**NETWORK FINGERPRINTING**



**Submitted by:** Spencer Vital

**Date:** 03/23/2023

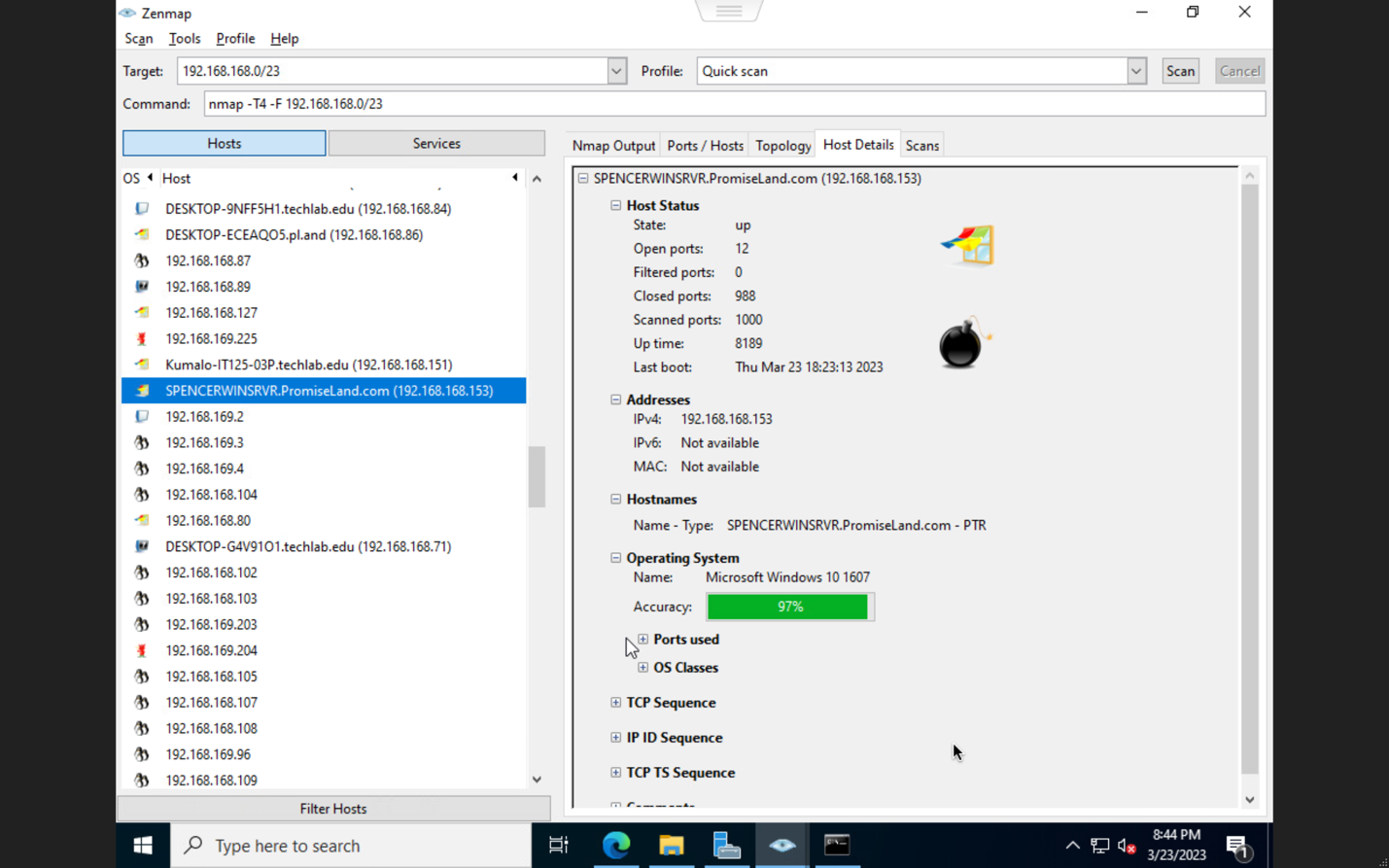
**Class:** IT255

The project involved conducting a network scan using Nmap to identify the types of devices on the network and their vulnerabilities.

