Hands-on Lab: Scanning Network Environment with NMap

Estimated time needed: 20 minutes

About This Lab

In this lab, you will learn how to scan a network with the domain name and/or IP Address using the ZenMap tool.

ZenMap Output Error (Expected Behavior in this lab)

While completing the ZenMap scanning lab, I encountered repeated `Error building command` messages at the end of successful scans. The error reported that ZenMap could not save the temporary `.xml` output file to a dynamically generated path under the `Temp` directory (e.g., `AppData\Local\Temp\zenmap-xxxx.xml`). Despite this error, the scans completed successfully and displayed output in the UI.

This issure appears to be a known limitation of the lab environment or ZenMap's configuration on Windows systems without proper temp folder access. Running ZenMap as administrator or clearing/re-creating the temp directory might resolve this in a non-lab context. However, since scan functionality was unaffected, I proceeded with the lab as instructed.

Objectives

After completing this lab, you will be able to:

1. Use ZenMap, the GUI utility, provided by NMap
2. Perform a network scan based on the IP Address or domain name
3. Review different scan options in the ZenMap utility

1. Open any browser of your choice in your virtual environment.

2. Type https://nmap.org/download in the search bar and press enter.

3. Click the OS that you need the software for. This lab's instructions are based on Windows OS. The steps might slightly vary for other operating systems.
4. Click the installation executable for windows.
5. Once the download completes, click the .exe file to begin the installation.

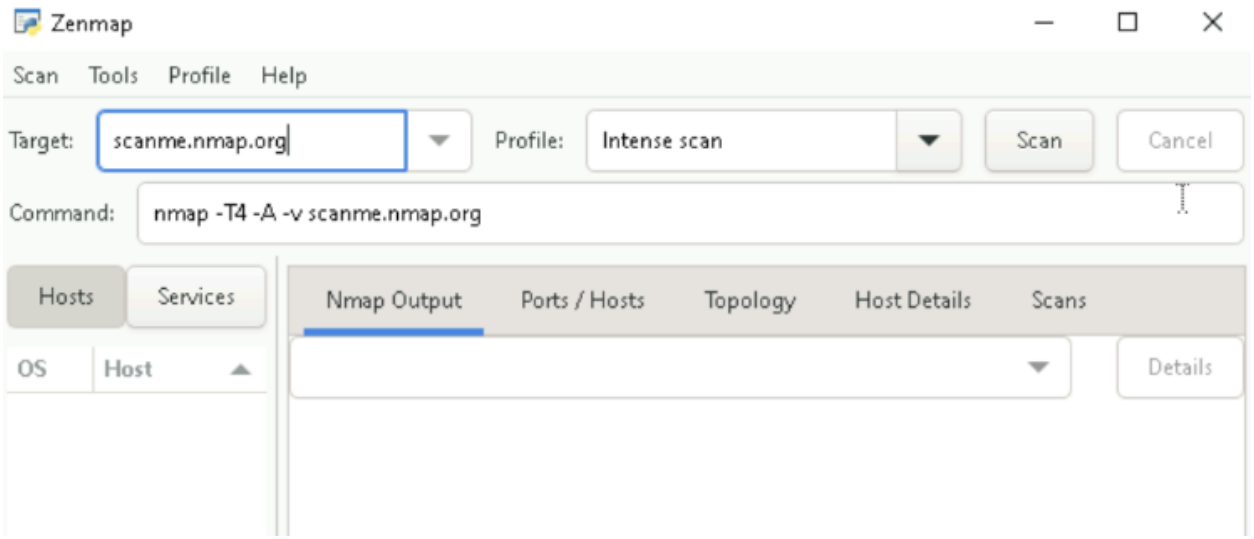
This will download NMap and Zenmap a GUI utility for NMap which is a great tool to use when you begin learning NMap.

