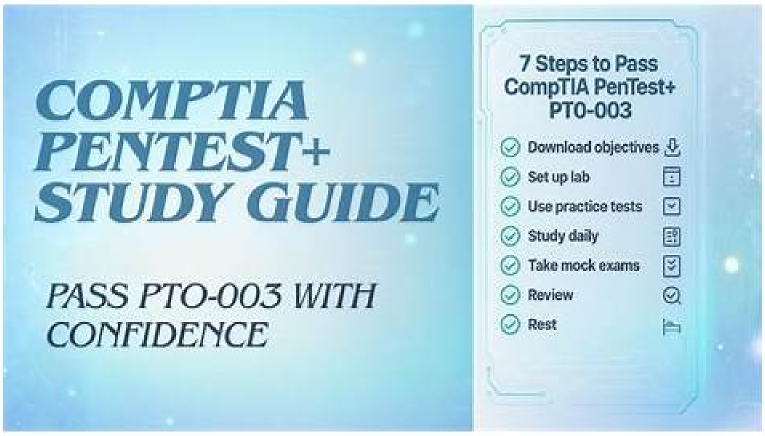
Study PT0-003 Center, New PT0-003 Test Papers


COMPTIA PENTEST+ STUDY GUIDE
PASS PTO-003 WITH CONFIDENCE
7 Steps to Pass CompTIA PenTest+ PT0-003
Download objectives
Set up lab
Use practice tests
Study daily
Take mock exams
Review
Rest

P.S. Free 2026 CompTIA PT0-003 dumps are available on Google Drive shared by PrepPDF: https://drive.google.com/open?id=1DOiSvpCDQQPWVDD-yoW7fc8ru5U5GNgb

The CompTIA PenTest+ Exam (PT0-003) certification exam is one of the top-rated career advancement certifications in the market. This CompTIA PenTest+ Exam (PT0-003) exam dumps have been inspiring beginners and experienced professionals since its beginning. There are several personal and professional benefits that you can gain after passing the CompTIA PT0-003 Exam. The validation of expertise, more career opportunities, salary enhancement, instant promotion, and membership of CompTIA certified professional community.

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	• 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	• 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 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.

>> Study PT0-003 Center <<

High-quality CompTIA Study PT0-003 Center offer you accurate New Test Papers | CompTIA PenTest+ Exam

If you study with our PT0-003 exam questions, you will have a 99% chance to pass the exam. Of course, you don't have to buy any other study materials. Our PT0-003 exam questions can satisfy all your learning needs. During this time, you must really be learning. If you just put PT0-003 Real Exam in front of them and didn't look at them, then we have no way. Our PT0-003 exam questions want to work with you to help you achieve your dreams.

CompTIA PenTest+ Exam Sample Questions (Q35-Q40):

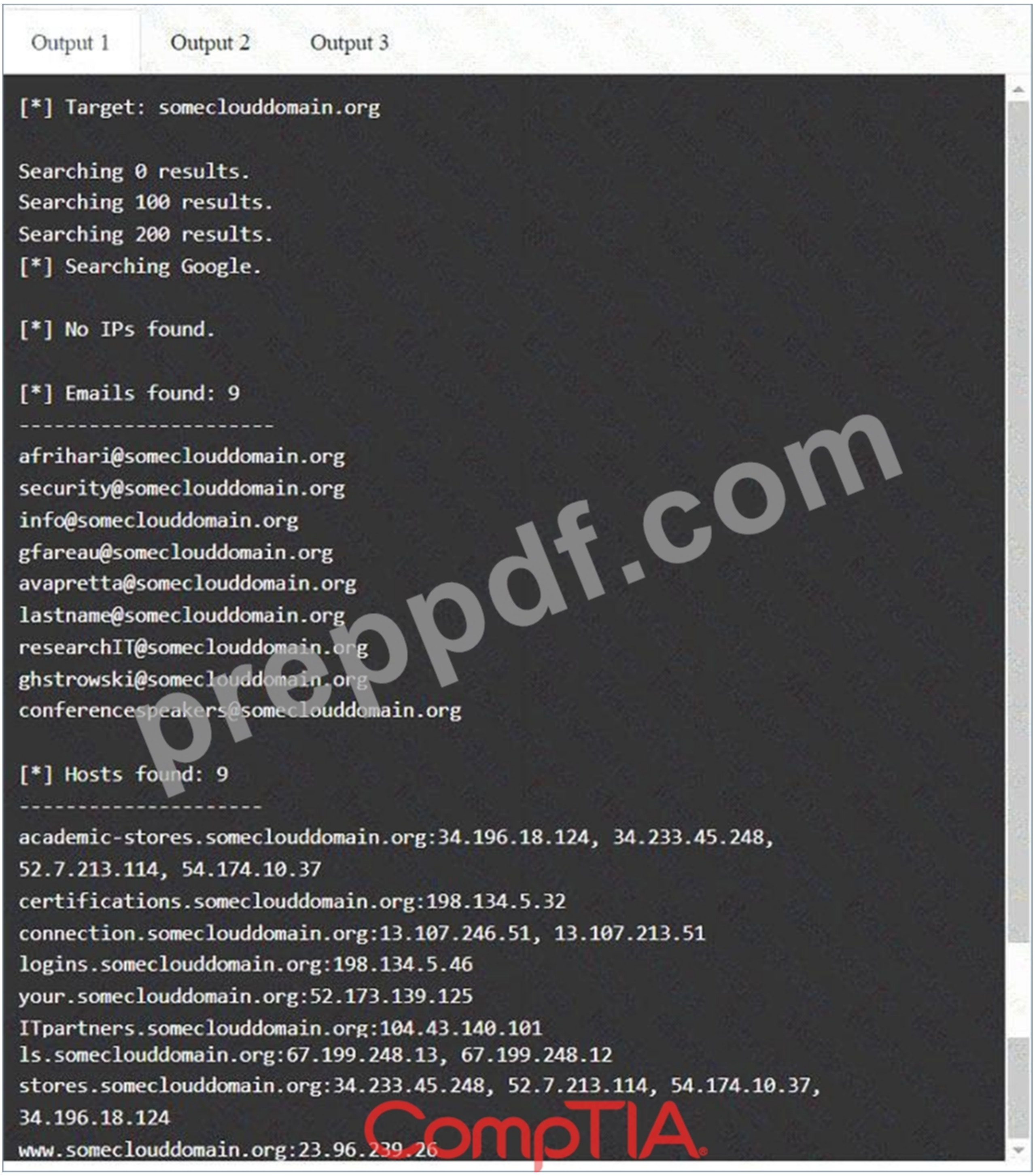
NEW QUESTION # 35
A penetration tester is performing a cloud-based penetration test against a company. Stakeholders have indicated the priority is to see if the tester can get into privileged systems that are not directly accessible from the internet. Given the following scanner information:
* Server-side request forgery (SSRF) vulnerability in test.comptia.org
* Reflected cross-site scripting (XSS) vulnerability in test2.comptia.org
* Publicly accessible storage system named static_comptia_assets
* SSH port 22 open to the internet on test3.comptia.org
* Open redirect vulnerability in test4.comptia.org
Which of the following attack paths should the tester prioritize first?

