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

CompTIA PenTest+ Certification Exam

QUESTION 1

A compliance-based penetration test is primarily concerned with:

A. obtaining Pll from the protected network.

B. bypassing protection on edge devices.

C. determining the efficacy of a specific set of security standards.

D. obtaining specific information from the protected network.

Correct Answer: C

QUESTION 2

A company has hired a penetration tester to deploy and set up a rogue access point on the network.

Which of the following is the BEST tool to use to accomplish this goal?

A. Wireshark

B. Aircrack-ng

C. Kismet

D. Wifite

Correct Answer: B

Reference: https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords- with-evil-twin-attack-0183880/

https://thecybersecurityman.com/2018/08/11/creating-an-evil-twin-or-fake-access-point- using-aircrack-ng-and-dnsmasq-part-2-the-attack/

QUESTION 3

An Nmap scan shows open ports on web servers and databases. A penetration tester decides to run WPScan and SQLmap to identify vulnerabilities and additional information about those systems.

Which of the following is the penetration tester trying to accomplish?

A. Uncover potential criminal activity based on the evidence gathered.

B. Identify all the vulnerabilities in the environment.

C. Limit invasiveness based on scope.

D. Maintain confidentiality of the findings.

Correct Answer: C

QUESTION 4

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

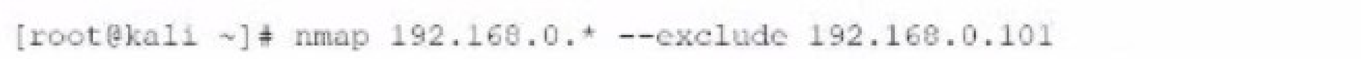
Correct Answer: C

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 5

Given the following Nmap scan command:

[root@kali ~]# nmap 192.168.0 .* -- exclude 192.168.0.101



```
[root@kali ~]# nmap 192.168.0.* --exclude 192.168.0.101
```

Which of the following is the total number of servers that Nmap will attempt to scan?

A. 1

B. 101

C. 255

D. 256

Correct Answer: C

The Nmap scan command given will scan all the hosts in the 192.168.0.0/24 subnet, except for the one with the IP address 192.168.0.101. The subnet has 256 possible hosts, but one of them is excluded, so the total number of servers that

Nmap will attempt to scan is 255.

References:

Nmap Commands - 17 Basic Commands for Linux Network, Section: Scan Multiple Hosts, Subsection: Excluding Hosts from Search Nmap Cheat Sheet 2023: All the Commands and More, Section: Target Specification, Subsection: -exclude