6. Complete the process of installation by following the instructions.

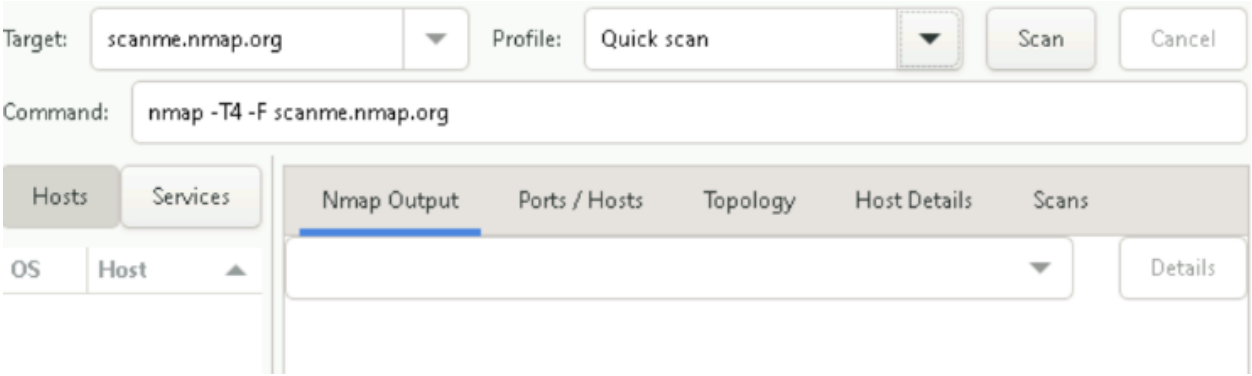
Note: Click "I agree" to proceed with the installation. Make sure to install all required dependencies and then click "Finish" to complete the setup.

Task 2 NMap with Zenmap

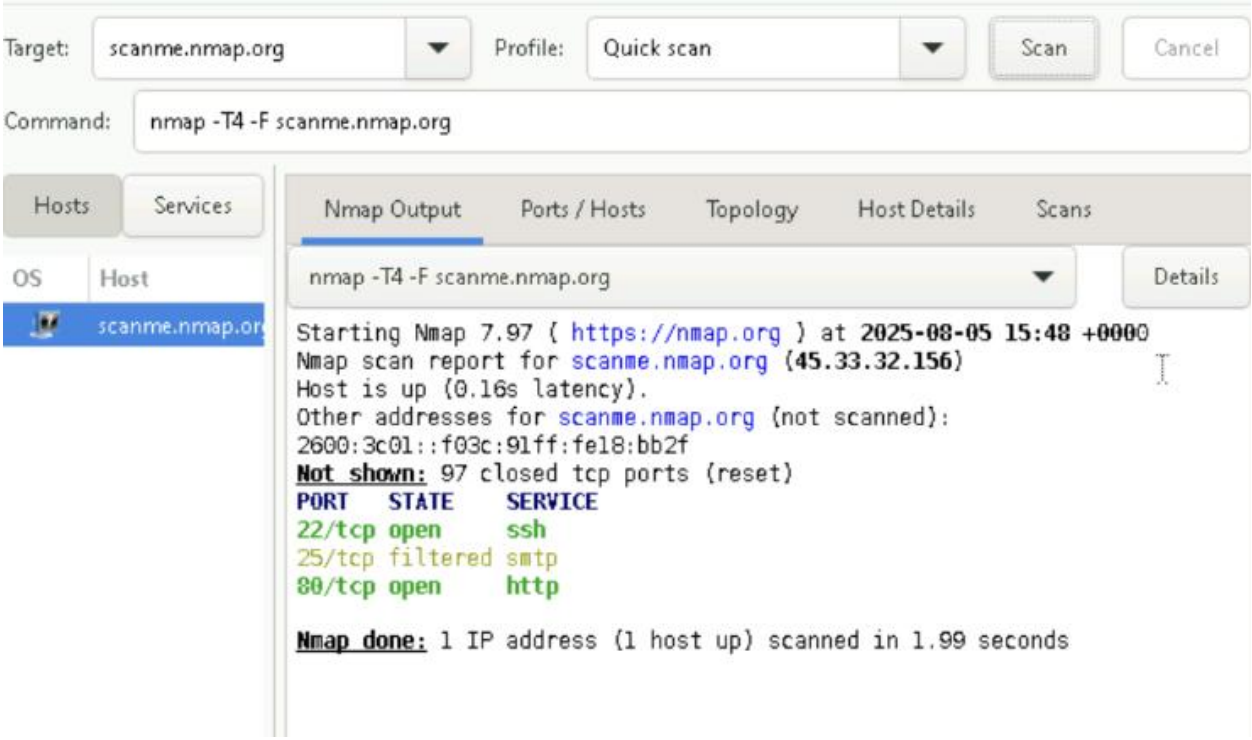
1. Click to open the Zenmap app on your desktop.
2. This opens the Zenmap application.
3. In the **Target** field, enter **scanme.nmap.org**. This routes to your local system.