- A. Perform a full dictionary brute-force attack against the open SSH service using Hydra.
- B. Synchronize all the information from the public bucket and scan it with Trufflehog.
- C. Run Pacu to enumerate permissions and roles within the cloud-based systems.
- D. Leverage the SSRF to gain access to credentials from the metadata service.
- E. Use the reflected cross-site scripting attack within a phishing campaign to attack administrators.

Answer: D

Explanation:
* Leverage SSRF for Metadata Access:
* Server-side request forgery (SSRF) vulnerabilities allow attackers to force a server to send requests to internal resources. In cloud environments, SSRF can often be used to access the metadata service (e.g., AWS EC2 metadata) to retrieve credentials for cloud services.
* Once credentials are obtained, they can be used to access privileged systems that are not directly accessible from the internet.
* Why Not Other Options?
* A (Public bucket): Analyzing the bucket for sensitive data is useful but does not directly lead to privileged system access.
* B (Pacu): Pacu is used for AWS exploitation but requires credentials or misconfigured roles.
SSRF can provide the credentials needed to run Pacu effectively.
* C (SSH brute force): Brute-forcing SSH is noisy and inefficient. Privileged systems are likely better protected than SSH open to the internet.
* D (Phishing via XSS): This is a longer-term attack and less direct compared to leveraging SSRF.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* SSRF Exploitation and Cloud Metadata Access Techniques

NEW QUESTION # 36
A penetration tester has been provided with only the public domain name and must enumerate additional information for the public-facing assets.
INSTRUCTIONS
Select the appropriate answer(s), given the output from each section.
Output 1



