Network Administration

Prepared by: Anastasiya Gruneva

Date: December 9th, 2024

Executive Summary/Introduction

We demonstrate the use of Nmap, a network scanning tool, to monitor and analyze network activity. This scenario focuses on utilizing Nmap to identify key attributes of two virtual machines—LinuxServer and Windows11—through detailed scans and traffic monitoring.

The goal is to:

- Identify Network and Host Details: Gather information such as IP addresses, operating systems, open ports, and running services.
- Monitor Network Traffic: Capture real-time packet data using Wireshark to complement findings from Nmap.
- Assess Security Posture: Evaluate open ports and services to understand potential vulnerabilities.

By combining Nmap's scanning capabilities with Wireshark's packet analysis, this example highlights how these tools can be effectively used to monitor and secure networks, detect unauthorized activity, and troubleshoot connectivity issues.

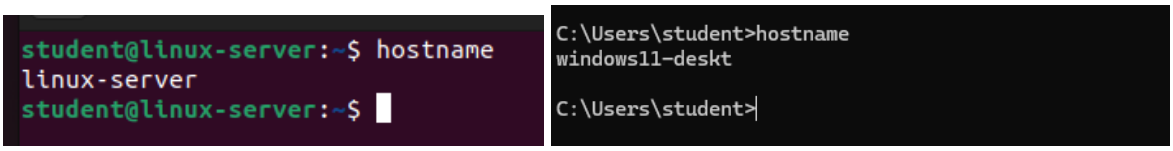
Network Devices Information

Nmap and Wireshark are two powerful tools widely used by cybersecurity professionals for network analysis and monitoring. **Nmap** (Network Mapper) is an open-source utility designed to scan networks and identify connected devices, their services, and open ports. It is frequently used to detect potential vulnerabilities in network infrastructure (*Nmap, retrieved 2024-12-10*). **Wireshark**, on the other hand, is a network traffic analyzer that allows for in-depth examination of data packets in real time. This tool helps identify network issues, detect threats, and analyze application behavior within the network (*Wireshark, retrieved 2024-12-10*). Together, these tools play a vital role in securing information systems.

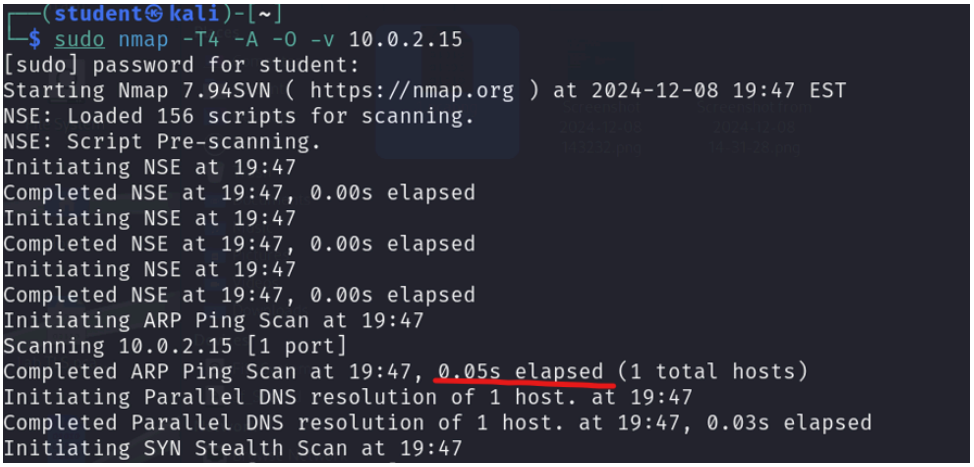
Device	1	2
Machine designation	LinuxServer	Windows11
Device Host Name	linux-server	windows11-deskt
IP address	10.0.2.15	10.0.2.4
MAC address	08:00:27:DD:D8:F8	08:00:27:CB:20:4A
Operating System & version	Linux 4.15-5.8	Microsoft Windows 11 21H2 (97% guess)

Open ports with associated services	21/tcp open ftp 80/tcp open http 3306/tcp open mysql	80/tcp open http
ARP Ping Scan elapsed time	0,05s	0,04s

Pic. 1. Network devices information



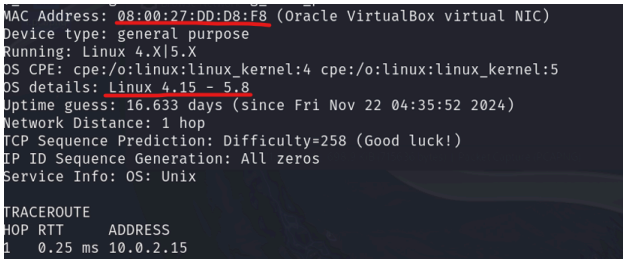
Pic. 2. Determining the hostname using the `hostname` command in the command line.