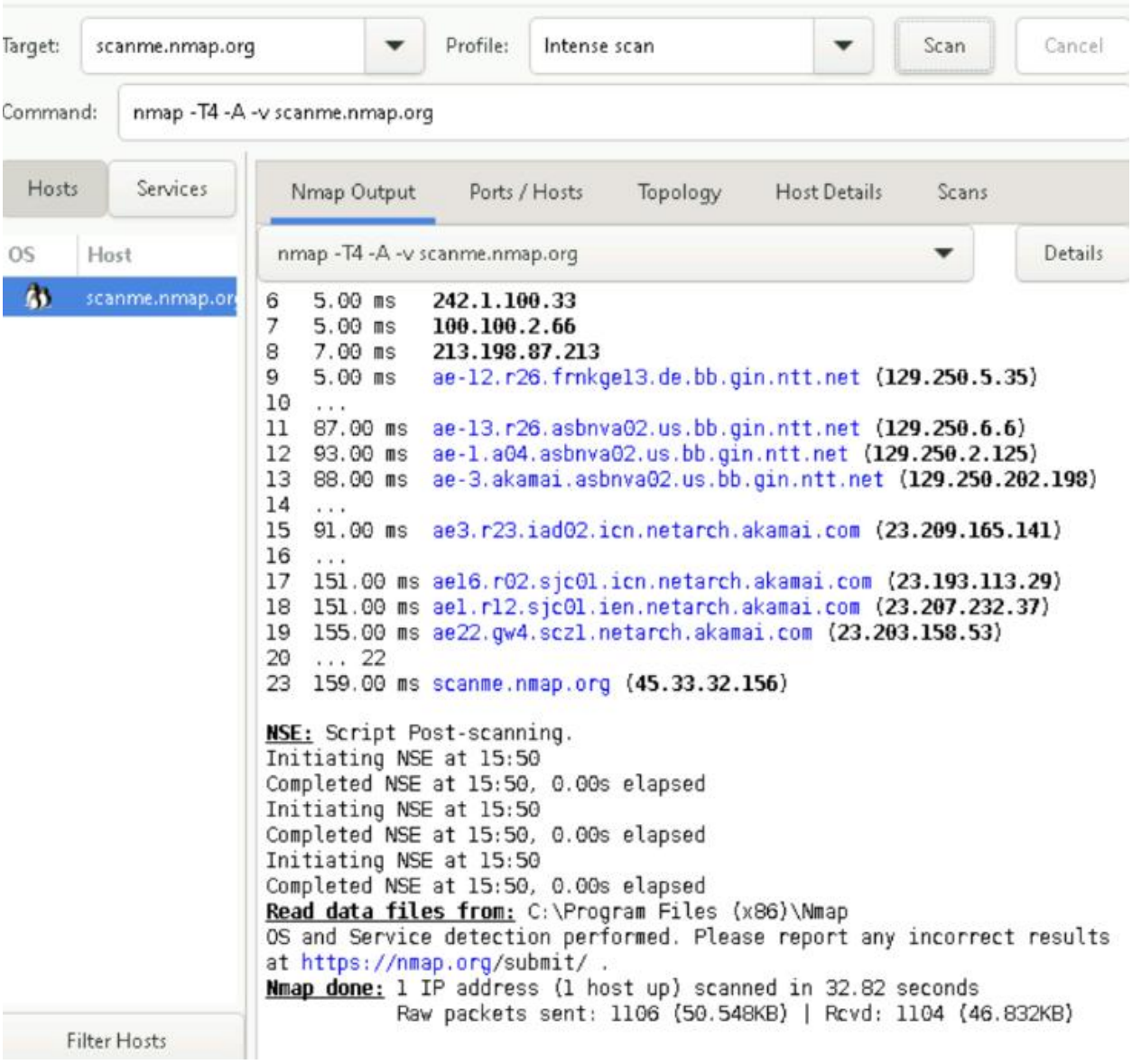
4. Choose **Quick Scan** from the scan options.



