Network Penetration Testing Methodology-External

1 Hr 8 Min Remaining

Instructions Resources Help  100%

Exercise 1: Exploring and Auditing a Machine Using Nmap

Scenario

Network scan plays a crucial role in identifying the hosts that are up and running in a network. Additionally, it helps a pentester in pulling out additional information associated with a machine such as the services running on the machine, the ports used by the service and the operating system details.  
As a penetration tester, you need to have extensive knowledge of network mapping tools, top ports running different services, etc.

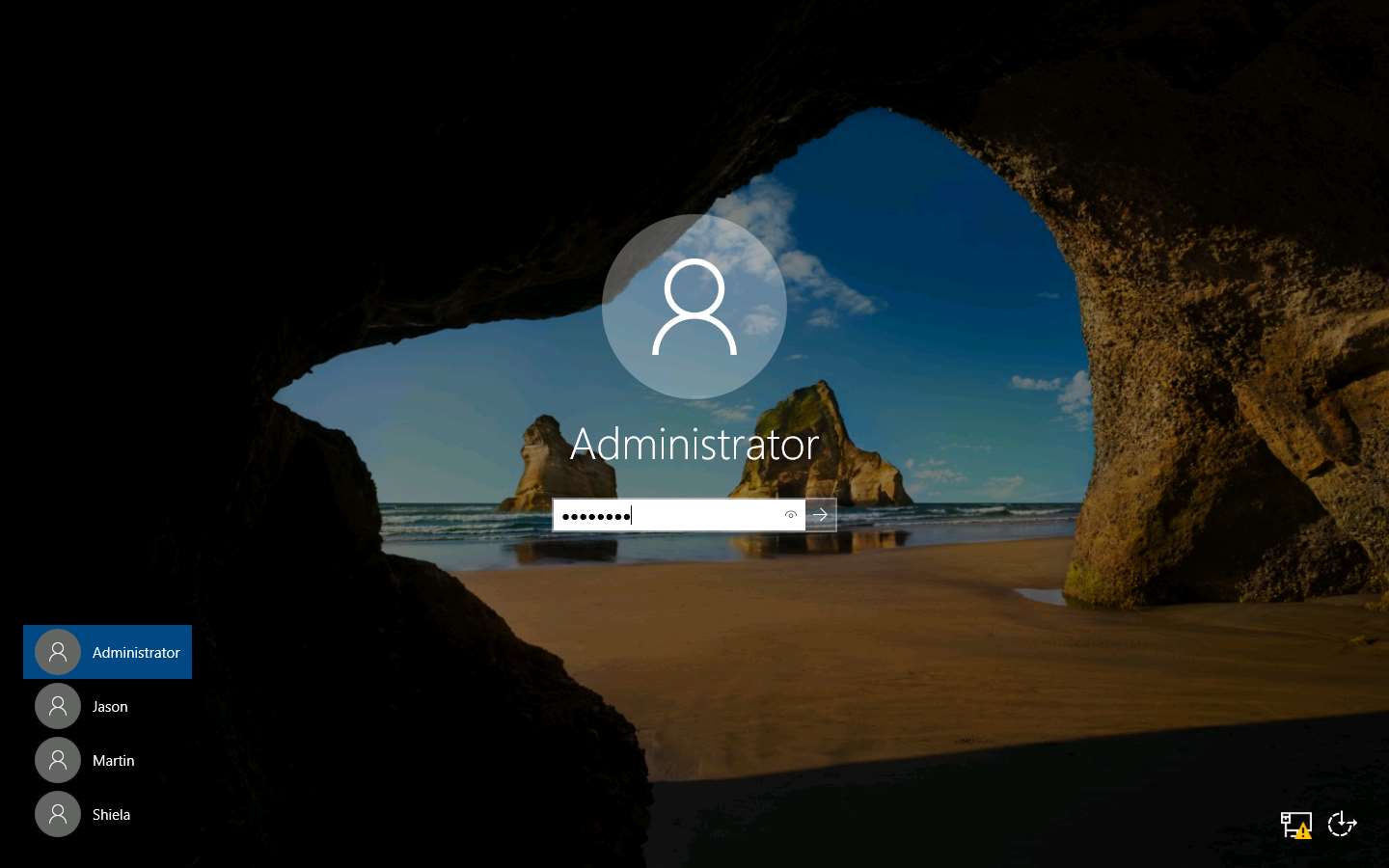
**Lab Duration**: **30** Minutes

1. Click [Windows Server 2019](https://labclient.labondemand.com/Instructions/d51b1821-8ebe-4479-bf4b-33b56a1978d1?rc=10). Click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/d51b1821-8ebe-4479-bf4b-33b56a1978d1?rc=10).

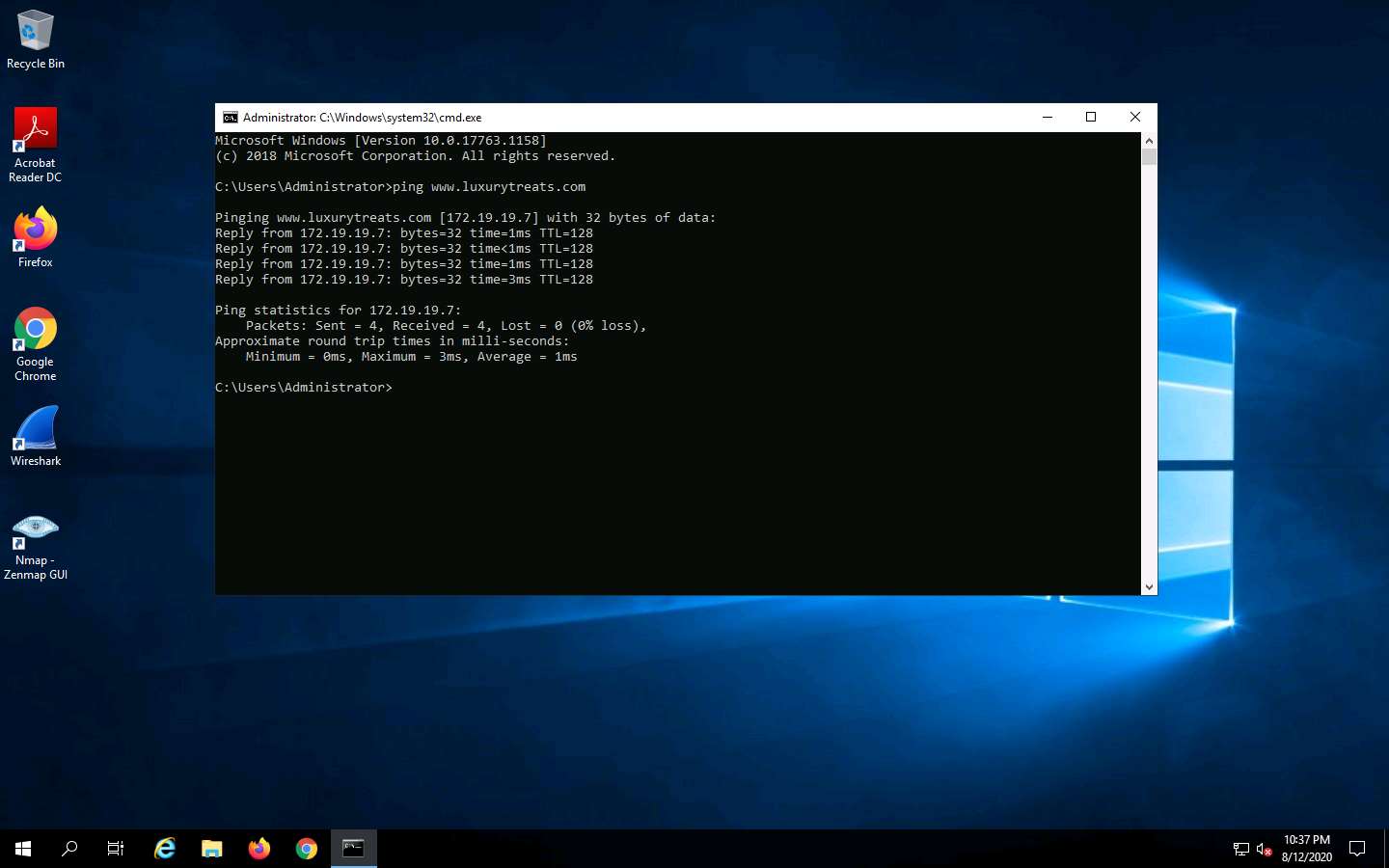


1. In the password field click Pa$$w0rd and press **Enter**

You can use the **Type Password** option from the **Commands** menu to enter the password.



