



Network Administration

Prepared by: Anastasiya Gruneva

Date: December 9th, 2024



Executive Summary/Introduction.....3

Network Devices Information..... 3

Information Collection Methodology..... 6

Recommended Topology.....7

References..... 8



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

```
student@linux-server:~$ hostname
linux-server
student@linux-server:~$
```

```
C:\Users\student>hostname
windows11-deskt
C:\Users\student>
```

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

```
(student@kali)-[~]
└─$ sudo nmap -T4 -A -O -v 10.0.2.15
[sudo] password for student:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 19:47 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:47
Completed NSE at 19:47, 0.00s elapsed
Initiating NSE at 19:47
Completed NSE at 19:47, 0.00s elapsed
Initiating NSE at 19:47
Completed NSE at 19:47, 0.00s elapsed
Initiating ARP Ping Scan at 19:47
Scanning 10.0.2.15 [1 port]
Completed ARP Ping Scan at 19:47, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:47
Completed Parallel DNS resolution of 1 host. at 19:47, 0.03s elapsed
Initiating SYN Stealth Scan at 19:47
```

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.



```
MAC Address: 08:00:27:DD:D8:F8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Uptime guess: 16.633 days (since Fri Nov 22 04:35:52 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE
HOP RTT ADDRESS
1 0.25 ms 10.0.2.15
```

```
MAC Address: 08:00:27:CB:20:4A (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 11|10|2022|Phone|2008 (97%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008::sp1
Aggressive OS guesses: Microsoft Windows 11 21H2 (97%), Microsoft Windows 10 (92%), Microsoft Windows S
erver 2022 (91%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows Server 2008 SP1 (88%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.004 days (since Sun Dec 8 19:43:02 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE
HOP RTT ADDRESS
1 0.39 ms 10.0.2.4
```

```
File Actions Edit View Help
student@kali ~
[student@kali]~$ sudo nmap -T4 -A -O -v 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 19:47 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:47
Completed NSE at 19:47, 0.00s elapsed
Initiating NSE at 19:47
Completed NSE at 19:47, 0.00s elapsed
Initiating NSE at 19:47
Completed NSE at 19:47, 0.00s elapsed
Initiating ARP Ping Scan at 19:47
Scanning 10.0.2.4 [1 port]
Completed ARP Ping Scan at 19:47, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:47
Completed Parallel DNS resolution of 1 host. at 19:47, 0.03s elapsed
```

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.

```
[student@kali]~$ nmap 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 20:39 EST
Nmap scan report for 10.0.2.15
Host is up (0.00039s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
30/tcp    open  http
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

[student@kali]~$ nmap 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 20:39 EST
Nmap scan report for 10.0.2.4
Host is up (0.00058s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
30/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
```

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



ip.dst == 10.0.2.15						
No.	Time	Source	Scr Port	Destination	Dst Port	Protocol
47	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	5900	TCP
48	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	139	TCP
49	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	554	TCP
50	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	21	TCP
56	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	993	TCP
57	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	25	TCP
61	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	21	TCP
64	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	443	TCP
65	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	1723	TCP
66	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	8080	TCP
67	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	995	TCP
68	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	53	TCP
71	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	80	TCP
72	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	1025	TCP
73	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	3389	TCP
74	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	40911	TCP
75	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	5003	TCP
84	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	80	TCP
85	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	301	TCP
86	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	4129	TCP
87	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	9593	TCP
88	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	18101	TCP
89	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	3766	TCP
93	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	4550	TCP
94	2024-12-08 19:47:01...	10.0.2.8	51199	10.0.2.15	1025	TCP

Frame 71: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface
Ethernet II, Src: PCSSystemtec_1b:76:b0 (08:00:27:1b:76:b0), Dst: PCSSystemtec_dd:d8:f8 (08:00:27:dd:d8:f8)
Destination: PCSSystemtec_dd:d8:f8 (08:00:27:dd:d8:f8)
Source: PCSSystemtec_1b:76:b0 (08:00:27:1b:76:b0)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 51199, Dst Port: 80, Seq: 0, Len: 0
Source Port: 51199
Destination Port: 80