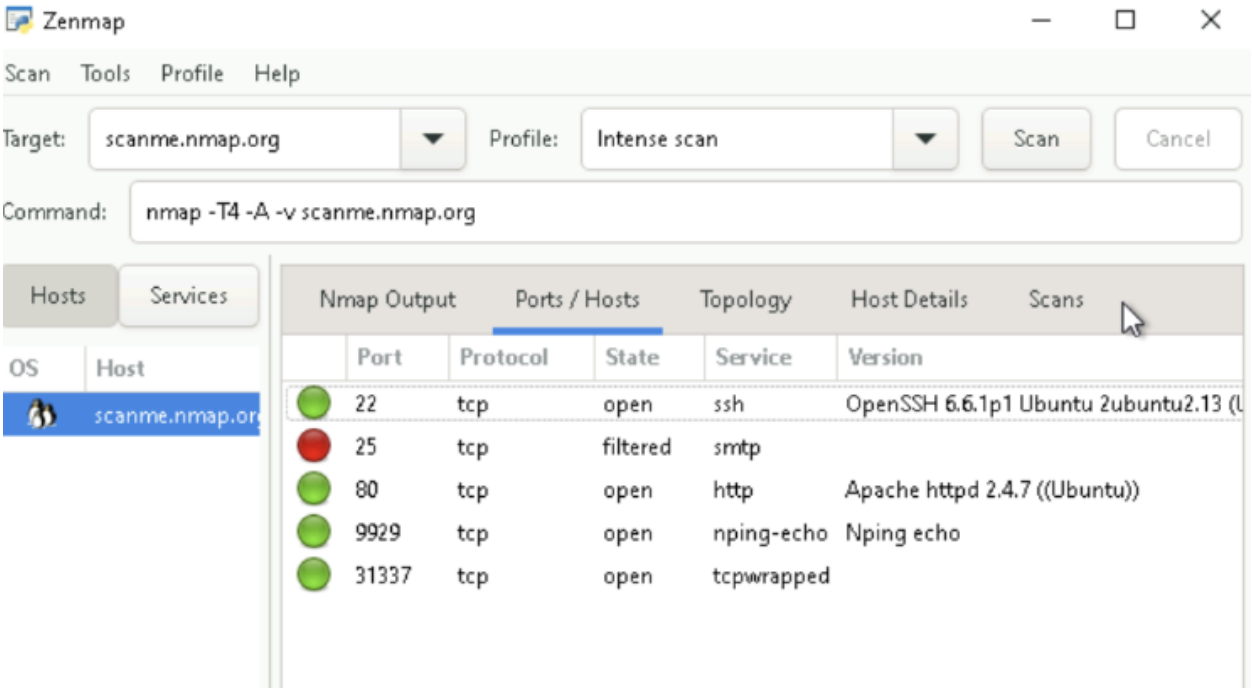
5. Click **Scan** to begin the scan process.
6. You can see the output of the scan in the first **Nmap Output** scan results tab.



