Lab – Detecting Threats and Vulnerabilities (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

1. Objectives

Use Nmap, a port scanner and network mapping tool to detect threats and vulnerabilities on a system.

1. Background / Scenario

Network Mapper, or Nmap, is an open source utility used for network discovery and security auditing. Administrators also use Nmap for monitoring hosts or managing service upgrade schedules. Nmap determines what hosts are available on a network, what services are running, what operating systems are running, and what packet filters or firewalls are running.

1. Required Resources

* PC with Ubuntu 16.0.4 LTS installed in a VMware workstation.
  1. Open a terminal window in Ubuntu.
     1. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**



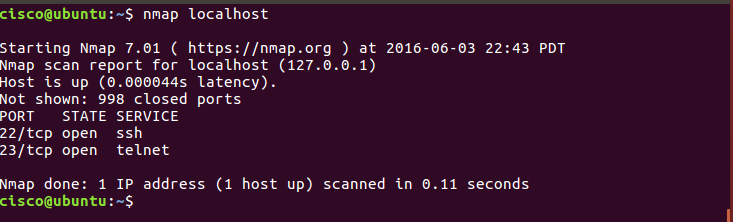
* + 1. Click on the **terminal** icon to open a terminal.



* 1. Run Nmap.

At the command prompt, enter the following command to run a basic scan against this Ubuntu system:

cisco@ubuntu:~$ **nmap localhost**



The results are a scan of the first 1024 TCP ports.

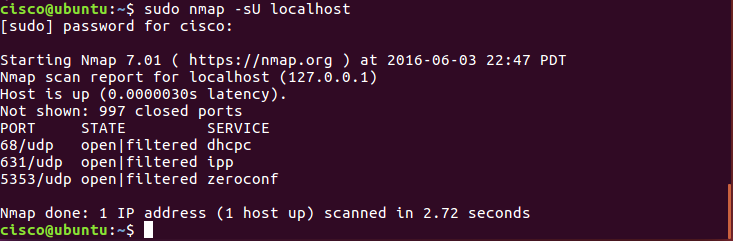
What TCP ports are open?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ports 22, 23, and 631

* 1. Use administrative privileges with Nmap.
     1. Type the following command in the terminal to scan the computer’s UDP ports (remember, Ubuntu is case sensitive) and enter the password **password** when prompted:

cisco@ubuntu:~$ **sudo nmap –sU localhost**



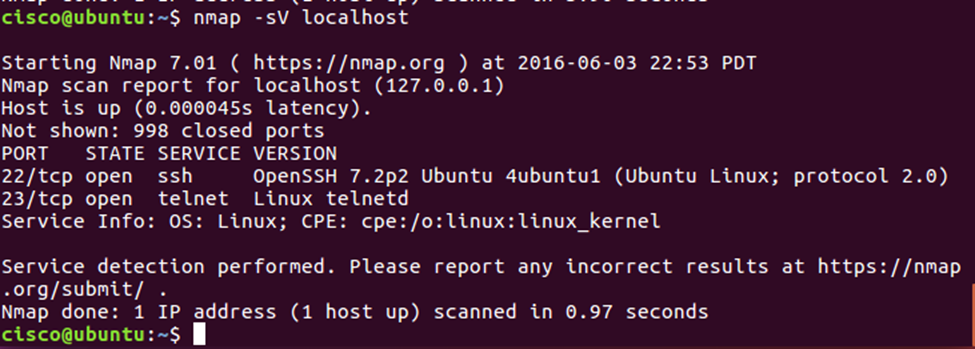
What UDP ports are open?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ports 68, 631, and 5353

* + 1. Type the following command in the terminal:

cisco@ubuntu:~$ **nmap –sV localhost**

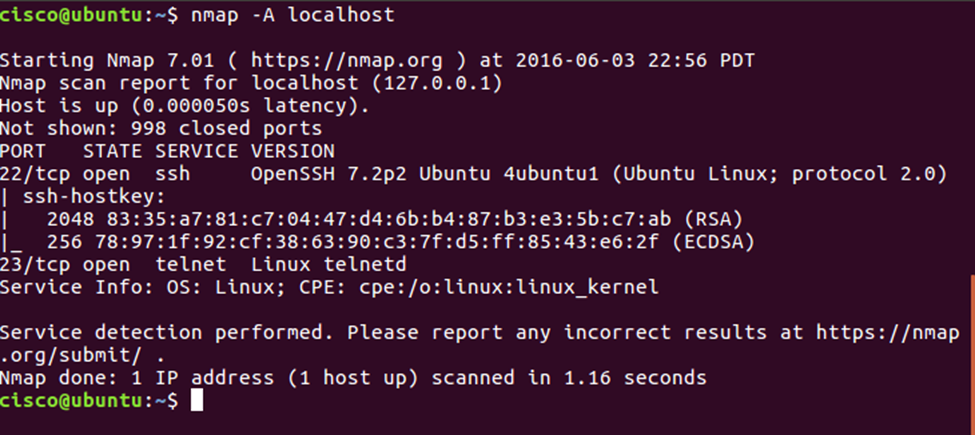


Using the **–sV** switch with the **nmap** command performs a version detection which you can use to research vulnerabilities.

* 1. Capture SSH keys.

Type the following command in the terminal to initiate a script scan:

cisco@ubuntu:~$ **nmap –A localhost**



You captured the SSH keys for the host system. The command runs a set of scripts built into Nmap to test specific vulnerabilities.

**References**

Nmap: <https://nmap.org/>