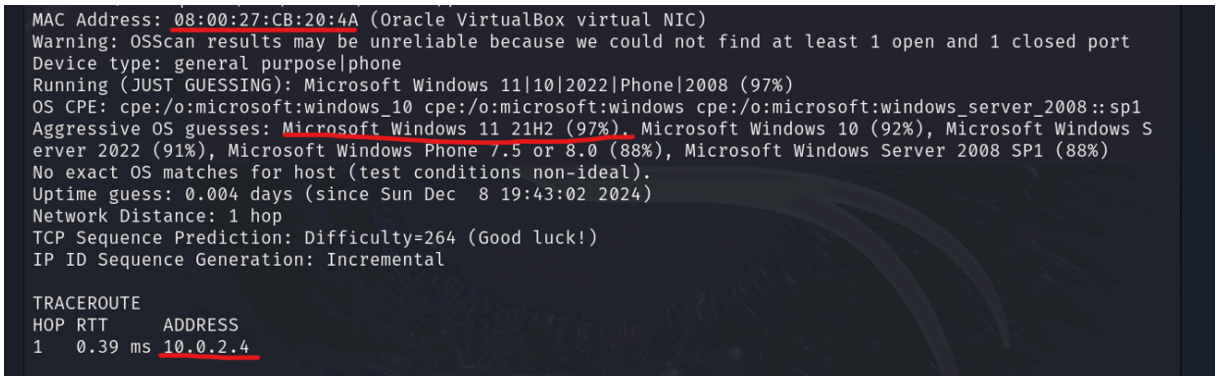


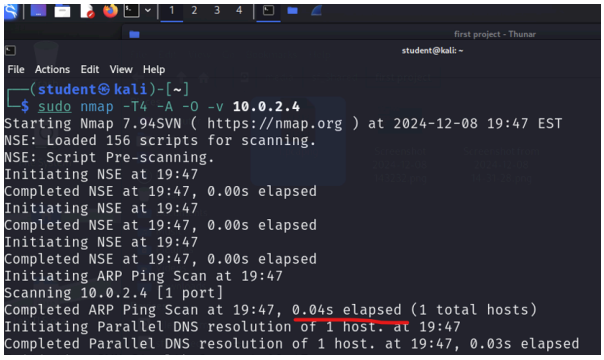
Pic.3. The command `sudo nmap -T4 -A -O -v 10.0.2.15` is used to perform a detailed scan of the target IP address `10.0.2.15` with administrative privileges. Here's a breakdown:

- `sudo`: Runs the command with administrative privileges.
- `nmap`: Invokes the Nmap tool.
- `-T4`: Sets the timing template to "aggressive," making the scan faster.
- `-A`: Enables advanced scanning, including OS detection, version detection, script scanning, and traceroute.
- `-O`: Enables OS detection specifically.
- `-v`: Increases verbosity, providing more detailed output during the scan.
- `10.0.2.15`: The target IP address to be scanned.

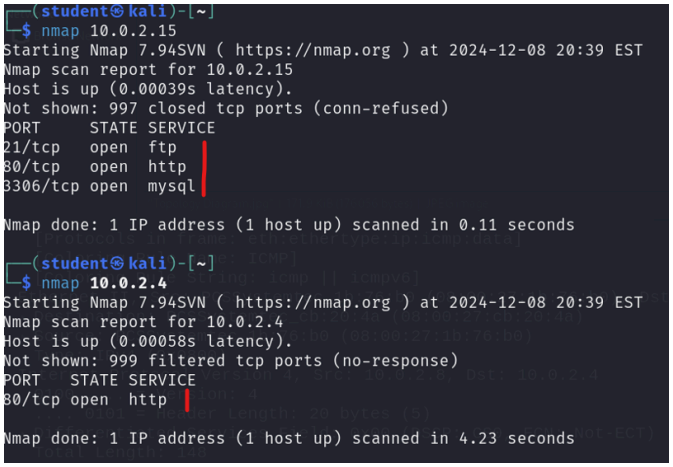
This command provides detailed information about the target's open ports, services, OS, and network details.