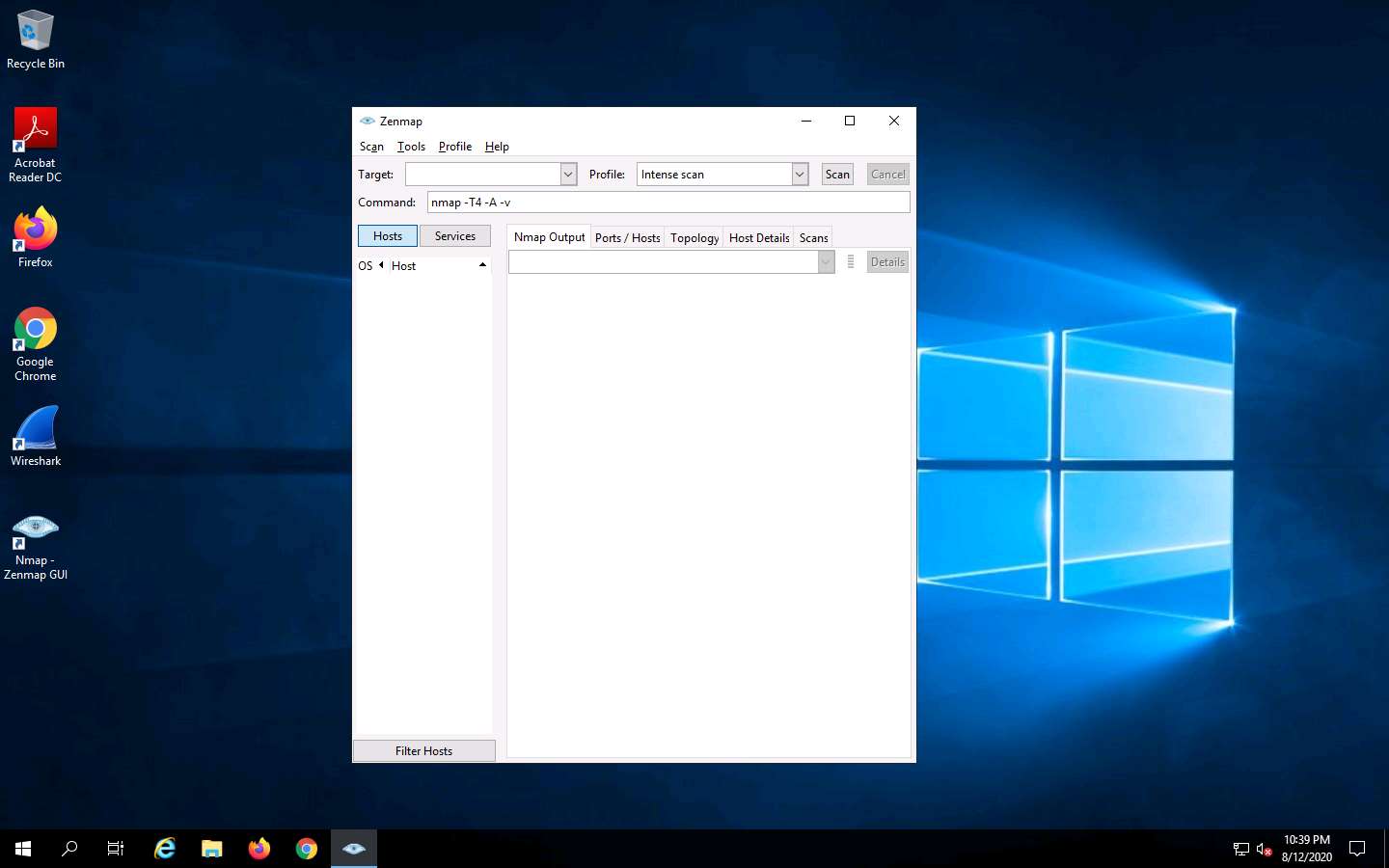
1. In this lab, you are given the assignment to audit the server hosting the website **http://www.luxurytreats.com**. So, before beginning this lab, we shall identify the IP Address of the website using the **ping** utility. Launch a command prompt, type **ping www.luxurytreats.com** and press **Enter**. This returns the IP Address of the server as **172.19.19.7** in the response. We will be scanning this IP address using Nmap in the forthcoming tasks.



