PT0-002$^{Q\&As}$

CompTIA PenTest+ Certification Exam

QUESTION 1

During a vulnerability scanning phase, a penetration tester wants to execute an Nmap scan using custom NSE scripts stored in the following folder:

/home/user/scripts

Which of the following commands should the penetration tester use to perform this scan?

A. nmap resume "not intrusive"

B. nmap script default safe

C. nmap script /home/user/scripts

D. nmap -load /home/user/scripts

Correct Answer: C

The Nmap command in the question aims to use custom NSE scripts stored in a specific folder. The correct syntax for this option is to use the script argument followed by the path to the folder. The other commands are either invalid, use the wrong argument, or do not specify the folder path. References: Best PenTest+ certification study resources and training materials, CompTIA PenTest+ PT0-002 Cert Guide, 101 Labs -- CompTIA PenTest+: Hands-on Labs for the PT0-002 Exam

QUESTION 2

A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company\\'s privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?

A. OpenVAS

B. Nikto

C. SQLmap

D. Nessus

Correct Answer: C

Reference: https://phoenixnap.com/blog/best-penetration-testing-tools

QUESTION 3

Which of the following describes the reason why a penetration tester would run the command sdelete mimikatz. * on a Windows server that the tester compromised?

A. To remove hash-cracking registry entries

B. To remove the tester-created Mimikatz account

C. To remove tools from the server

D. To remove a reverse shell from the system

Correct Answer: B

QUESTION 4

A penetration tester has gained access to the Chief Executive Officer\\'s (CEO\\'s) internal, corporate email. The next objective is to gain access to the network. Which of the following methods will MOST likely work?

A. Try to obtain the private key used for S/MIME from the CEO\\'s account.

B. Send an email from the CEO\\'s account, requesting a new account.

C. Move laterally from the mail server to the domain controller.

D. Attempt to escalate privileges on the mail server to gain root access.

Correct Answer: D

QUESTION 5

Which of the following is the most secure method for sending the penetration test report to the client?

A. Sending the penetration test report on an online storage system.

B. Sending the penetration test report inside a password-protected ZIP file.

C. Sending the penetration test report via webmail using an HTTPS connection.

D. Encrypting the penetration test report with the client\\'s public key and sending it via email.

Correct Answer: D

This is the most secure method for sending the penetration test report to the client because it ensures that only the client can decrypt and read the report using their private key. Encrypting the report with the client\\'s public key prevents anyone else from accessing the report, even if they intercept or compromise the email. The other methods are not as secure because they rely on weaker or no encryption, or they expose the report to third-party services that may not be trustworthy or compliant.