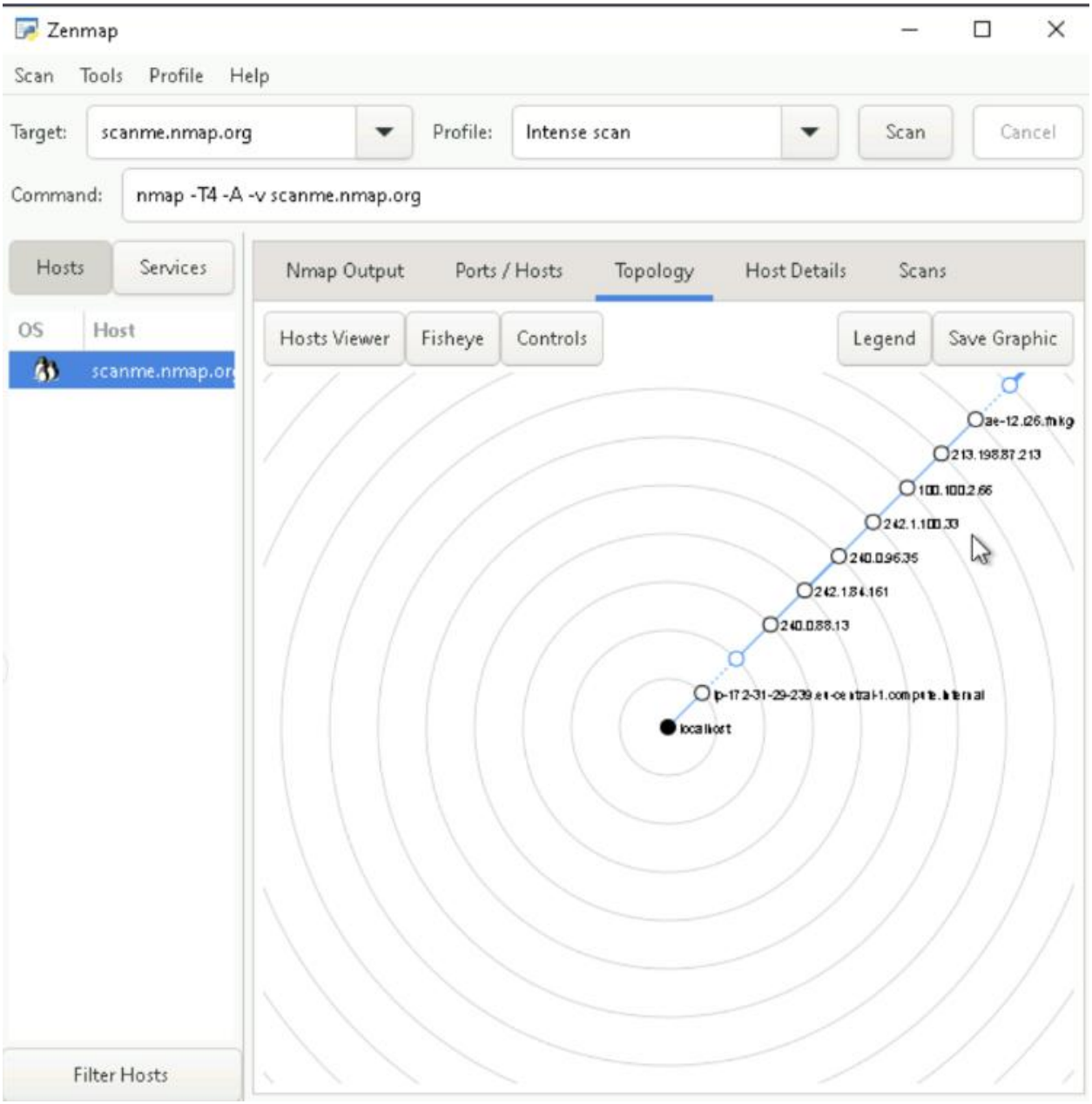
7. Now from the list of scan options choose **Intense scan**. This is a more intense scan and gives detailed results. In realtime this will take a few minutes. Click **Scan** to begin intense scanning.
8. Once the scan finishes, you will see the detailed output along with how long the scanning took in the NMap output tab.