1. To launch **Nmap**, double-click **Nmap - Zenmap GUI** icon on the desktop.

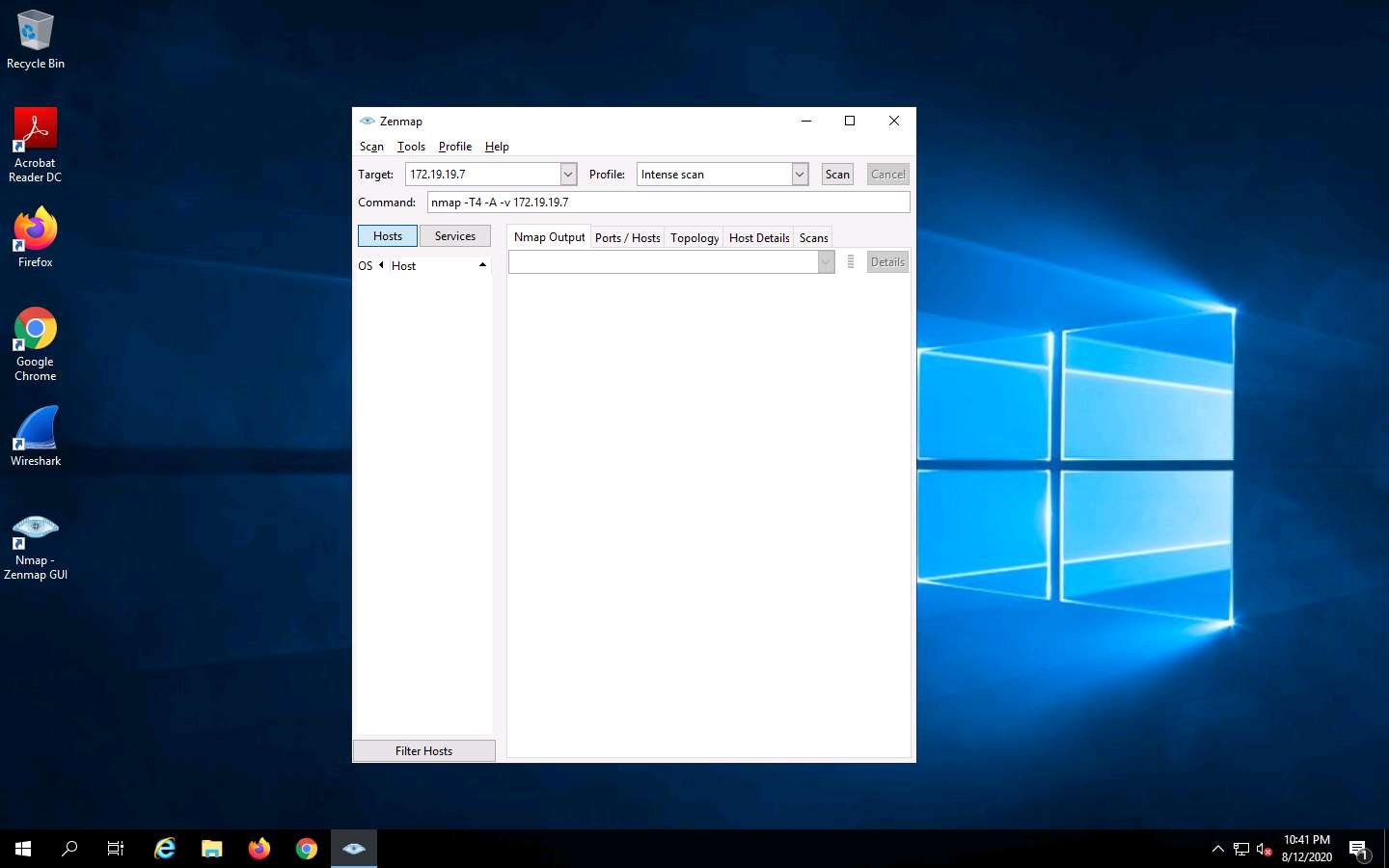


1. **Zenmap** (**Nmap**) main window appears as shown in the screenshot.



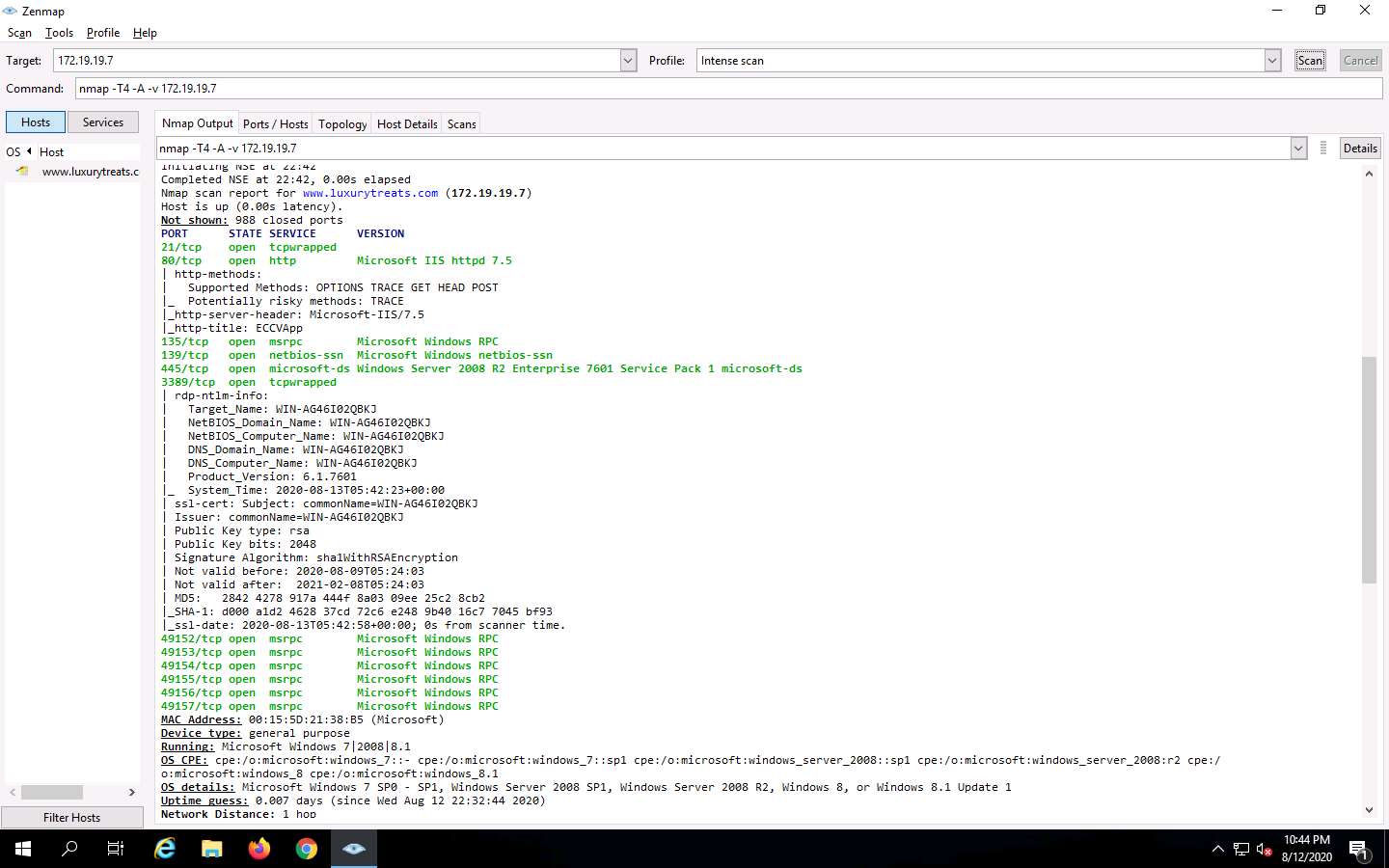
1. To perform **Intense Scan**, enter IP address in the **Target** field and choose **Intense Scan** from **Profile** drop-down list and click **Scan**. In this lab, we are performing Intense Scan on **Web Server** machine (which is hosting www.luxurytreats.com) whose IP address, **172.19.19.7** was identified in the earlier steps.

The scan will take a few minutes to complete.