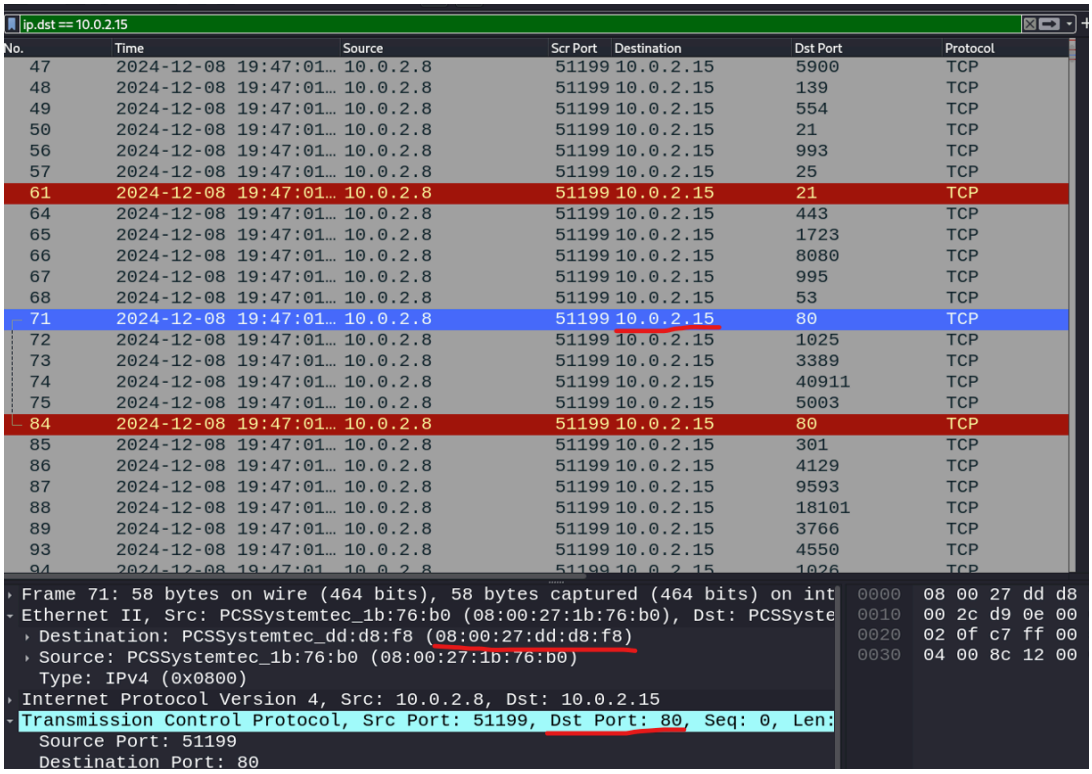




Pic 4-6. The images show the results of the above-mentioned team, where we can see, for example, IP address, MAC address, Operating System & version, and ARP Ping Scan elapsed time.



Pic. 7. The command `nmap` is used to perform a scan to determine open ports.



Pic. 8. Wireshark is used to determine Mac addresses and open ports.

Information Collection Methodology

Step 1:
Start all virtual machines.

Step 2:
Determine the IP addresses of the LinuxServer and Windows11 machines:

On the **LinuxServer**, use the command:
`ip a`
On the **Windows11 machine**, open the Command Prompt and use:
`ipconfig`

Step 3:
Begin capturing network traffic in Wireshark on the **Ethernet** interface.

