Network Penetration Testing Methodology-Internal

6 Hr 42 Min Remaining

Instructions Resources Help  100%

Exercise 6: OS Fingerprinting with Nmap

Scenario

A penetration tester must use a tool to fingerprint the OS. The choice of tool here is the most popular tool on the market that is free and open source: Nmap. The objective of this lab is to help students use the Nmap tool and focus on the tool’s OS capability. In this lab, you will

• Fingerprint the OS

• Compare different scan options

• Analyze the tool output

**Lab Duration**: **10** Minutes

1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.

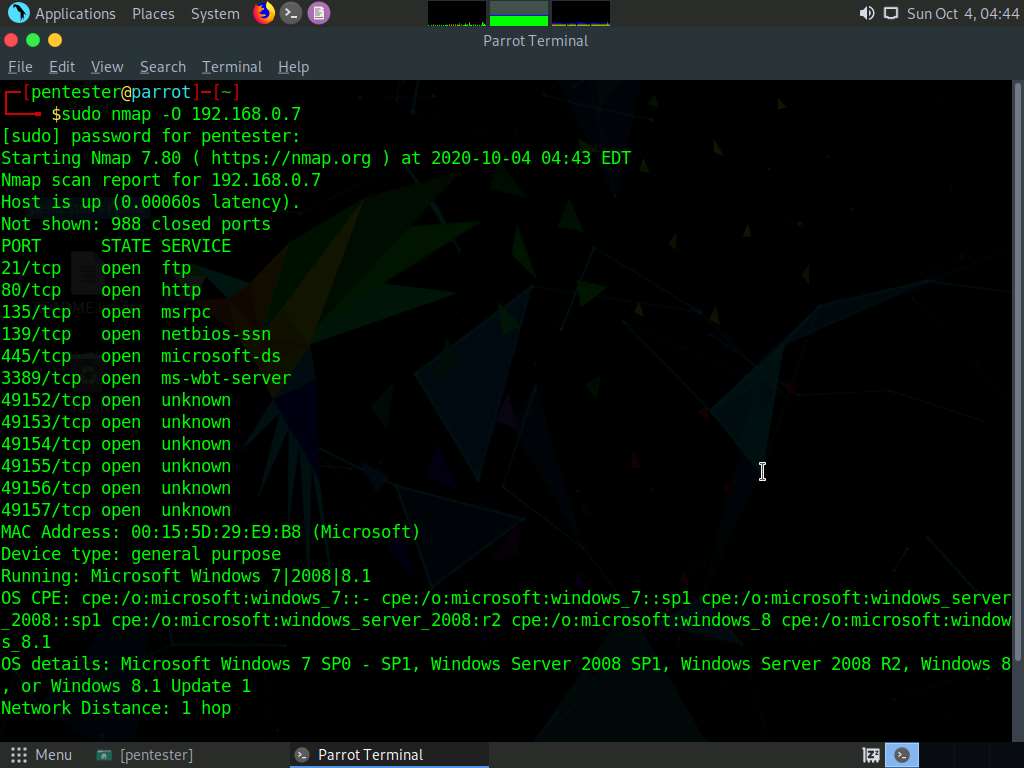


1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.



1. There is a specific option for attempting to enumerate the OS with Nmap: –O option (the “O” does not stand for zero).
2. Using your target database, use the –O option to fingerprint the OS.
3. Start capturing on Wireshark.
4. In a terminal window, type **sudo nmap –O 192.168.0.X**, replacing the “**X**” with the required IP address number from your target database, as shown in the screenshot.

If you are asked to enter the password, type **toor** and press **Enter**.



1. Carefully review the results and transfer the required data to the target database.
2. As required, re-scan and enter the required IP addresses for the other machines to finish populating your target database.
3. Note that Nmap is noisy and uses many packets to detect the OS; if stealth is a requirement, this may not be the best tool.
4. It is imperative to use multiple tools—at least two to validate and verify the information that a tool discovers.
5. Once you fully understand the process, you may continue to review and evaluate the tools that you need to be a professional security tester.
6. This concludes the lab exercise.