IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **PT0-001**

Title : CompTIA PenTest+ Certification Exam

Version : DEMO

1.A penetration tester has successfully exploited a Windows host with low privileges and found directories with the following permissions:

```
> C:\folder
Everyone: (OI) (CI) (F)
BUILTIN\Administrators: (I) (F)
NT AUTHORITY\SYSTEM: (I) (F)
BUILTIN\Users: (I) (OI) (CI) (RX)
NT AUTHOTITY\Authenticated Users: (I) (M)
> C:\folder\software.exe
Everyone: (I) (F)
BUILTIN\Administrators: (I) (F)
NT AUTHORITY\SYSTEM: (I) (F)
BUILTIN\Users: (I) (RX)
NT AUTHORITY\Authenticated Users: (I) (M)
```

F	Full access
M	Modify access
RX	Read and execute access
OI	Object inherit
CI	Container inherit

Which of the following should be performed to escalate the privileges?

A. Kerberoasting

B. Retrieval of the SAM database

C. Migration of the shell to another process

D. Writable services

Answer: C

Explanation:

Reference: https://book.hacktricks.xyz/windows/windows-local-privilege-escalation

2.A security team is switching firewall vendors. The director of security wants to scope a penetration test to satisfy requirements to perform the test after major architectural changes.

Which of the following is the BEST way to approach the project?

A. Design a penetration test approach, focusing on publicly released firewall DoS vulnerabilities.

B. Review the firewall configuration, followed by a targeted attack by a read team.

C. Perform a discovery scan to identify changes in the network.

D. Focus on an objective-based approach to assess network assets with a red team.

Answer: D

3.Which of the following commands starts the Metasploit database?

A. msfconsole

B. workspace

C. msfvenom

D. db_init

E. db_connect

Answer: A

Explanation:
References: https://www.offensive-security.com/metasploit-unleashed/msfconsole/

4.A penetration tester delivers a web application vulnerability scan report to a client. The penetration tester rates a vulnerability as medium severity. The same vulnerability was reported as a critical severity finding on the previous report.
Which of the following is the MOST likely reason for the reduced severity?
A. The client has applied a hot fix without updating the version.
B. The threat landscape has significantly changed.
C. The client has updated their codebase with new features.
D. Thera are currently no known exploits for this vulnerability.
Answer: A

5.An internal network penetration test is conducted against a network that is protected by an unknown NAC system In an effort to bypass the NAC restrictions the penetration tester spoofs the MAC address and hostname of an authorized system.
Which of the following devices if impersonated would be MOST likely to provide the tester with network access?
A. Network-attached printer
B. Power-over-Ethernet injector
C. User workstation
D. Wireless router
Answer: A