Network Penetration Testing Methodology-Internal

6 Hr 40 Min Remaining

Instructions Resources Help  100%

Exercise 10: Enumerating SMB

Scenario

A proficient tester should be aware of the different tools used to enumerate the Server Message Block (SMB). The Parrot security OS has SMB tools that can be used to familiarize oneself with data for enumeration. The objective of this lab is to help students use tools to enumerate the SMB. In this lab, you will

• Identify SMB is running

• Scan for SMB information

• Enumerate information from the SMB protocol

• Add information, based on your analysis, to the target database

**Lab Duration**: **5** Minutes

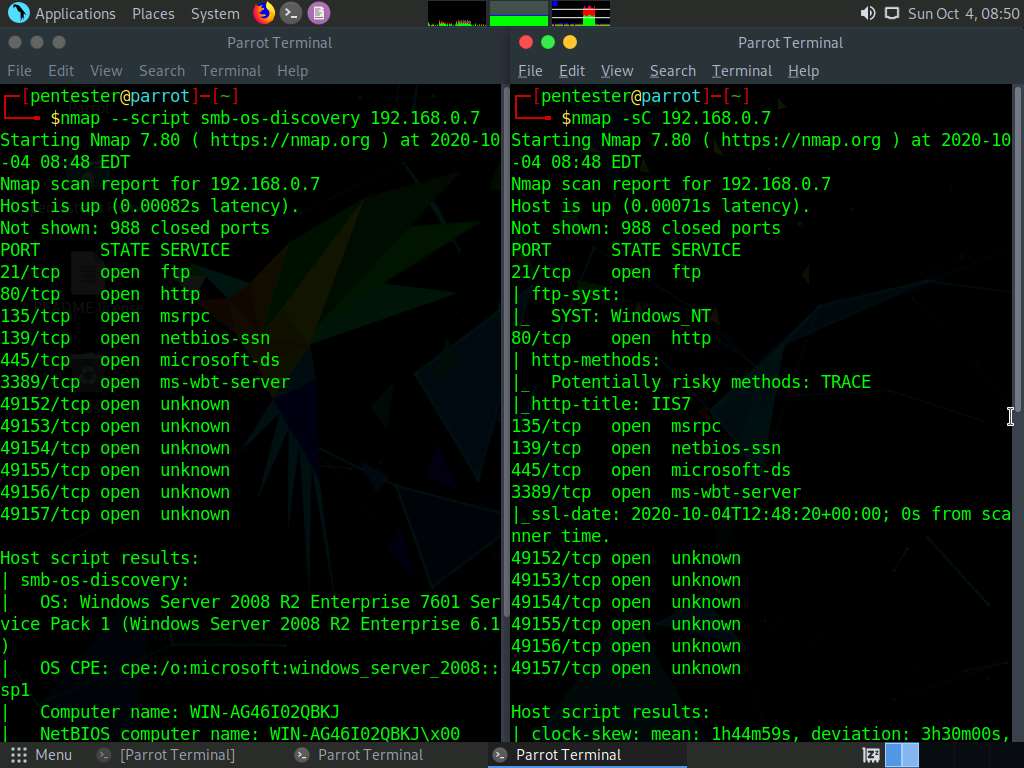
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



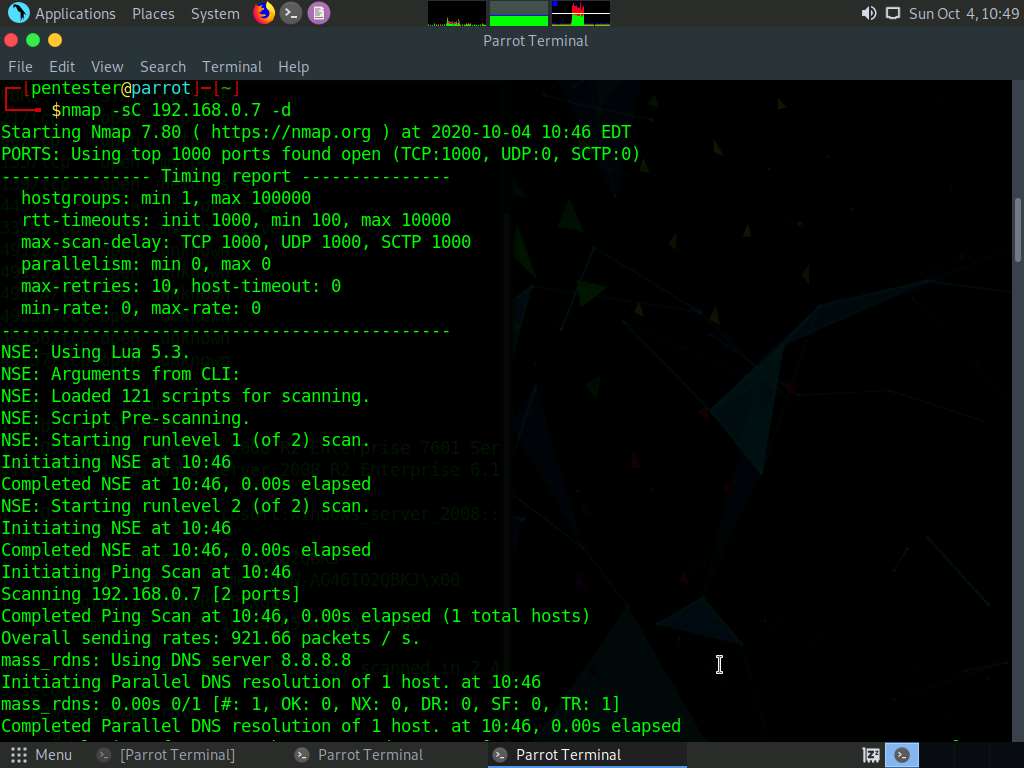
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.