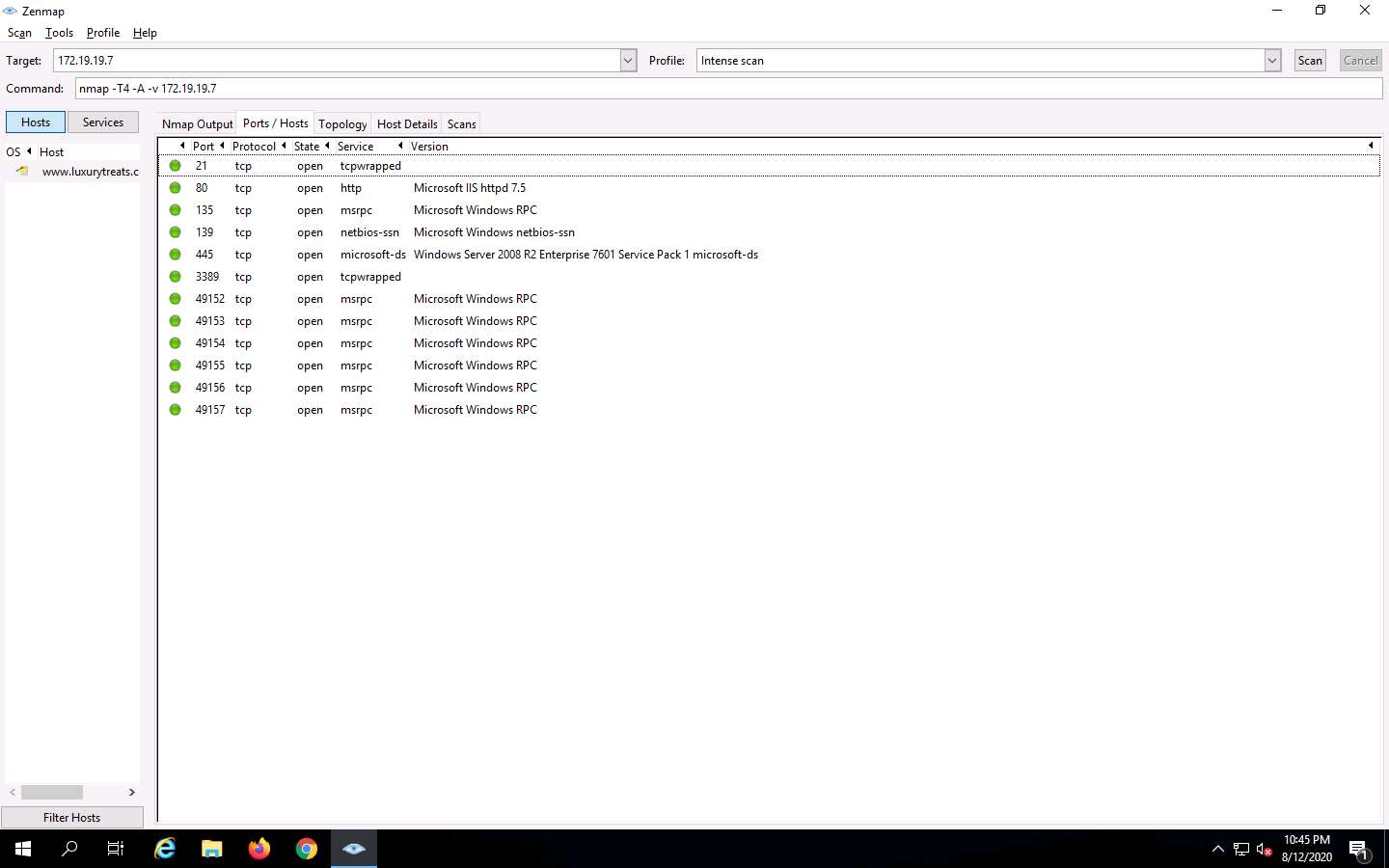


1. Nmap scans the provided IP address with Intense scan and scan results are shown in the **Nmap Output** tab.

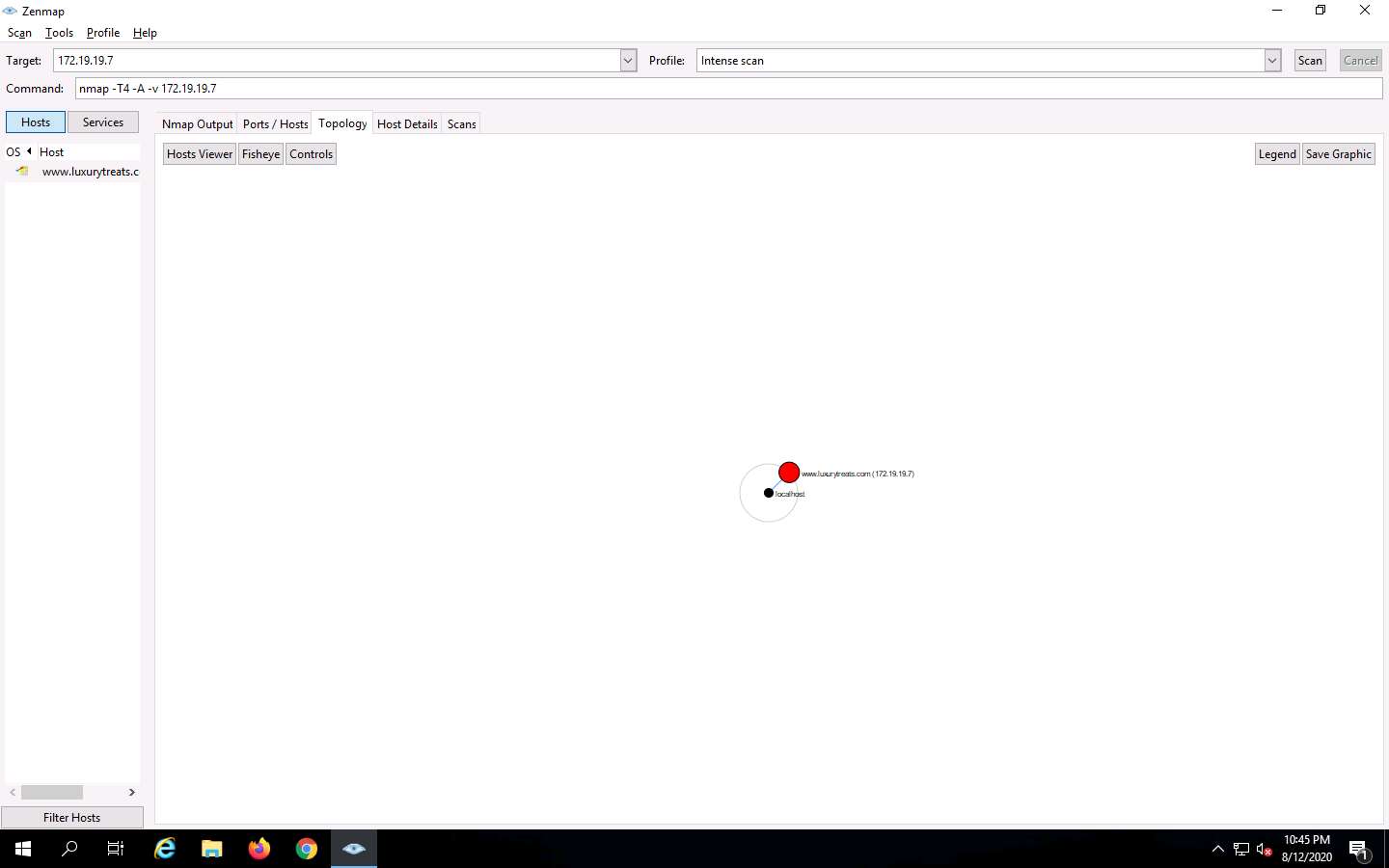
Scan results may vary in your lab environment.