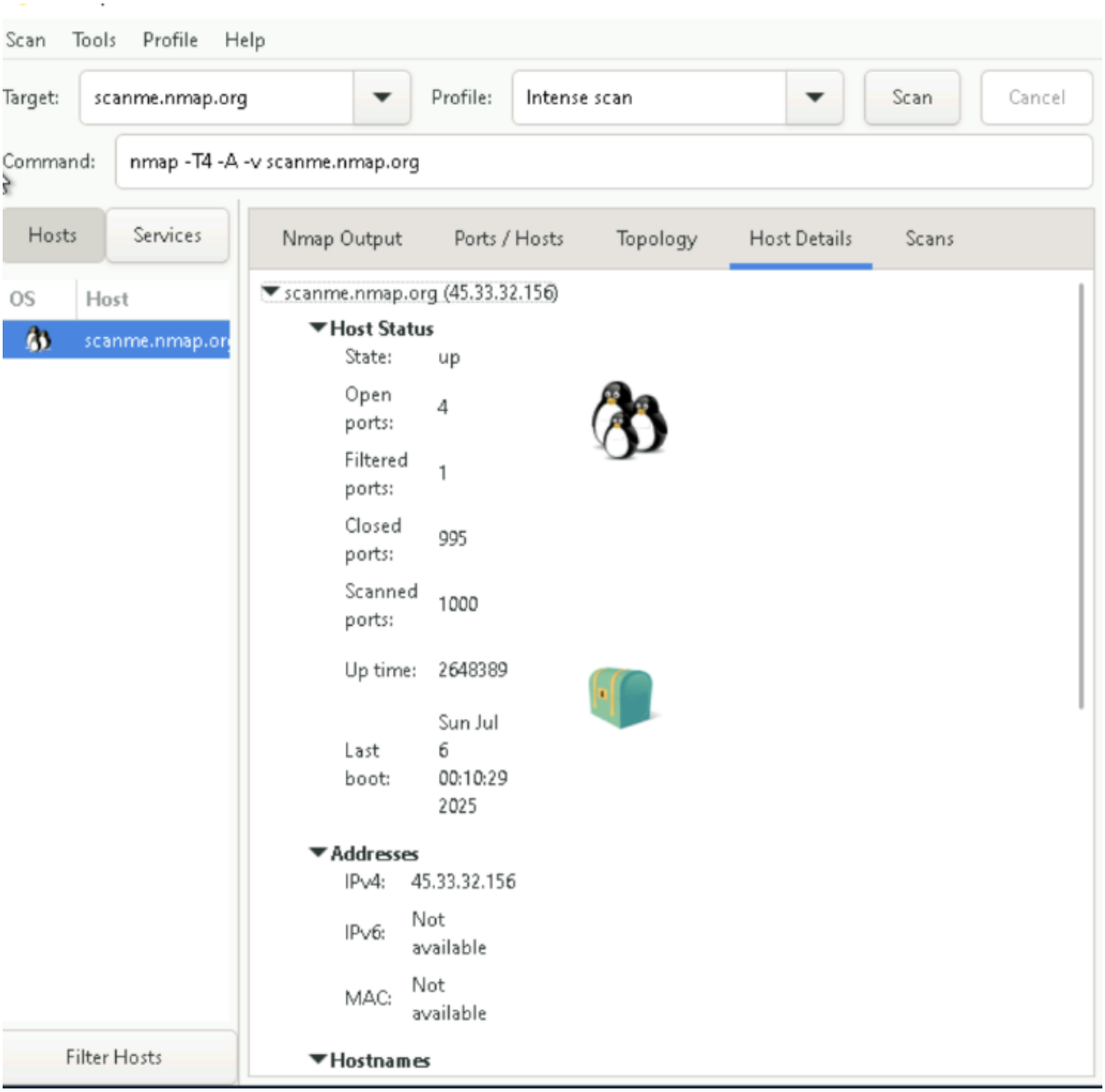
9. Click the **Ports/Hosts** tab to see state the ports in the target system.
   The **green** indicates open ports and **red** indicates closed ports.