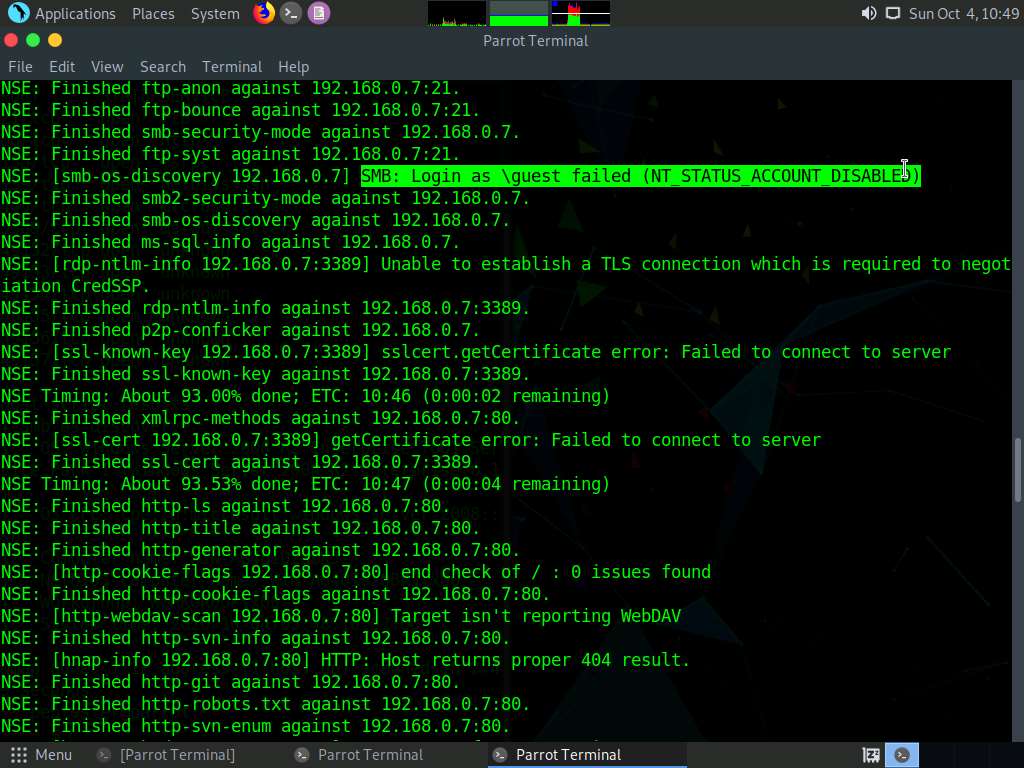


1. Nmap has a number of scripting engines that you can use. So far, there are over 200 engines. This lab concerns the one for the SBM.
2. Open a terminal window, type **nmap --script smb-os-discovery 192.168.0.7**, and press **Enter**.
3. In the terminal window, type **nmap –sC 192.168.0.7** and press **Enter**.
4. The output of the command in step 5 reveals more details than that of the command in step 4. The scan may take approximately 5 to 10 minutes complete.



1. Add the “d” option to the command to show the debug trace, as shown in the screenshot illustrating the output.





1. As the ERROR shows, the login attempts fail. This result is common when dealing with newer Windows systems.
2. If you add the XML output capability, the information can be displayed on a graphic user interface (GUI) in an easy-to-read format for documentation