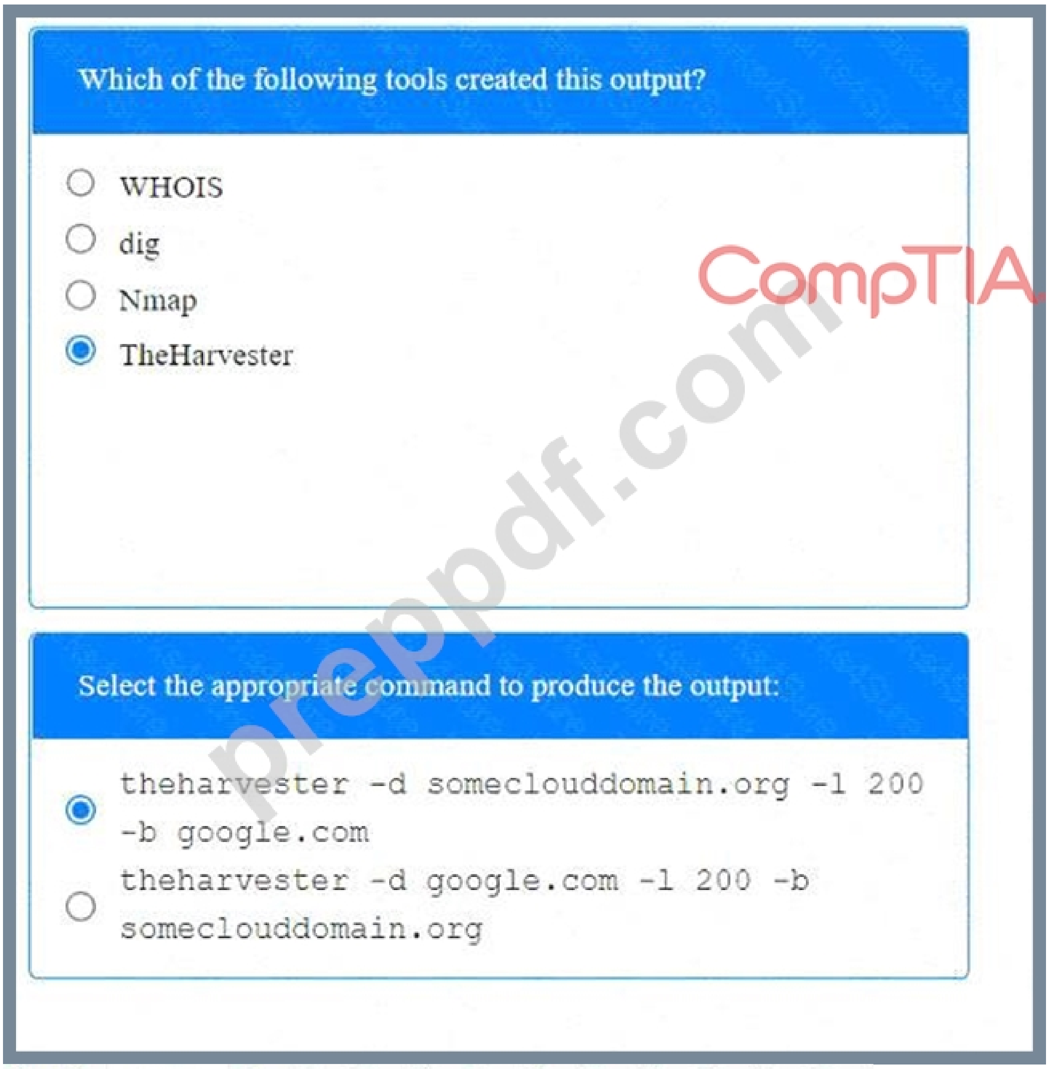
```
[*] Target: someclouddomain.org

Searching 0 results.
Searching 100 results.
Searching 200 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 9
----------------------
afrihari@someclouddomain.org
security@someclouddomain.org
info@someclouddomain.org
gfareau@someclouddomain.org
avapretta@someclouddomain.org
lastname@someclouddomain.org
researchIT@someclouddomain.org
ghstrowski@someclouddomain.org
conferencespeakers@someclouddomain.org

[*] Hosts found: 9
---------------------
academic-stores.someclouddomain.org:34.196.18.124, 34.233.45.248,
52.7.213.114, 54.174.10.37
certifications.someclouddomain.org:198.134.5.32
connection.someclouddomain.org:13.107.246.51, 13.107.213.51
logins.someclouddomain.org:198.134.5.46
your.someclouddomain.org:52.173.139.125
ITpartners.someclouddomain.org:104.43.140.101
ls.someclouddomain.org:67.199.248.13, 67.199.248.12
stores.someclouddomain.org:34.233.45.248, 52.7.213.114, 54.174.10.37,
34.196.18.124
www.someclouddomain.org:23.96.239.26
```



Which of the following tools created this output?

○ WHOIS

○ dig

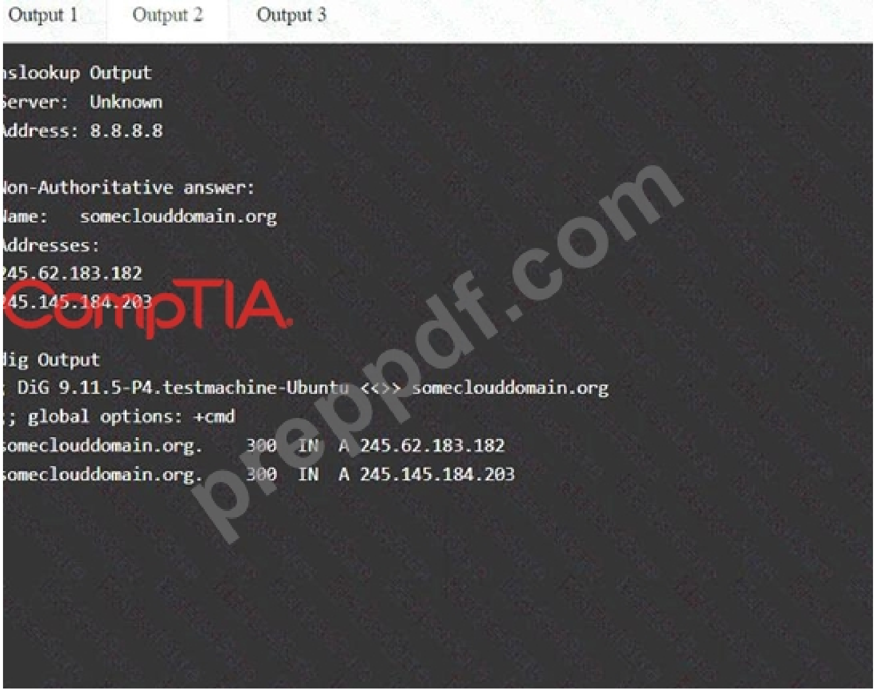
○ Nmap

● TheHarvester

Select the appropriate command to produce the output:

● `theharvester -d someclouddomain.org -l 200 -b google.com`

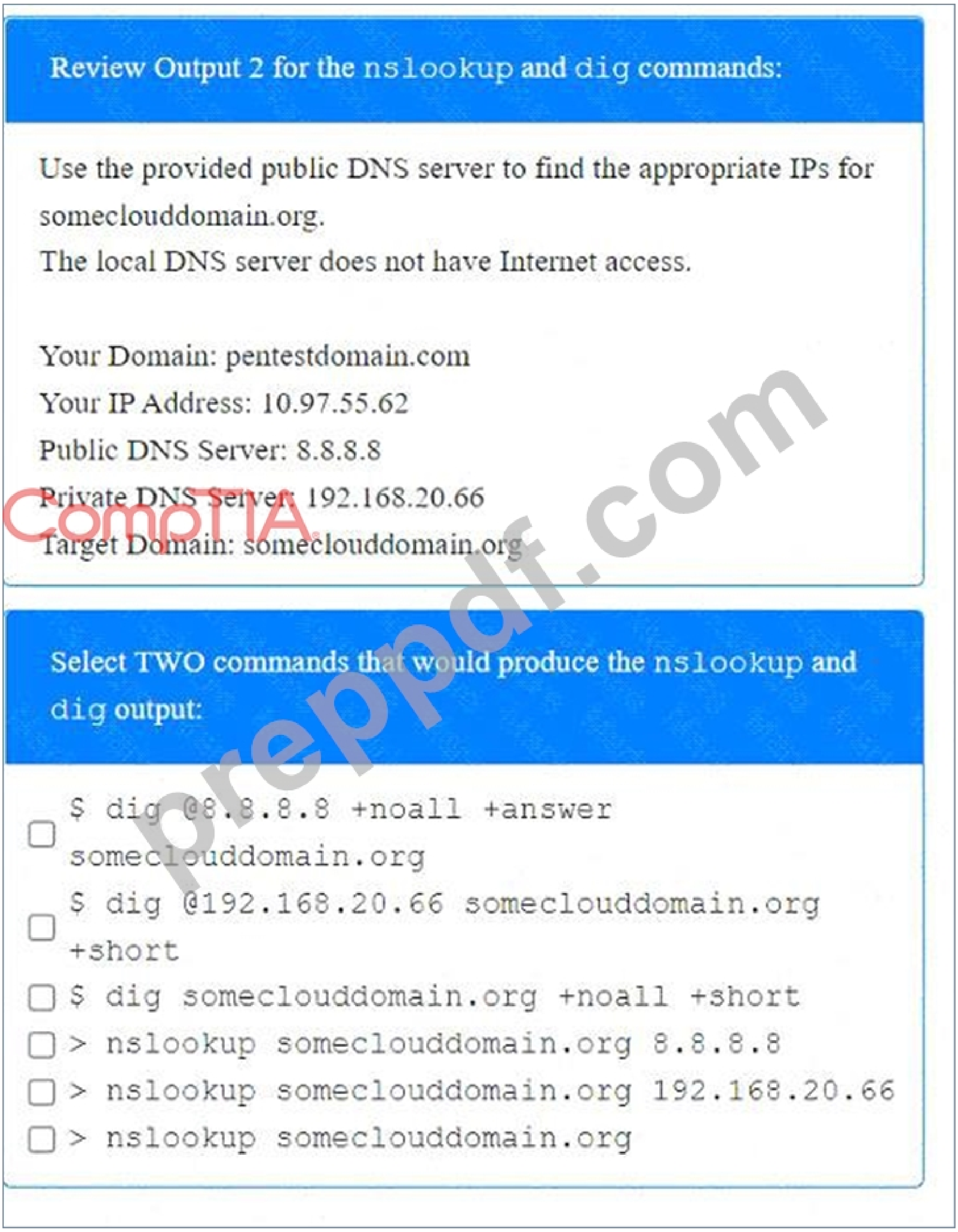
○ `theharvester -d google.com -l 200 -b someclouddomain.org`



```
slookup Output
erver:  Unknown
ddress: 8.8.8.8

on-Authoritative answer:
ame:    someclouddomain.org
ddresses:
45.62.183.182
45.145.184.203

ig Output
 DiG 9.11.5-P4.testmachine-Ubuntu <<>> someclouddomain.org
; global options: +cmd
omeclouddomain.org.     300  IN  A 245.62.183.182
omeclouddomain.org.     300  IN  A 245.145.184.203
```