Step 4:
Perform an Nmap scan on both machines:

Use the following command for a detailed scan:
`sudo nmap -T4 -A -O -v <IP address>`

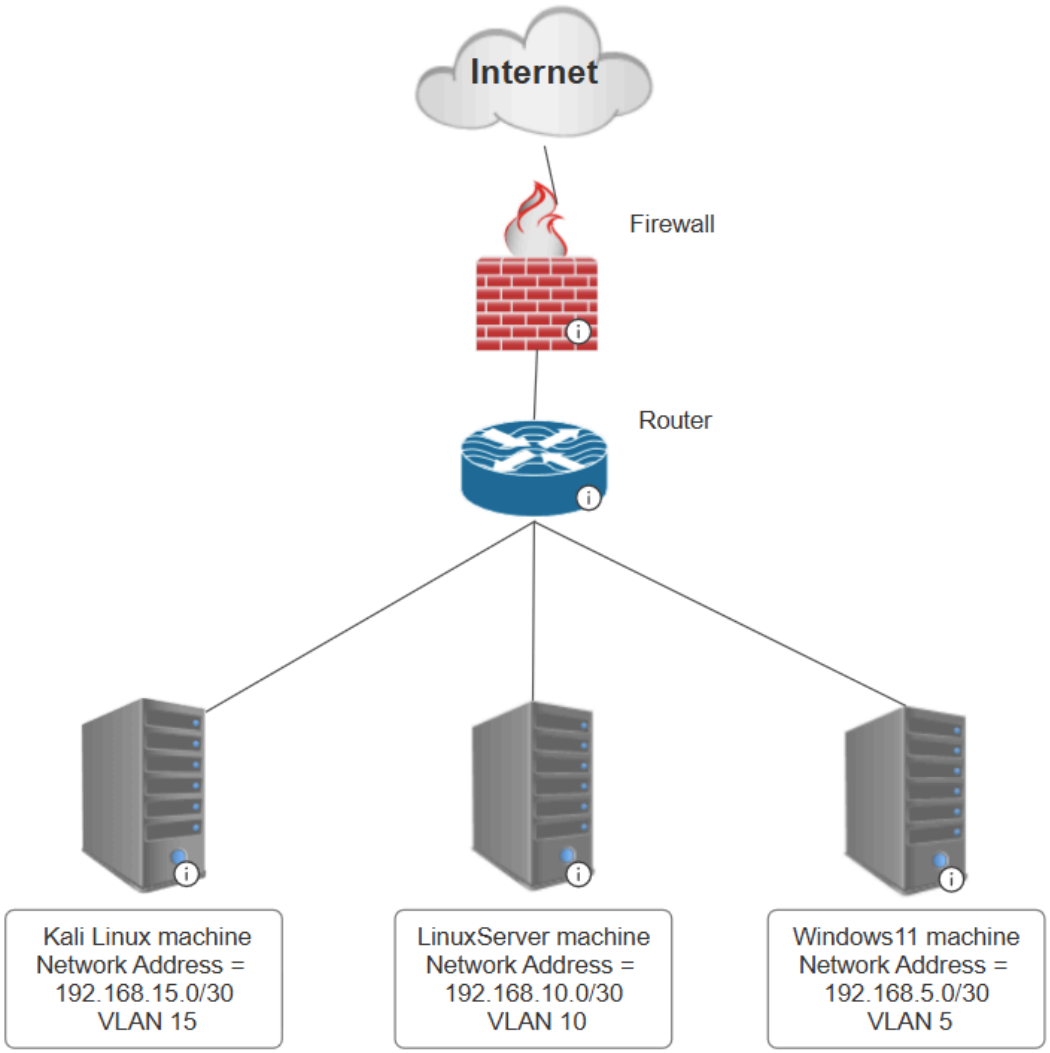
Run a basic scan to confirm connectivity:
`nmap <IP address>`

Step 5:
Analyze the results:

Collect and document information from the Nmap scan output, such as open ports, services, and OS details.

Examine the captured traffic from Wireshark for additional insights.

Recommended Topology



References

What's an example of a cybersecurity executive summary? Bitsight. (retrieved 2024-12-08). https://www.bitsight.com/glossary/cybersecurity-executive-summary-example

Writing a cybersecurity report executive summary (inc.. examples): Upguard. RSS. (11.18.2024). https://www.upguard.com/blog/writing-a-cybersecurity-executive-summary

Nmap(1) - linux man page. (retrieved 2024-12-08). https://linux.die.net/man/1/nmap

A unified visual collaboration app. SmartDraw. (retrieved 2024-12-08). https://www.smartdraw.com/

Wireshark · go deep. Wireshark. (retrieved 2024-12-08). https://www.wireshark.org/

Nmap. (retrieved 2024-12-08). https://nmap.org/