08: Assisted Lab: Understanding Nmap Common Usage

PenTest+ (Exam PT0-002)

Congratulations, you passed!

Duration: 15 minutes, 26 seconds

☑ What is the first section of the help information after Usage? *Score: 1*

TARGET SPECIFICATION

Correct

☑ How many active hosts were found on the network? *Score: 1*

5

Correct

☑ How many open ports were found on the LAMP server? *Score: 1*

4

Correct

☑ What is the version number of the Apache httpd running on the LAMP server? *Score: 1*

2.4.41

Correct

☑ What is the difference between a -sT and -sS scans? *Score: 1*

- ◉ The -sS scan does not complete the full TCP handshake
- ○ The -sT scan does not complete the full TCP handshake
- ○ The -sS scan does not complete the full SYN handshake
- ○ The -sT scan does not complete the full SYN handshake
- ○ None of the above

Correct

How many UDP ports are open on the Windows server? *Score: 1*

4

Correct

How many ports show open on the Windows server with the port only scan? *Score: 1*

- Fewer ports
- Same number of ports
- 2-3 more ports
- More than double the number of ports

Correct

What service is running on port 3389? *Score: 1*

- Microsoft Terminal Services
- Microsoft Domain Name Server
- Microsoft Active Directory
- Microsoft Active Directory LDAP

Correct

What is the port number of the one service which returned a banner? *Score: 1*

593

Correct

Which nmap option performs a ping sweep? *Score: 1*

- -Ps
- -sP
- -sS
- -sp

Correct

If you wanted to scan all possible 65535 ports on a target, which of the following options would you use? *Score: 1*

- -p-
- -p1-65535
- -p 1-65535
- All of the above
- None of the above

Correct

What nmap option performs an UDP scan? *Score: 1*

- -U
- -sU
- -PU
- -u

Correct

What does the -A option do? *Score: 1*

- OS detection
- Version detection
- Script scanning
- Traceroute
- All of the above
- None of the above

Correct