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

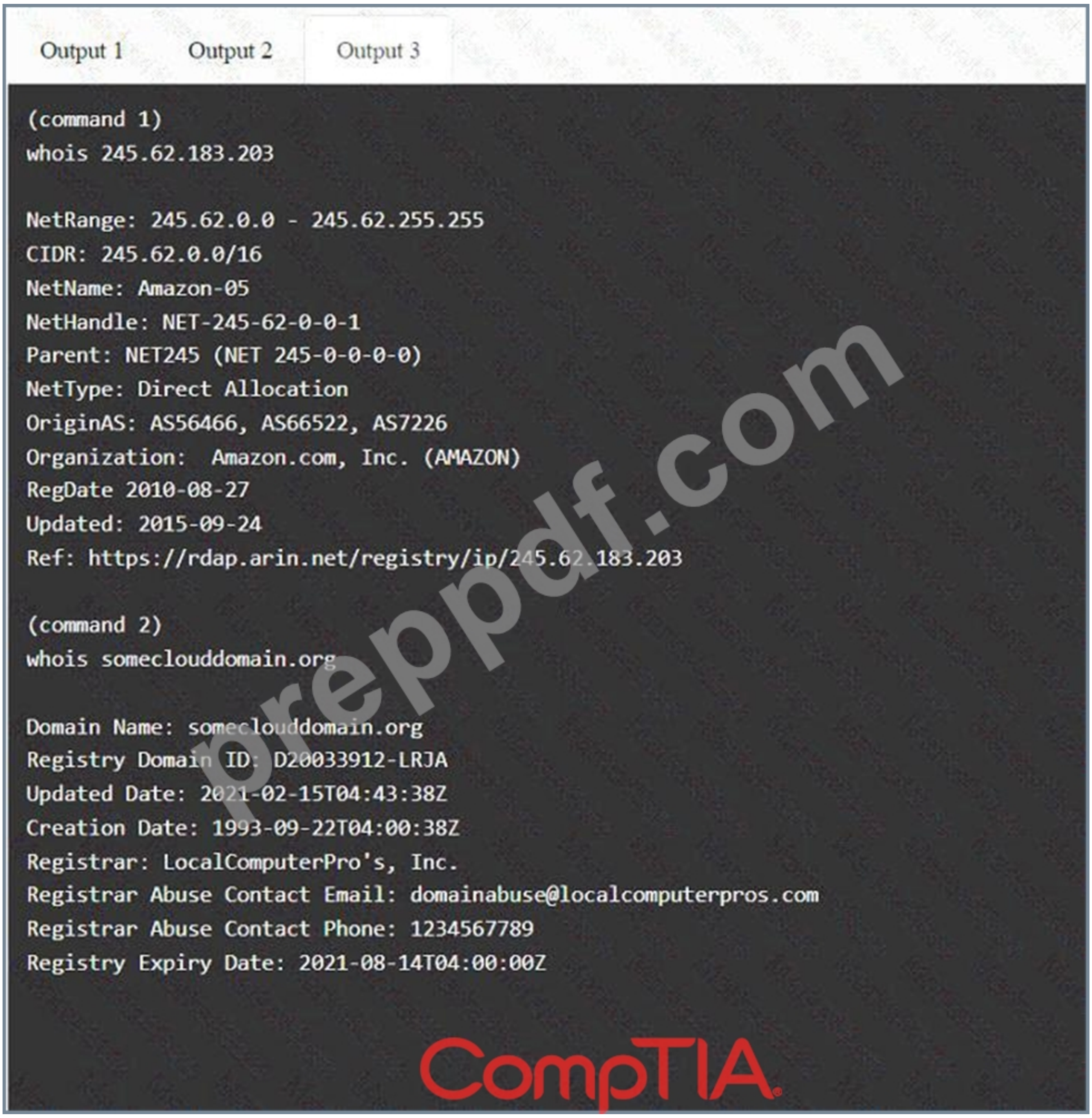
Public DNS Server: 8.8.8.8

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`

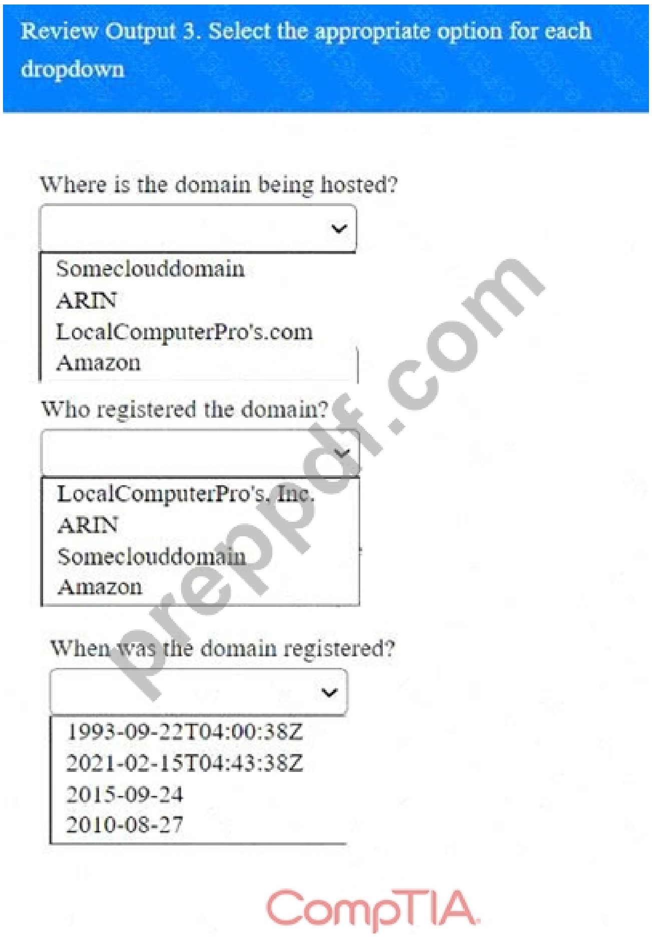


```
(command 1)
whois 245.62.183.203

NetRange: 245.62.0.0 - 245.62.255.255
CIDR: 245.62.0.0/16
NetName: Amazon-05
NetHandle: NET-245-62-0-0-1
Parent: NET245 (NET 245-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS56466, AS66522, AS7226
Organization:  Amazon.com, Inc. (AMAZON)
RegDate 2010-08-27
Updated: 2015-09-24
Ref: https://rdap.arin.net/registry/ip/245.62.183.203

(command 2)
whois someclouddomain.org

Domain Name: someclouddomain.org
Registry Domain ID: D20033912-LRJA
Updated Date: 2021-02-15T04:43:38Z
Creation Date: 1993-09-22T04:00:38Z
Registrar: LocalComputerPro's, Inc.
Registrar Abuse Contact Email: domainabuse@localcomputerpros.com
Registrar Abuse Contact Phone: 1234567789
Registry Expiry Date: 2021-08-14T04:00:00Z
```



Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

- Someclouddomain
- ARIN
- LocalComputerPro's.com
- Amazon

Who registered the domain?