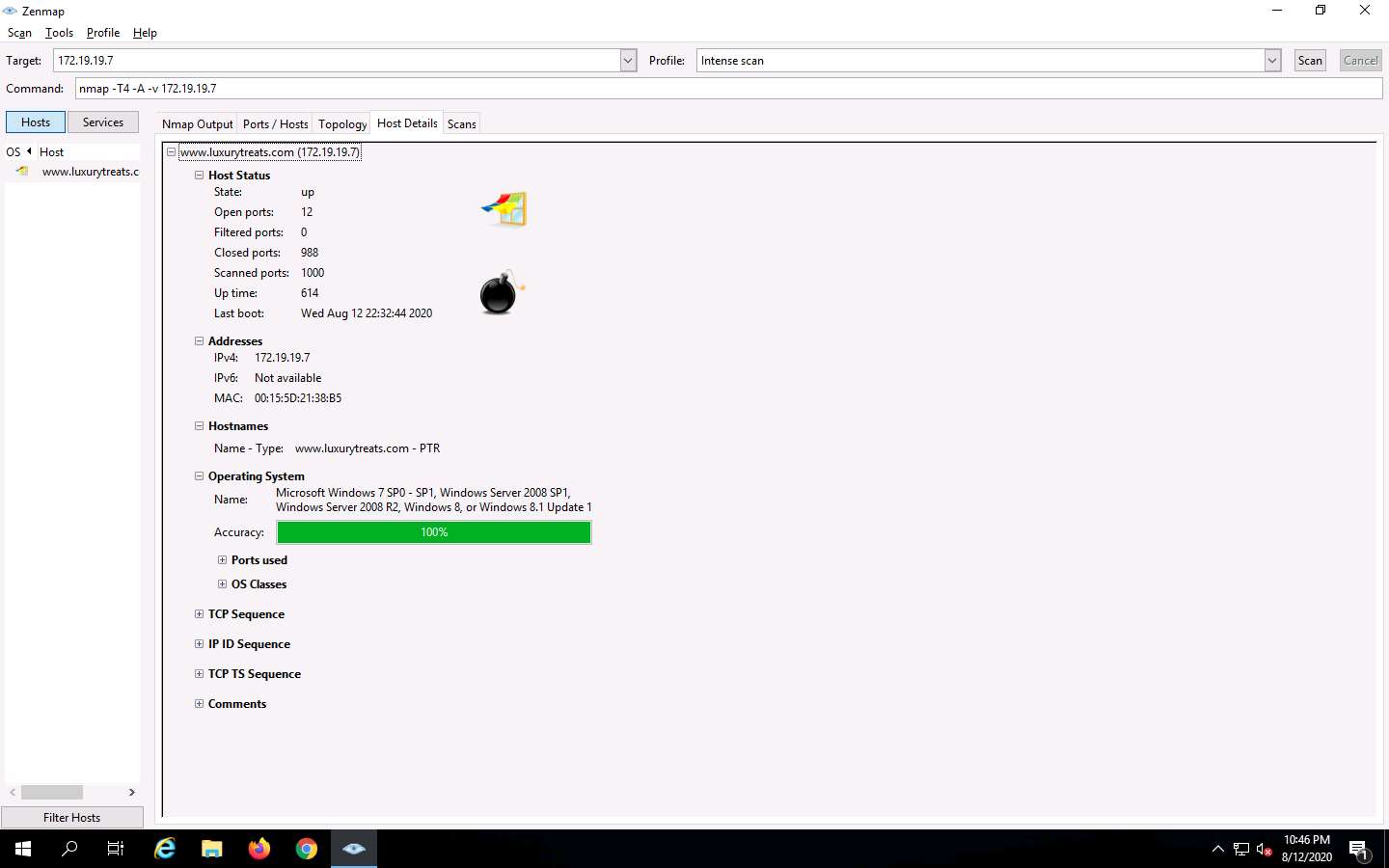
1. Click the **Ports/Hosts** tab to check the Port, Protocol, State, Service, and Version of services discovered during the scan.



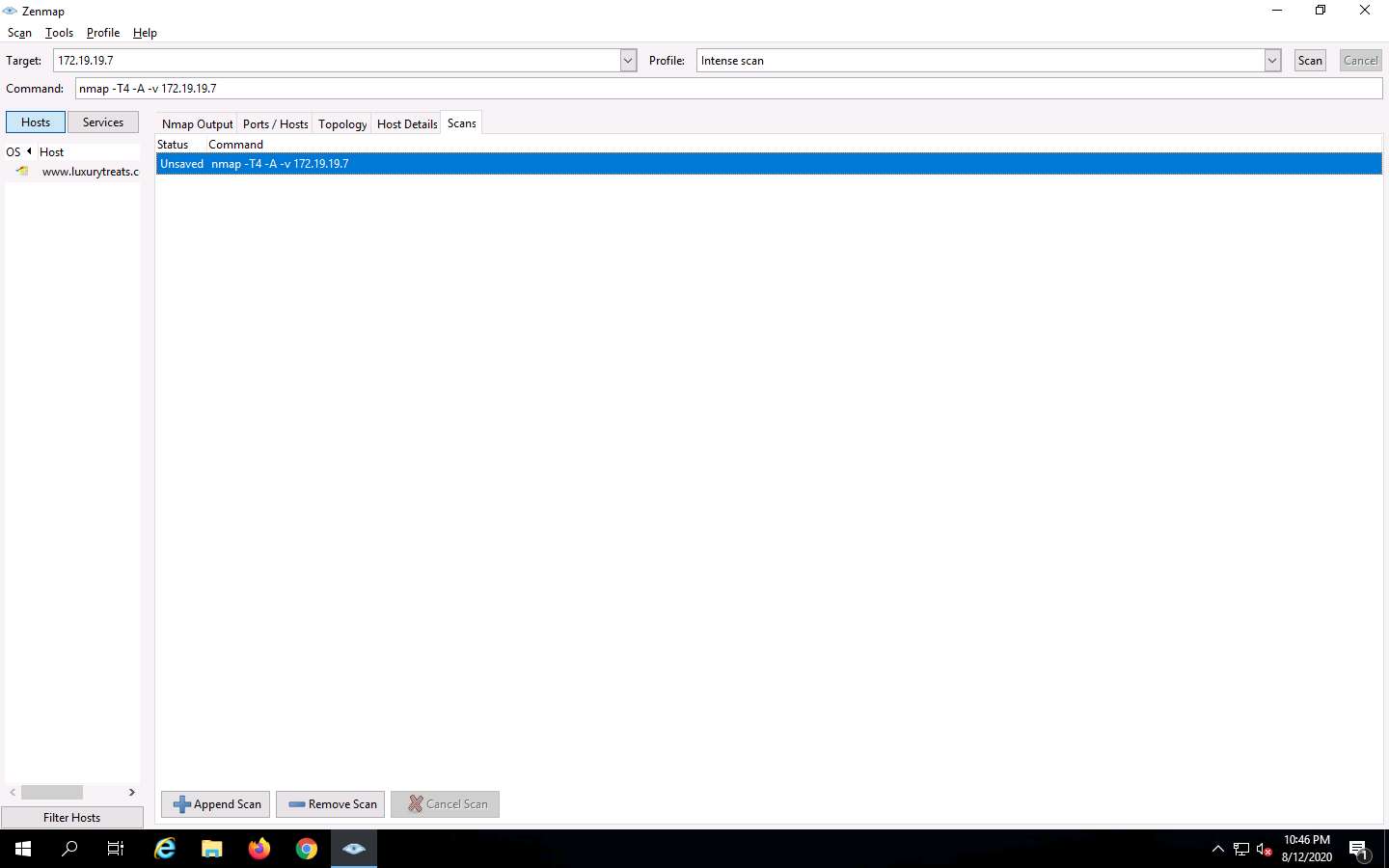
1. Click the **Topology** tab to view network topology of the target system.