0000 08 00 27 dd d8
0010 00 2c d9 0e 00
0020 02 0f c7 ff 00
0030 04 00 8c 12 00

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>`

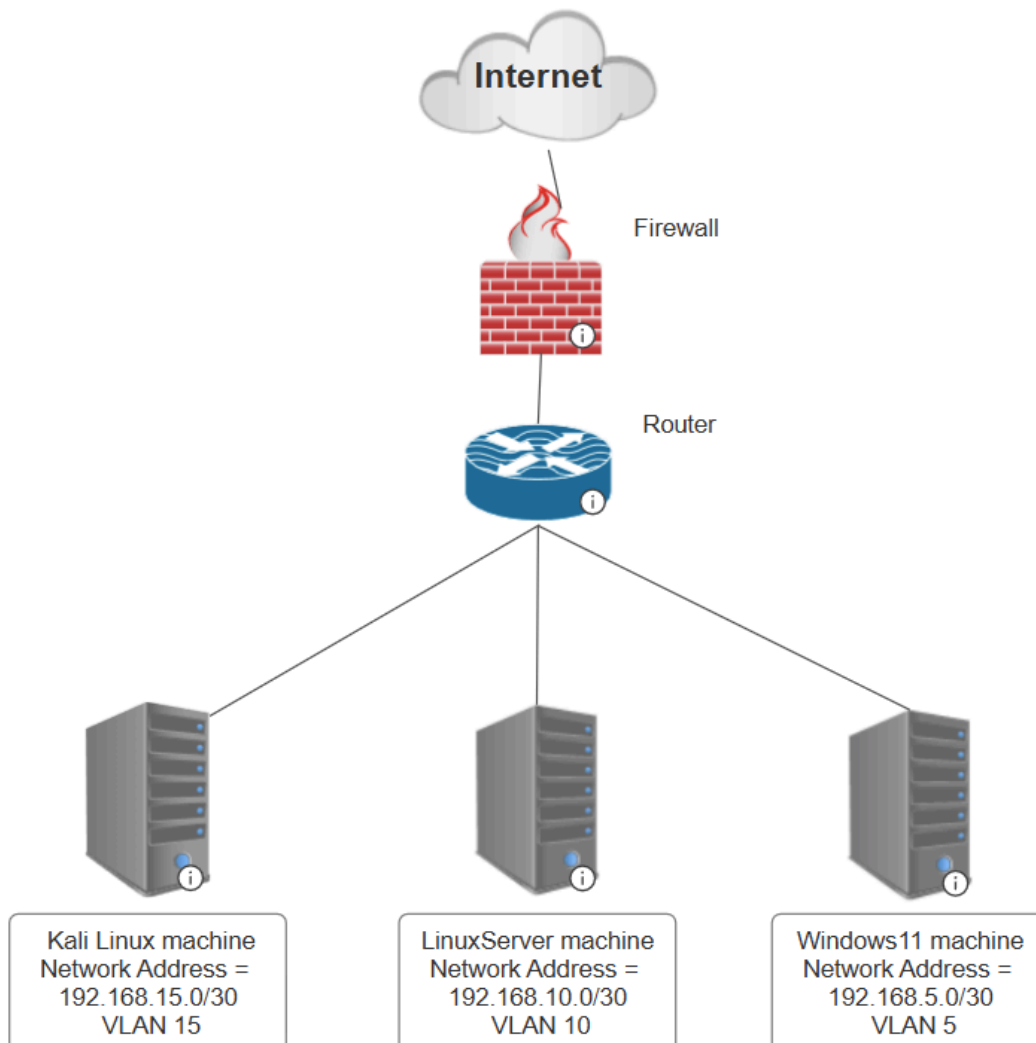
Step 5:

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/>