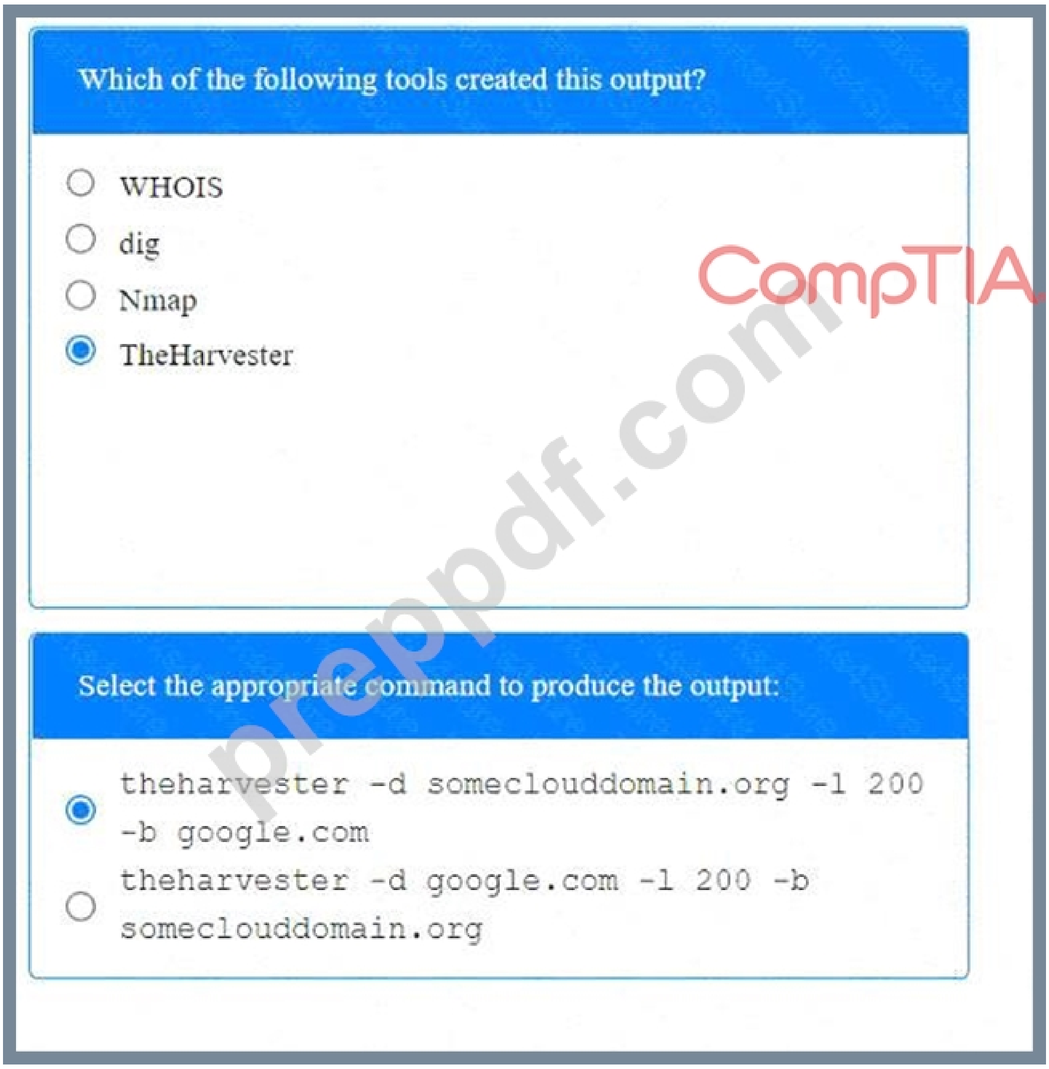
- LocalComputerPro's, Inc.
- ARIN
- Someclouddomain
- Amazon

When was the domain registered?

- 1993-09-22T04:00:38Z
- 2021-02-15T04:43:38Z
- 2015-09-24
- 2010-08-27

Answer:

Explanation:
See all the solutions below in Explanation.
Explanation:
A screenshot of a computer Description automatically generated



Which of the following tools created this output?