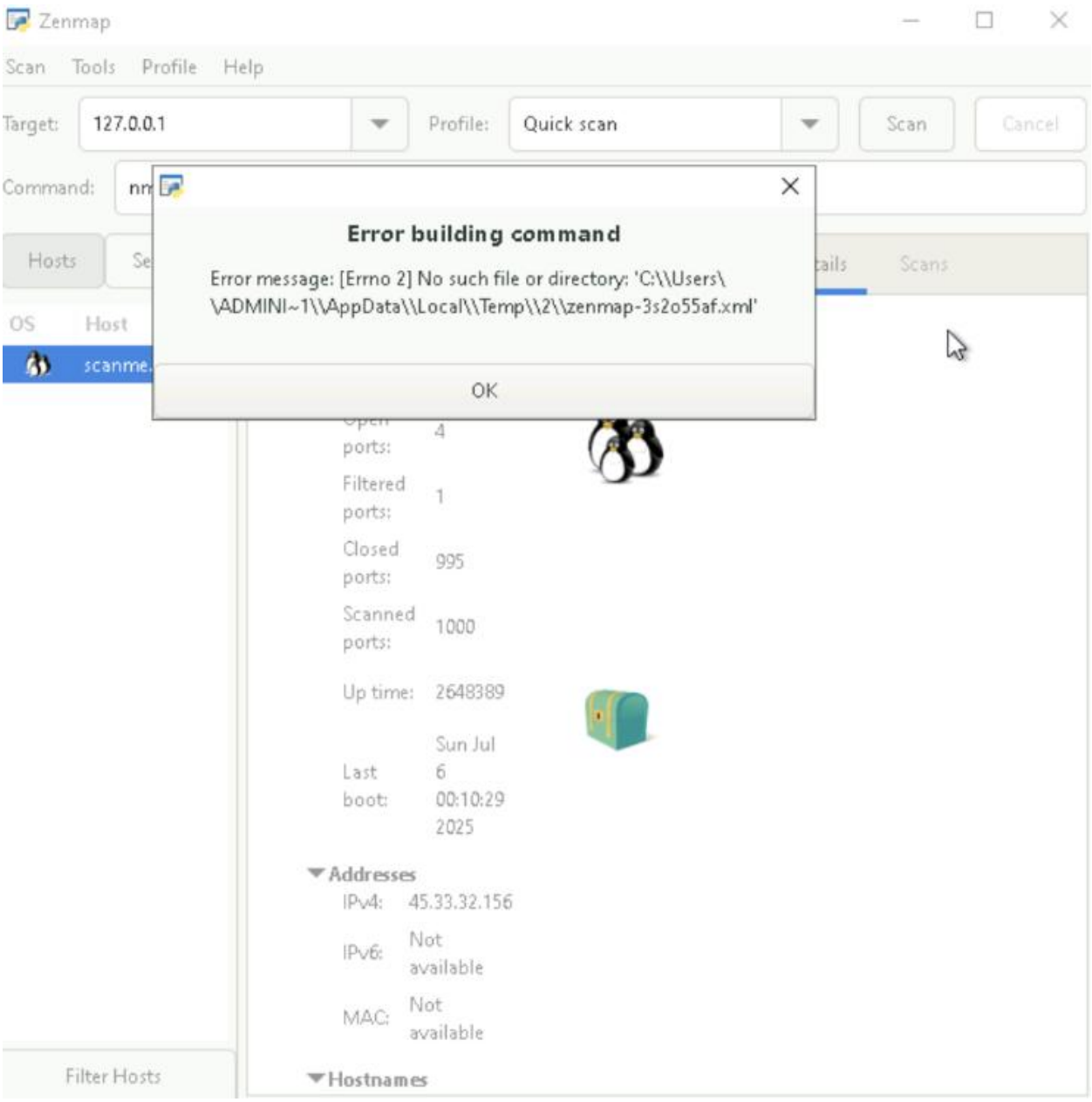
10. Click the **Topology** tab to view the visualization of the hosts on this network. If a host has less than 3 ports, it will be green. If it has 3 to 5 ports it will be yellow. If it has more 6, it will be red. This will be evident when you test on real networks.



11. Click the **Host Details** tab to get the details about the host you are scanning. The details will include the Host status, Address, Hostname, Operating system, and so on.

