PT0-001$^{\text{Q\&As}}$

CompTIA PenTest+ Exam

Pass CompTIA PT0-001 Exam with 100% Guarantee

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

https://www.geekcert.com/pt0-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An assessor begins an internal security test of the Windows domain internal.comptia.net. The assessor is given network access via DHCP, but is not given any network maps or target IP addresses. Which of the following commands can the assessor use to find any likely Windows domain controllers?

A. dig -q any _kerberos._tcp.internal.comptia.net

B. dig -q any _lanman._tcp.internal.comptia.net

C. dig -q any _ntlm._tcp.internal.comptia.net

D. dig -q any _smtp._tcp.internal.comptia.net

Correct Answer: A

QUESTION 2

A penetration tester reviews the scan results of a web application. Which of the following vulnerabilities is MOST critical and should be prioritized for exploitation?

A. Stored XSS

B. Fill path disclosure

C. Expired certificate

D. Clickjacking

Correct Answer: A

References https://www.owasp.org/index.php/Top_10_2010-A2-Cross- Site_Scripting_(XSS)

QUESTION 3

A penetration tester wants to check manually if a “ghost” vulnerability exists in a system. Which of the following methods is the correct way to validate the vulnerability?

A. Download the GHOST file to a Linux system and compile

gcc -o GHOST

test i:

./GHOST

B. Download the GHOST file to a Windows system and compile

gcc -o GHOST GHOST.c

test i:

./GHOST

C. Download the GHOST file to a Linux system and compile

gcc -o GHOST GHOST.c

test i:

./GHOST

D. Download the GHOST file to a Windows system and compile

gcc -o GHOST

test i:

./GHOST

Correct Answer: C

QUESTION 4

A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack Which of the following remediation steps should be recommended? (Select THREE)

A. Mandate all employees take security awareness training

B. Implement two-factor authentication for remote access

C. Install an intrusion prevention system

D. Increase password complexity requirements

E. Install a security information event monitoring solution.

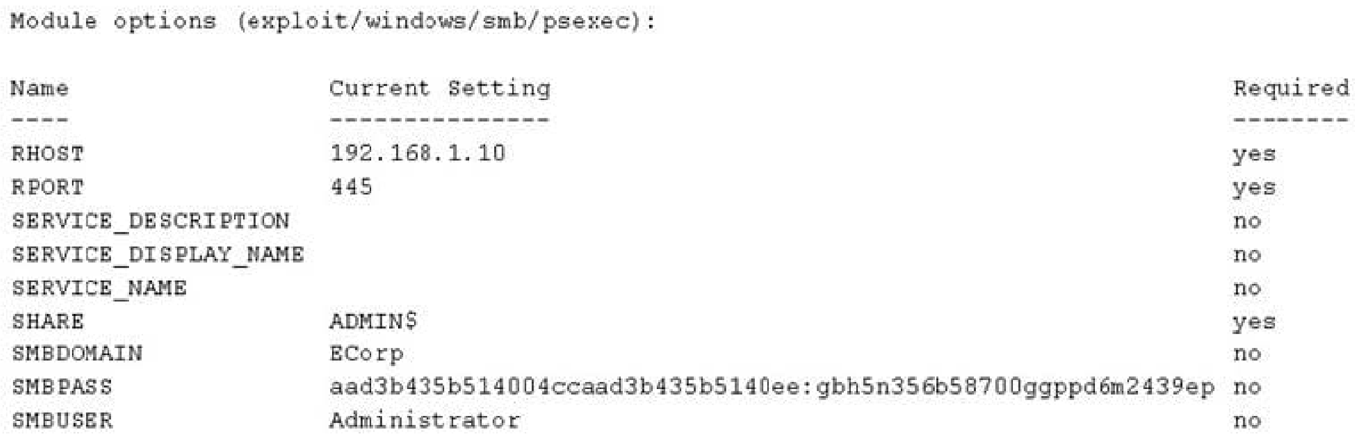
F. Prevent members of the IT department from interactively logging in as administrators

G. Upgrade the cipher suite used for the VPN solution

Correct Answer: BCG

QUESTION 5

A security consultant is trying to attack a device with a previously identified user account.



```
Module options (exploit/windows/smb/psexec):

Name                  Current Setting                                              Required
----                  ---------------                                              --------
RHOST                 192.168.1.10                                                 yes
RPORT                 445                                                          yes
SERVICE_DESCRIPTION                                                                no
SERVICE_DISPLAY_NAME                                                               no
SERVICE_NAME                                                                       no
SHARE                 ADMIN$                                                       yes
SMBDOMAIN             ECorp                                                        no
SMBPASS               aad3b435b514004ccaad3b435b5140ee:gbh5n356b58700ggppd6m2439ep no
SMBUSER               Administrator                                                no
```

Which of the following types of attacks is being executed?

A. Credential dump attack

B. DLL injection attack

C. Reverse shell attack

D. Pass the hash attack

Correct Answer: D

PT0-001 PDF Dumps PT0-001 VCE Dumps PT0-001 Practice Test