○ WHOIS

○ dig

○ Nmap

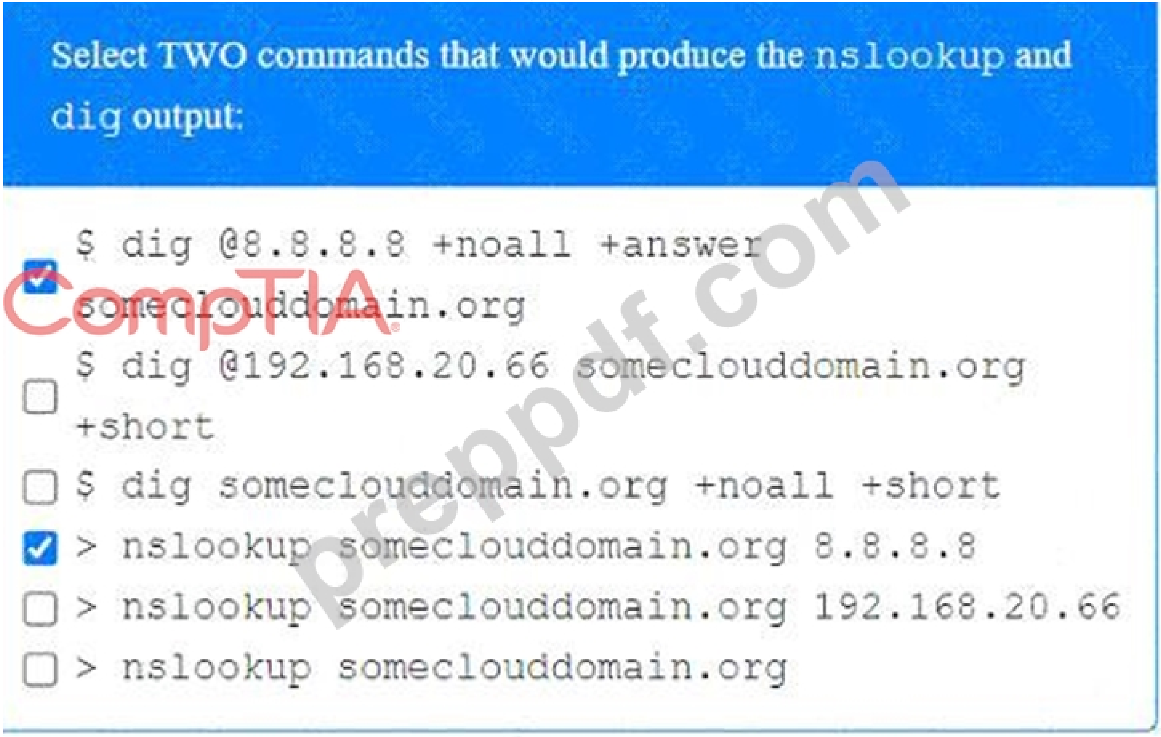
● TheHarvester

Select the appropriate command to produce the output:

● `theharvester -d someclouddomain.org -l 200 -b google.com`

○ `theharvester -d google.com -l 200 -b someclouddomain.org`

A screenshot of a computer Description automatically generated



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`

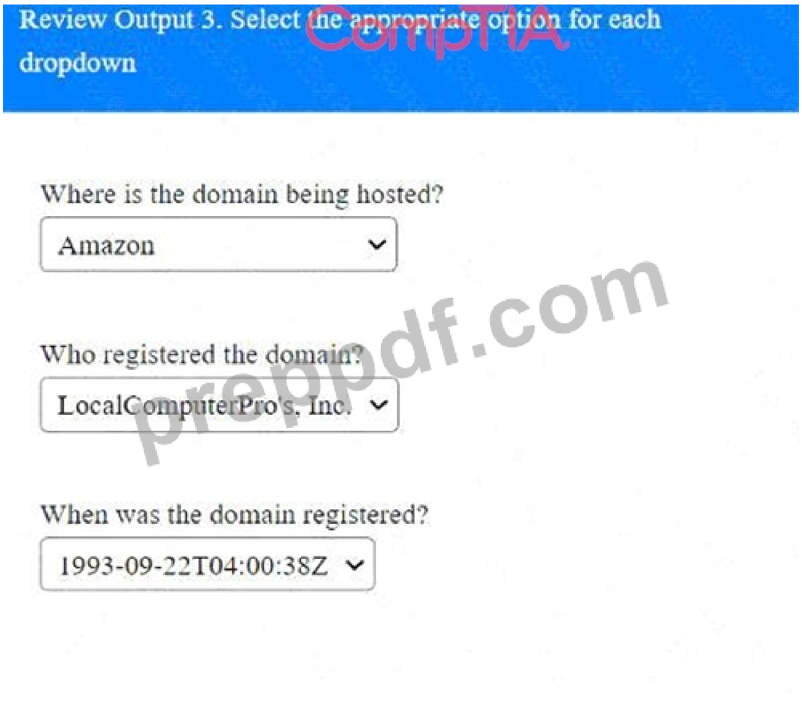
□ `$ dig someclouddomain.org +noall +short`

☑ `> nslookup someclouddomain.org 8.8.8.8`

□ `> nslookup someclouddomain.org 192.168.20.66`

□ `> nslookup someclouddomain.org`

A screenshot of a computer Description automatically generated



Review Output 3. Select the appropriate option for each dropdown

Where is the domain being hosted?

Amazon

Who registered the domain?

LocalComputerPro's, Inc.

When was the domain registered?

1993-09-22T04:00:38Z

NEW QUESTION # 37

A penetration tester wants to maintain access to a compromised system after a reboot. 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 persistence after a reboot, the tester needs a method that automatically restarts when the system reboots.

* Option A (Reverse shell) #: Reverse shells do not persist after a reboot unless paired with scheduled tasks or registry modifications.

* Option B (Process injection) #: Injecting into a process is temporary-once the system reboots, the injected process is gone.

* Option C (Scheduled task) #: Correct.

* A scheduled task can execute malware, reverse shells, or scripts on system startup, ensuring persistence.

* Example:

```
schtasks /create /sc onlogon /tn "SystemUpdate" /tr "C:\malicious.exe"
```

* Option D (Credential dumping) #: While useful for privilege escalation, it does not provide persistence.

# Reference: CompTIA PenTest+ PT0-003 Official Guide - Persistence Techniques

NEW QUESTION # 38

A client recently hired a penetration testing firm to conduct an assessment of their consumer-facing web application. Several days into the assessment, the client's networking team observes a substantial increase in DNS traffic. Which of the following would most likely explain the increase in DNS traffic?

