PT0-002 Q&As

CompTIA PenTest+ Certification Exam

Pass CompTIA PT0-002 Exam with 100% Guarantee

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

https://www.leads4pass.com/pt0-002.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

When planning a penetration-testing effort, clearly expressing the rules surrounding the optimal time of day for test execution is important because:

A. security compliance regulations or laws may be violated.

B. testing can make detecting actual APT more challenging.

C. testing adds to the workload of defensive cyber- and threat-hunting teams.

D. business and network operations may be impacted.

Correct Answer: D

QUESTION 2

A penetration tester gains access to a system and establishes persistence, and then runs the following commands: cat /dev/null > temp touch -r .bash_history temp mv temp .bash_history Which of the following actions is the tester MOST likely performing?

A. Redirecting Bash history to /dev/null

B. Making a copy of the user\\'s Bash history for further enumeration

C. Covering tracks by clearing the Bash history

D. Making decoy files on the system to confuse incident responders

Correct Answer: C

Reference: https://null-byte.wonderhowto.com/how-to/clear-logs-bash-history-hacked-linux-systems-cover-your-tracks-remain-undetected-0244768/

QUESTION 3

A Chief Information Security Officer wants a penetration tester to evaluate whether a recently installed firewall is protecting a subnetwork on which many decades- old legacy systems are connected. The penetration tester decides to run an OS discovery and a full port scan to identify all the systems and any potential vulnerability.

Which of the following should the penetration tester consider BEFORE running a scan?

A. The timing of the scan

B. The bandwidth limitations

C. The inventory of assets and versions

D. The type of scan

Correct Answer: C

QUESTION 4

A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible. Which of the following Nmap scan syntaxes would BEST accomplish this objective?

A. nmap-sT -vvv -O 192.168.1.2/24-PO

B. nmap -sV 192.168.1.2/24-PO

C. nmap -sA -v -O 192.168.1.2/24

D. nmap -sS -O 192.168.1.2/24-T1

Correct Answer: D

Reference: https://nmap.org/book/man-port-scanning-techniques.html

QUESTION 5

A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

A. A signed statement of work

B. The correct user accounts and associated passwords

C. The expected time frame of the assessment

D. The proper emergency contacts for the client

Correct Answer: D