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

A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.

Which of the following is the BEST action for the penetration tester to take?

A. Utilize the tunnel as a means of pivoting to other internal devices.

B. Disregard the IP range, as it is out of scope.

C. Stop the assessment and inform the emergency contact.

D. Scan the IP range for additional systems to exploit.

Correct Answer: D

QUESTION 2

A penetration tester receives the following results from an Nmap scan:

```
Interesting ports on 192.168.1.1:

Port      State     Service
21/tcp    closed    ftp
22/tcp    open      ssh
23/tcp    closed    telnet
25/tcp    closed    smtp
80/tcp    open      http
110/tcp   closed    pop3
139/tcp   closed    nethics-ssn
443/tcp   closed    https
3389/tcp  closed    rdp
```

Which of the following OSs is the target MOST likely running?

A. CentOS

B. Arch Linux

C. Windows Server

D. Ubuntu

Correct Answer: C

QUESTION 3

In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company\\'s servers.

Which of the following actions would BEST enable the tester to perform phishing in a later stage of the assessment?

A. Test for RFC-defined protocol conformance.

B. Attempt to brute force authentication to the service.

C. Perform a reverse DNS query and match to the service banner.

D. Check for an open relay configuration.

Correct Answer: D

SMTP is a protocol associated with mail servers. Therefore, for a penetration tester, an open relay configuration can be exploited to launch phishing attacks.

QUESTION 4

After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:

```
Nmap scan report for 192.168.10.10

Port      State     Service        Version
135/tcp   open      msrpc          Microsoft Windows RPC
139/tcp   open      netbios-ssn    Microsoft Windows netbios-ssn
5985/tcp  open      Microsoft      HTTPAPI httpd 2.0 (SSDP/UPnP)

Nmap scan report for 192.168.10.11

Port      State     Service        Version
135/tcp   open      msrpc              Microsoft Windows RPC
139/tcp   open      netbios-ssn        Microsoft Windows netbios-ssn
3389/tcp  open      ms-wbt-server      Microsoft Terminal Services
```

The tester then runs the following command from the previous exploited system, which fails: Which of the following explains the reason why the command failed?

A. The tester input the incorrect IP address.

B. The command requires the-port 135 option.

C. An account for RDP does not exist on the server.

D. PowerShell requires administrative privilege.

Correct Answer: C

QUESTION 5

A penetration tester wants to scan a target network without being detected by the client\\'s IDS. Which of the following scans is MOST likely to avoid detection?

A. nmap -p0 -T0 -sS 192.168.1.10

B. nmap -sA -sV --host-timeout 60 192.168.1.10

C. nmap -f --badsum 192.168.1.10

D. nmap -A -n 192.168.1.10

Correct Answer: A

Reference: https://www.oreilly.com/library/view/network-security- assessment/9780596510305/ch04.html