The IP ranges for the scan were determined by analyzing the network topology and identifying subnets. A total of 217 devices were discovered, with the majority being Windows-based machines.

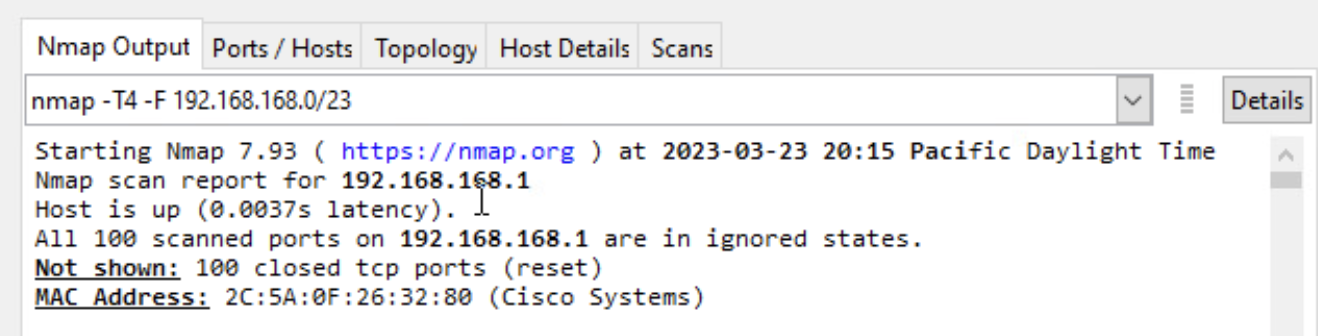
Devices were grouped based on OS. The most common OS was Windows, followed by Linux and BSD. The most common manufacturers were Intel, Hewlet Packard, Dell, and Cisco.

Based on the scan results, I have identified several machines that appear vulnerable or suspect due to the presence of open and exploitable ports such as Telnet. These machines have the following MAC addresses: 00:80:56:91:59:63, 00:50:56:91:9A:8F, 00:0C:29:AD:62:AC, 00:0C:29:29:C9:84, 00:0C:29:32:8C:1E, 00:0C:29:48:53:41, and 9A:27:68:4F:02:2A.These machines could potentially be at risk of a security breach as they have open ports that can be exploited by attackers to gain unauthorized access to the network. Telnet is a commonly exploited port that provides a potential entry point for attackers.

*A snip of the Host Details tab for the computer performing the scan*

The Nmap output provided detailed information on each device, including open ports, operating system, and network services. The output for the gateway router and one other device were provided, as well as the description for five devices from Techlab.

*Snips from the Nmap output of my gateway router and one additional device*



Graphical user interface, text, application, chat or text message

Description automatically generated

Here are the details for five devices:

1. Kumalo-IT125-03.techlab.edu - IP 192.168.168.151, Windows XP OS, 4 open ports, 96 filtered ports, 0 closed ports.
2. Desktop-G4V9101 - IP 192.168.168.71, unknown OS, 0 open ports, 100 filtered ports, 100 closed ports.
3. Desmond Liam Chaparadze.com - IP 192.168.168.39, Windows XP OS, 1 open port, 99 filtered ports, 100 scanned ports.
4. IT-235.PL.com - IP 192.168.168.148, Linux OS, 8 open ports, 0 filtered ports, 0 closed ports.
5. Desktop-FBJCMR.carson.local - IP 192.168.168.116, Windows XP OS, 1 open port, 999 filtered ports, 0 closed ports.

The project demonstrated the value of network scanning tools in discovering devices, identifying potential security risks, and optimizing network resources. It provided valuable insights into the current state of the network and helped to develop a comprehensive security strategy to mitigate potential risks.