-known endpoint in cloud environments (e.g., AWS) to access instance metadata.
* Purpose: By exploiting SSRF to access this URL, an attacker can retrieve sensitive information such as instance credentials and other metadata.
* Comparison with Other Commands:
* 127.0.0.1/etc/passwd: This is more about local file inclusion, not specific to cloud metadata.
* <script>alert(1)</script>: This tests for XSS, not SSRF.
* 127.0.0.1: This is a generic loopback address and does not specifically test for metadata access in a cloud environment.
Using curl <url>?param=http://169.254.169.254/latest/meta-data/
is the correct approach to test for SSRF vulnerabilities in cloud environments to potentially expose secrets.

NEW QUESTION # 32
A penetration tester runs the unshadow command on a machine. Which of the following tools will the tester most likely use NEXT?

- A. Hydra
- B. Cain and Abel
- C. John the Ripper
- D. Mimikatz

Answer: C

Explanation:
Reference: https://www.cyberciti.biz/faq/unix-linux-password-cracking-john-the-ripper/

NEW QUESTION # 33

A penetration tester is performing an assessment focused on attacking the authentication identity provider hosted within a cloud provider. During the reconnaissance phase, the tester finds that the system is using OpenID Connect with OAuth and has dynamic registration enabled. Which of the following attacks should the tester try first?

- A. A replay attack against the authentication flow in the system
- B. A brute-force attack against the authentication system
- C. A mask attack against the authentication system
- D. A password-spraying attack against the authentication system

Answer: A

Explanation:
OpenID Connect (OIDC) with OAuth allows applications to authenticate users using third-party identity providers (IdPs). If dynamic registration is enabled, attackers can abuse this feature to capture and replay authentication requests.
Replay attack (Option C):
Attackers capture legitimate authentication tokens and reuse them to impersonate users.
OIDC uses JWTs (JSON Web Tokens), which may not expire quickly, making replay attacks highly effective.
Reference: CompTIA PenTest+ PT0-003 Official Study Guide - "Attacking Identity Providers and OAuth" Incorrect options:
Option A (Password spraying): Effective against user accounts, but this attack targets authentication tokens.
Option B (Brute-force attack): Less effective against OAuth-based authentication since tokens replace passwords.
Option D (Mask attack): Related to password cracking, not OAuth authentication attacks.

NEW QUESTION # 34
......

TopExamCollection's study material is available in three different formats. The reason we have introduced three formats of the CompTIA PenTest+ Exam (PT0-003) practice material is to meet the learning needs of every student. Some candidates prefer PT0-003 practice exams and some want Real PT0-003 Questions due to a shortage of time. At TopExamCollection, we meet the needs of both types of aspirants. We have CompTIA PT0-003 PDF format, a web-based practice exam, and CompTIA PenTest+ Exam (PT0-003) desktop practice test software.

Dumps PT0-003 Questions: https://www.topexamcollection.com/PT0-003-vce-collection.html

2026 Latest TopExamCollection PT0-003 PDF Dumps and PT0-003 Exam Engine Free Share: https://drive.google.com/open?

id=1Hc0M5FEoZGdvCg1P6xXxmxMG4OJ3ZhK4