- A. HTML scrapping
- B. URL spidering
- C. Covert data exfiltration
- D. DoS attack

Answer: C

Explanation:

* Covert Data Exfiltration:
* DNS traffic can be leveraged for covert data exfiltration because it is often allowed through firewalls and not heavily monitored.
* Tools or techniques for DNS tunneling encode sensitive information into DNS queries or responses, resulting in an observable increase in DNS traffic.
* Why Not Other Options?
* B (URL spidering): This increases HTTP traffic, not DNS traffic.
* C (HTML scrapping): Involves downloading website content, which primarily uses HTTP or HTTPS.
* D (DoS attack): A DNS-based DoS attack would likely involve query floods from many sources, not necessarily related to the observed behavior in a penetration test.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)
* Covert Communication Techniques and DNS Tunneling

NEW QUESTION # 39

A penetration tester is researching a path to escalate privileges. While enumerating current user privileges, the tester observes the following output:

mathematica

Copy code

```
SeAssignPrimaryTokenPrivilege Disabled
SeIncreaseQuotaPrivilege Disabled
SeChangeNotifyPrivilege Enabled
SeManageVolumePrivilege Enabled
SeImpersonatePrivilege Enabled
SeCreateGlobalPrivilege Enabled
SeIncreaseWorkingSetPrivilege Disabled
```

Which of the following privileges should the tester use to achieve the goal?

- A. SeChangeNotifyPrivilege
- B. SeImpersonatePrivilege
- C. SeCreateGlobalPrivilege
- D. SeManageVolumePrivilege

Answer: B

Explanation:
* ImpersonatePrivilege for Escalation:
* The SeImpersonatePrivilege allows a process to impersonate a user after authentication. This is a common privilege used in token stealing or pass-the-token attacks to escalate privileges.
* Exploits like Rotten Potato and Juicy Potato specifically target this privilege to elevate access to SYSTEM.
* Why Not Other Options?
* B (SeCreateGlobalPrivilege): This allows processes to create global objects but does not directly enable privilege escalation.
* C (SeChangeNotifyPrivilege): This is related to bypassing traverse checking and does not facilitate privilege escalation.
* D (SeManageVolumePrivilege): This allows volume maintenance but is not relevant for privilege escalation.
CompTIA Pentest+ References:
* Domain 3.0 (Attacks and Exploits)

NEW QUESTION # 40

......

By unremitting effort to improve the accuracy and being studious of the PT0-003 real questions all these years, our experts remain unpretentious attitude towards our PT0-003 practice materials all the time. They are unsuspecting experts who you can count on. Without unintelligible content within our PT0-003 Study Tool, all questions of the exam are based on their professional experience in this industry. Besides, they made three versions for your reference, the PDF, APP and Online software version.

New PT0-003 Test Papers: https://www.preppdf.com/CompTIA/PT0-003-prepaway-exam-dumps.html

- Online PT0-003 Tests □ Valid PT0-003 Exam Pdf □ PT0-003 Exam Bible □ Simply search for ➽ PT0-003 □ for free download on □ www.troytecdumps.com □ □PT0-003 Free Updates
- Test PT0-003 Dumps.zip □ Exam Dumps PT0-003 Demo □ Test PT0-003 Topics Pdf □ 「www.pdfvce.com」 is

best website to obtain □ PT0-003 □ for free download □Valid PT0-003 Exam Pdf

- PT0-003 Free Updates □ PT0-003 New Test Camp □ Latest PT0-003 Exam Topics □ Easily obtain [PT0-003] for free download through 「 www.practicevce.com 」 ℹLatest PT0-003 Exam Topics
- CompTIA PT0-003 Latest Dumps - Affordable Price and Free Updates □ Easily obtain ✔ PT0-003 □✔□ for free download through □ www.pdfvce.com □ □Valid Test PT0-003 Tips
- Test PT0-003 Dumps.zip □ Latest PT0-003 Dumps □ PT0-003 Valid Exam Topics ☢ Easily obtain ➠ PT0-003 □ for free download through ➥ www.exam4labs.com □ □Reliable PT0-003 Exam Cost
- Latest PT0-003 Exam Vce □ Interactive PT0-003 EBook □ Interactive PT0-003 EBook □ Search for ➥ PT0-003 □ and download exam materials for free through { www.pdfvce.com } □Latest PT0-003 Exam Vce
- Free PDF Quiz 2026 CompTIA PT0-003: CompTIA PenTest+ Exam – Efficient Study Center □ Easily obtain ▷ PT0-003 ◁ for free download through ➤ www.easy4engine.com □ □PT0-003 Free Updates
- Latest PT0-003 Exam Vce □ Reliable PT0-003 Exam Test □ Test PT0-003 Dumps.zip □ Easily obtain （ PT0-003 ） for free download through ➤ www.pdfvce.com □ □Regualer PT0-003 Update
- PT0-003 Online Tests □ PT0-003 Exam Bible □ PT0-003 Exam Bible □ Immediately open ✔ www.dumpsquestion.com □✔□ and search for ➽ PT0-003 □ to obtain a free download ☂Latest PT0-003 Exam Topics
- PT0-003 Free Updates □ Latest PT0-003 Exam Topics □ PT0-003 Online Tests □ Enter □ www.pdfvce.com □ and search for ▶ PT0-003 ◀ to download for free ➡Latest PT0-003 Dumps
- CompTIA - PT0-003 - Unparalleled Study CompTIA PenTest+ Exam Center !! Download ▶ PT0-003 ◀ for free by simply searching on ✔ www.examdiscuss.com □✔□ □Latest PT0-003 Exam Vce
- www.stes.tyc.edu.tw, paidforarticles.in, academia.thisismusic.ec, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, shortcourses.russellcollege.edu.au, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

BTW, DOWNLOAD part of PrepPDF PT0-003 dumps from Cloud Storage: https://drive.google.com/open?id=1DOiSvpCDQQPWVDD-yoW7fc8ru5U5GNgb