PT0-003 Q&As

CompTIA PenTest+

Pass CompTIA PT0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/pt0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A compliance-based penetration test is primarily concerned with:

A. obtaining Pll from the protected network.

B. bypassing protection on edge devices.

C. determining the efficacy of a specific set of security standards.

D. obtaining specific information from the protected network.

Correct Answer: C

QUESTION 2

A penetration tester gains initial access to a target system by exploiting a recent RCE vulnerability. The patch for the vulnerability will be deployed at the end of the week. Which of the following utilities would allow the tester to reenter the system remotely after the patch has been deployed? (Select two).

A. schtasks.exe

B. rundll.exe

C. cmd.exe

D. chgusr.exe

E. sc.exe

F. netsh.exe

Correct Answer: AE

To reenter the system remotely after the patch for the recently exploited RCE vulnerability has been deployed, the penetration tester can use schtasks.exe and sc.exe.

schtasks.exe:

schtasks /create /tn "Backdoor" /tr "C:\path\to\backdoor.exe" /sc daily /ru SYSTEM sc.exe:

sc create backdoor binPath= "C:\path\to\backdoor.exe" start= auto Other Utilities:

Pentest References:

Post-Exploitation: Establishing persistence is crucial to maintaining access after initial exploitation.

Windows Tools: Understanding how to leverage built-in Windows tools like schtasks.exe and sc.exe to create backdoors that persist through reboots and patches. By using schtasks.exe and sc.exe, the penetration tester can set up persistent

mechanisms that will allow reentry into the system even after the patch is applied.

QUESTION 3

Which of the following is a term used to describe a situation in which a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee?

A. Badge cloning

B. Shoulder surfing

C. Tailgating

D. Site survey

Correct Answer: C

Tailgating is the term used to describe a situation where a penetration tester bypasses physical access controls and gains access to a facility by entering at the same time as an employee.

Tailgating:

Physical Security:

Pentest References:

By understanding and using tailgating, penetration testers can evaluate the effectiveness of an organization\\'s physical security measures and identify potential vulnerabilities that could be exploited by malicious actors.

QUESTION 4

A penetration tester ran a simple Python-based scanner. The following is a snippet of the code: Which of the following BEST describes why this script triggered a `probable port scan` alert in the organization\\'s IDS?

```
…
<LINE NUM.>
<01> portlist: list[int] = [*range(1, 1025)]
<02> try;
<03>    port: object
<04>    resultList: list[Any] = []
<05>    for port in portList:
<06>      sock = socket.socket (socket.AF_INET, socket.SOCK_STREAM)
<07>      sock.settimeout(20)
<08>      result = sock.connect_ex((remoteSvr, port))
<09>      if result == 0:
<10>           resultList.append(port)
<11>      sock.close()
…
```

A. sock.settimeout(20) on line 7 caused each next socket to be created every 20 milliseconds.

B. *range(1, 1025) on line 1 populated the portList list in numerical order.

C. Line 6 uses socket.SOCK_STREAM instead of socket.SOCK_DGRAM

D. The remoteSvr variable has neither been type-hinted nor initialized.

Correct Answer: B

Port randomization is widely used in port scanners. By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons) https://nmap.org/book/man-portspecification.html

QUESTION 5

In a file stored in an unprotected source code repository, a penetration tester discovers the following line of code:

sshpass -p donotchange ssh admin@192.168.6.14

Which of the following should the tester attempt to do next to take advantage of this information? (Select two).

A. Use Nmap to identify all the SSH systems active on the network.

B. Take a screen capture of the source code repository for documentation purposes.

C. Investigate to find whether other files containing embedded passwords are in the code repository.

D. Confirm whether the server 192.168.6.14 is up by sending ICMP probes.

E. Run a password-spraying attack with Hydra against all the SSH servers.

F. Use an external exploit through Metasploit to compromise host 192.168.6.14.

Correct Answer: BC

When a penetration tester discovers hard-coded credentials in a file within an unprotected source code repository, the next steps should focus on documentation and further investigation to identify additional security issues.

Taking a Screen Capture (Option B):

Investigating for Other Embedded Passwords (Option C):

Pentest References:

Initial Discovery: Discovering hard-coded credentials often occurs during source code review or automated scanning of repositories. Documentation: Keeping detailed records of all findings is a critical part of the penetration testing process.

This ensures that all discovered vulnerabilities are reported accurately and comprehensively.

Further Investigation: After finding a hard-coded credential, it is best practice to look for other security issues within the same repository. This might include other credentials, API keys, or sensitive information.

Steps to Perform:

Take a Screen Capture:

Investigate Further:

grep -r \\'password\\' /path/to/repository

uk.co.certification.simulator.questionpool.PList@2fe88cb7 trufflehog --regex --entropy=True /path/to/repository By documenting the finding and investigating further, the penetration tester ensures a comprehensive assessment of the

repository, identifying and mitigating potential security risks effectively.