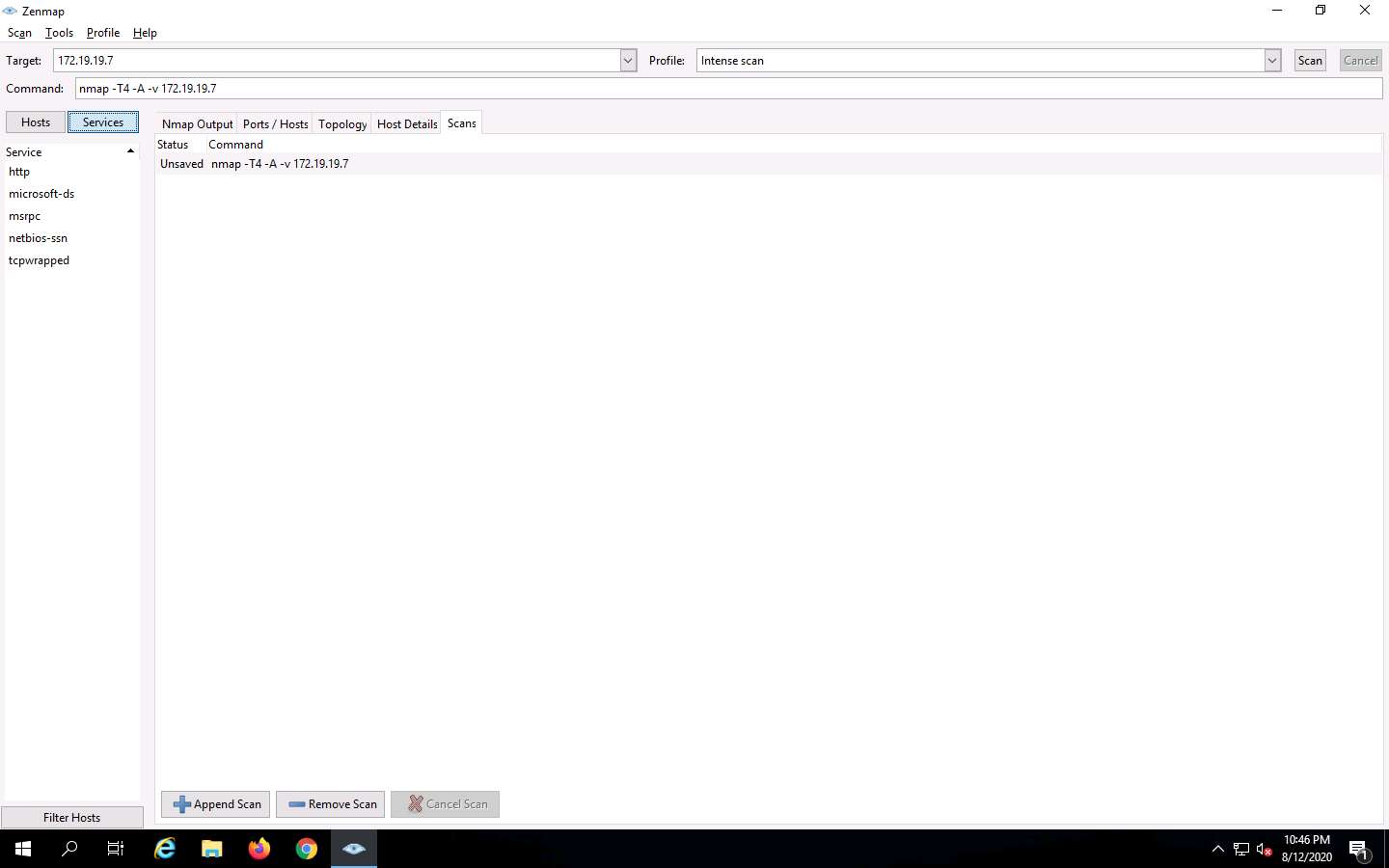
1. Click the **Host Details** tab to see the details of the hosts discovered during the intense scan.



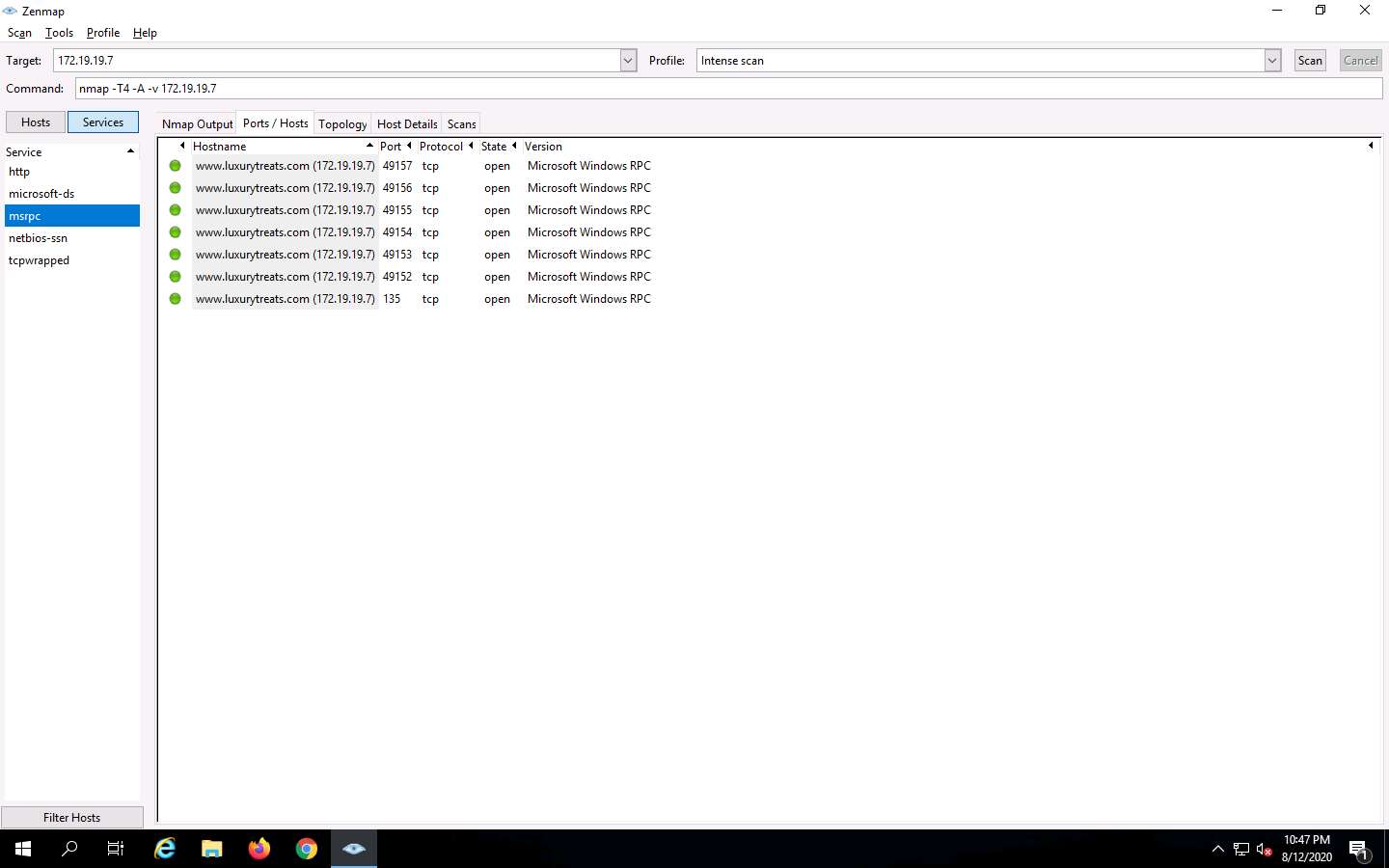
1. Click the **Scans** tab to view the status of the scan, and command used.