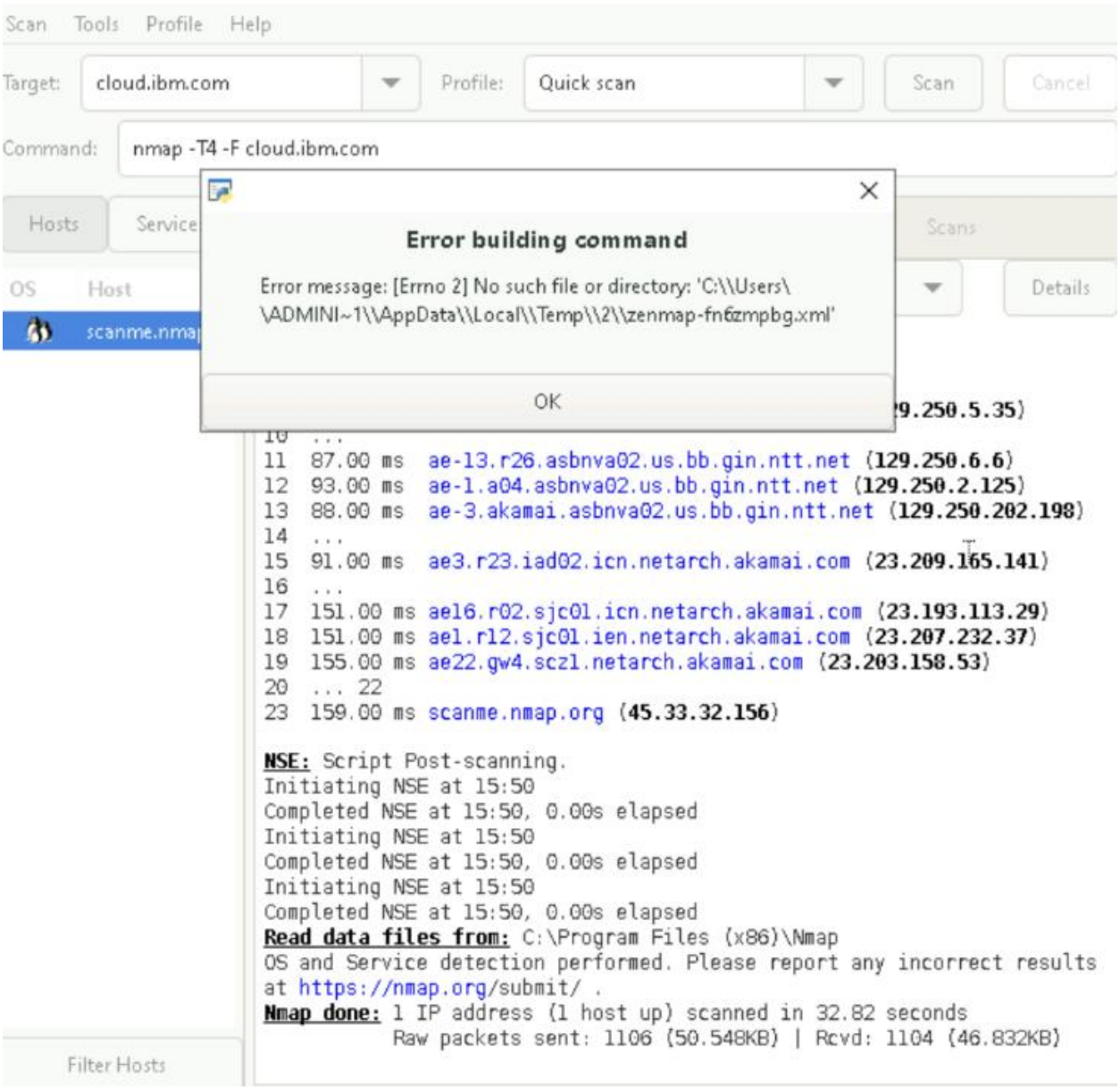


12. Change the target to 127.0.0.1 which is the IP address for your localhost and click **Scan**.



13. See the Nmap output of 127.0.0.1.

14. Change the target to cloud.ibm.com. and click **Scan**.



15. See the Nmap output of cloud.ibm.com.