PT0-001 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.pass2lead.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

A penetration tester is able to move laterally throughout a domain with minimal roadblocks after compromising a single workstation. Which of the following mitigation strategies would be BEST to recommend in the report? (Select THREE).

A. Randomize local administrator credentials for each machine.

B. Disable remote logons for local administrators.

C. Require multifactor authentication for all logins.

D. Increase minimum password complexity requirements.

E. Apply additional network access control.

F. Enable full-disk encryption on every workstation.

G. Segment each host into its own VLAN.

Correct Answer: CDE

QUESTION 2

After establishing a shell on a target system, Joe, a penetration tester is aware that his actions have not been detected. He now wants to maintain persistent access to the machine. Which of the following methods would be MOST easily detected?

A. Run a zero-day exploit.

B. Create a new domain user with a known password.

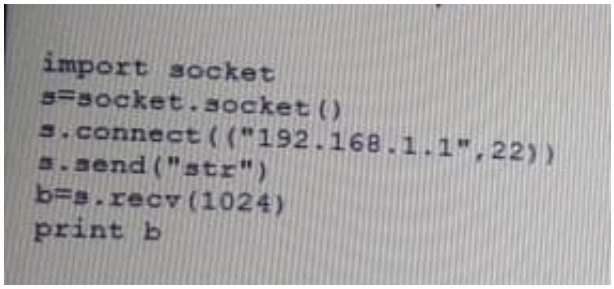
C. Modify a known boot time service to instantiate a call back.

D. Obtain cleartext credentials of the compromised user.

Correct Answer: C

QUESTION 3

Given the following Python script:



Which of the following actions will it perform?

A. ARP spoofing

B. Port scanner

C. Reverse shell

D. Banner grabbing

Correct Answer: D

QUESTION 4

A penetration tester has run multiple vulnerability scans against a target system. Which of the following would be unique to a credentialed scan?

A. Exploits for vulnerabilities found

B. Detailed service configurations

C. Unpatched third-party software

D. Weak access control configurations

Correct Answer: A

QUESTION 5

A security analyst was provided with a detailed penetration report, which was performed against the organization\\'s DMZ environment. It was noted on the report that a finding has a CVSS base score of 10.0.

Which of the following levels of difficulty would be required to exploit this vulnerability?

A. Very difficult; perimeter systems are usually behind a firewall.

B. Somewhat difficult; would require significant processing power to exploit.

C. Trivial; little effort is required to exploit this finding.

D. Impossible; external hosts are hardened to protect against attacks.

Correct Answer: C

Reference https://nvd.nist.gov/vuln-metrics/cvss