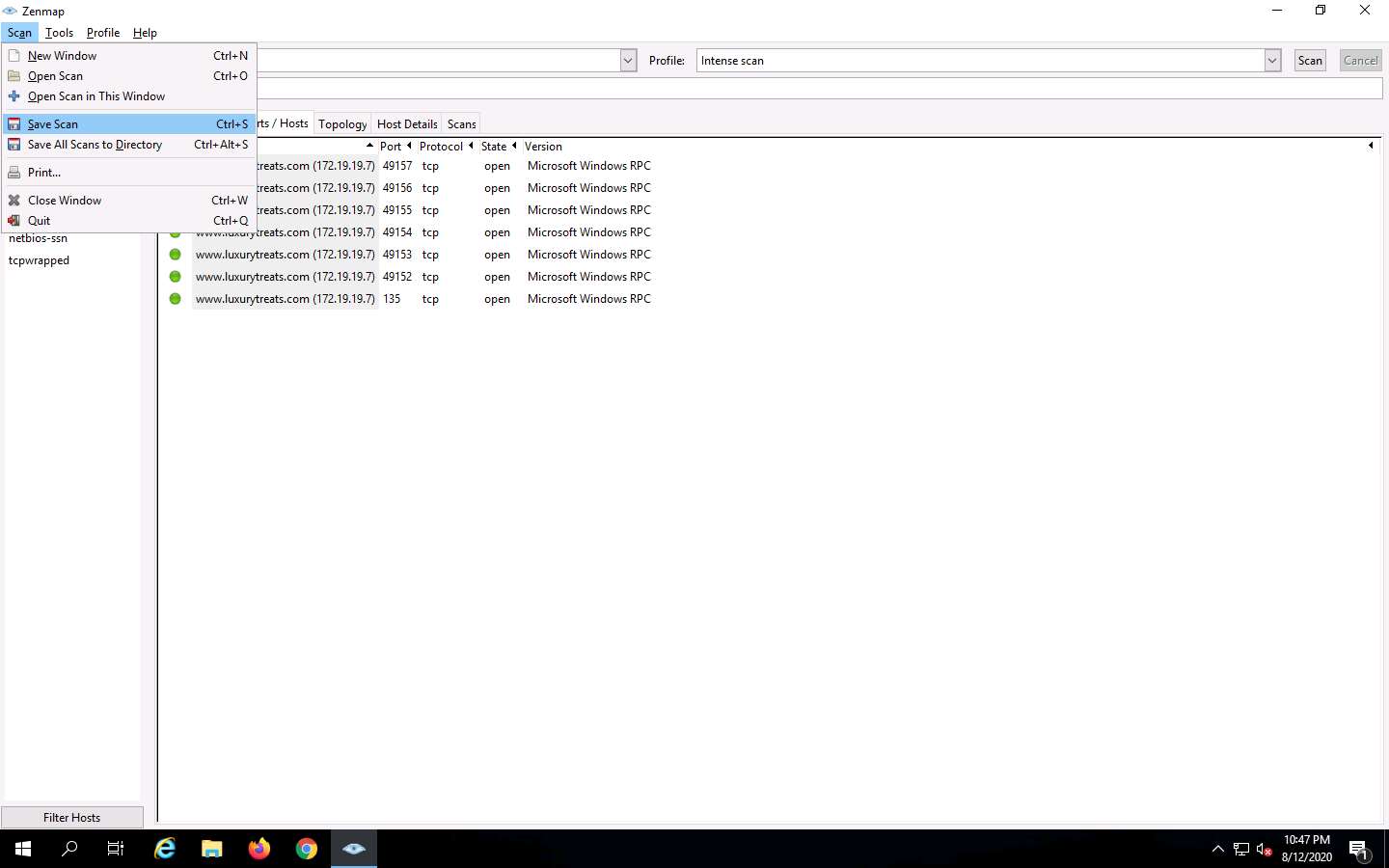
1. Now, click the **Services** tab in the left pane. This tab displays the list of services running on the machine.



1. Now, click **msrpc** service under **Services** section to view the ports on which the services are running. This way, you can access information about each service.



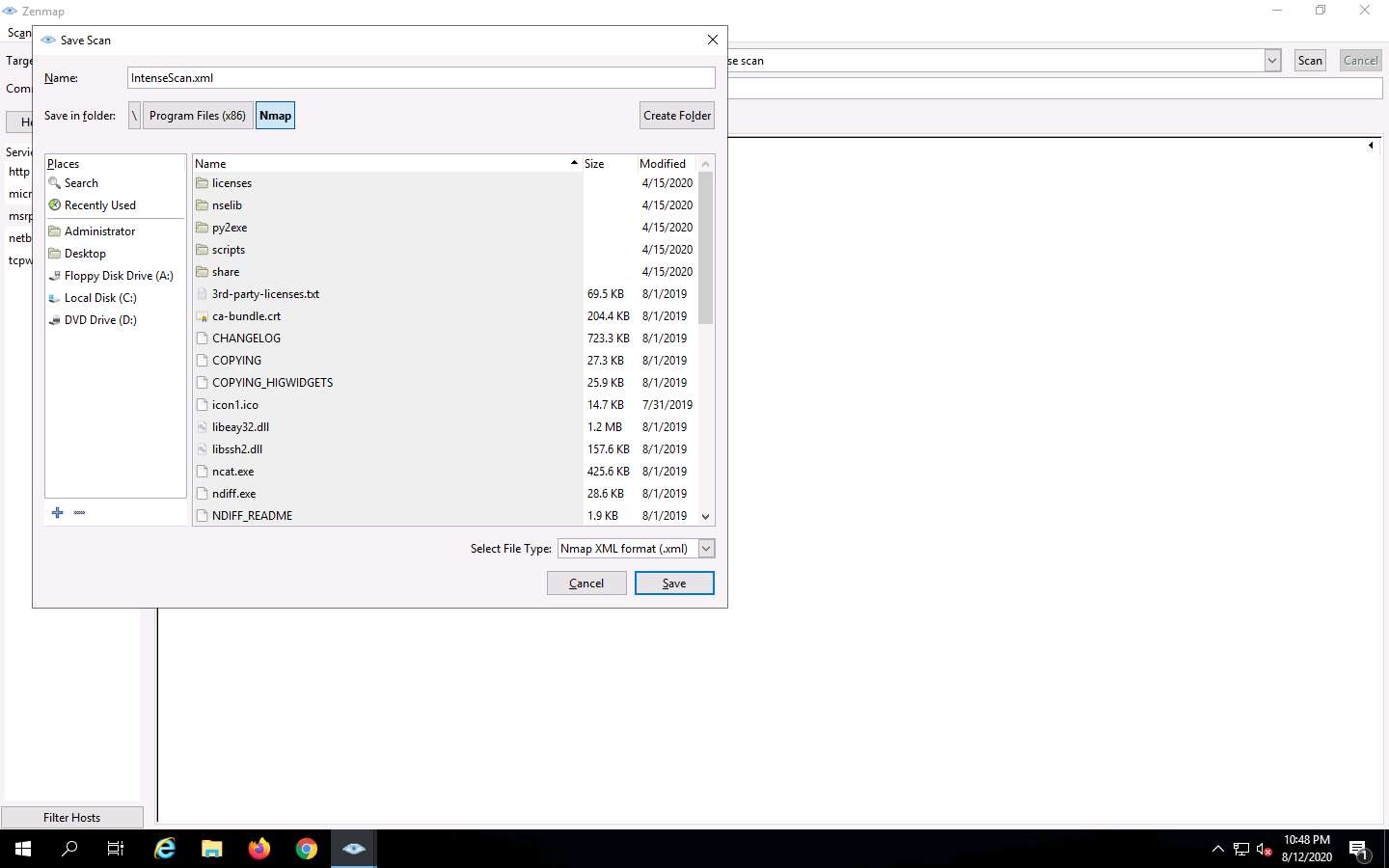
1. To save the scanned result, navigate to **Scan** and click **Save Scan** from the menu bar.



1. **Save Scan** window appears, specify the scan name in the **Name:** text field as **Intense Scan.xml**, specify the destination location in **Save in folder:** field, file type in **Select File Type:** field and click **Save**.

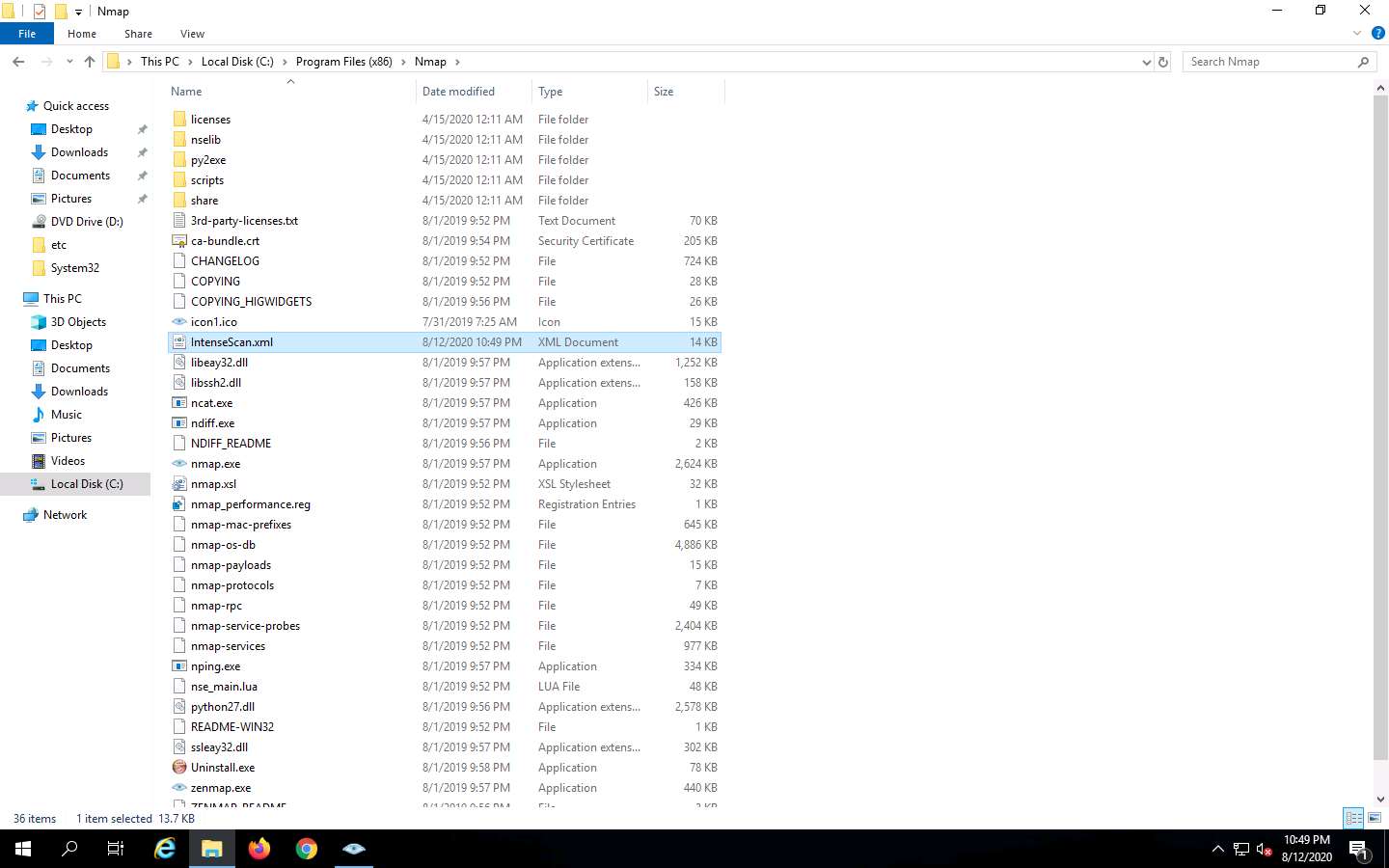
In this lab, the default file location and default file type have been chosen.

You can even choose your desired location to save the result.

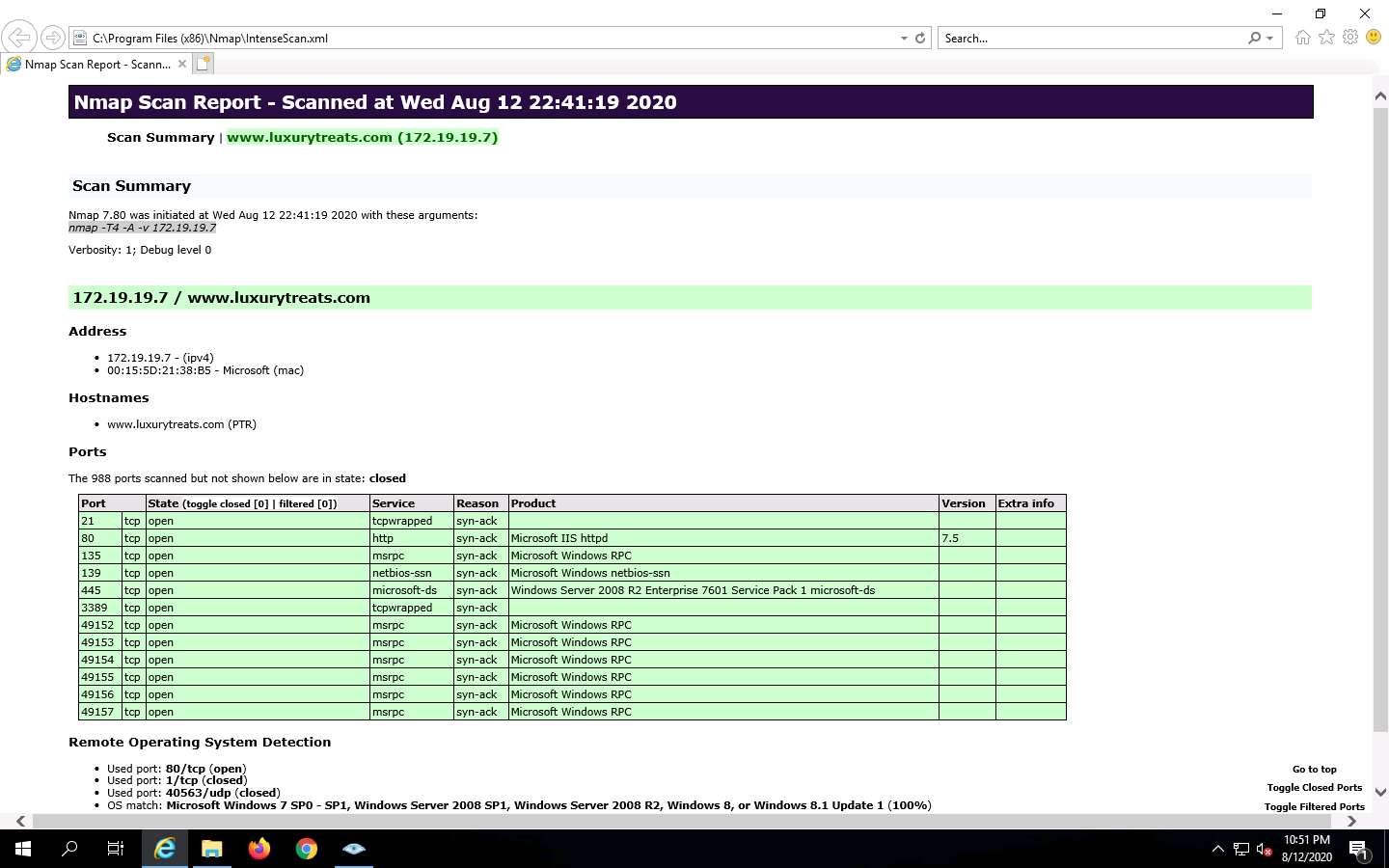


1. To view the result, navigate to **C:\Program Files (x86)\Nmap** and double-click **Intense Scan.xml**.

Here, the saved file location is **C:\Program Files (x86)\Nmap**.



1. Now, you can view the **Intense Scan** report in the browser as shown in the screenshot.



1. Now, close all the windows.

If **Errors Occurred** pop-up appears, click **OK**.

1. After analyzing the results in the report, close all the windows and the Nmap GUI.

In this lab you have analyzed all the IP addresses, open and closed ports, services, and protocols you discovered during the scan.