**LAB12 ZENMAP WIN or LINUX**

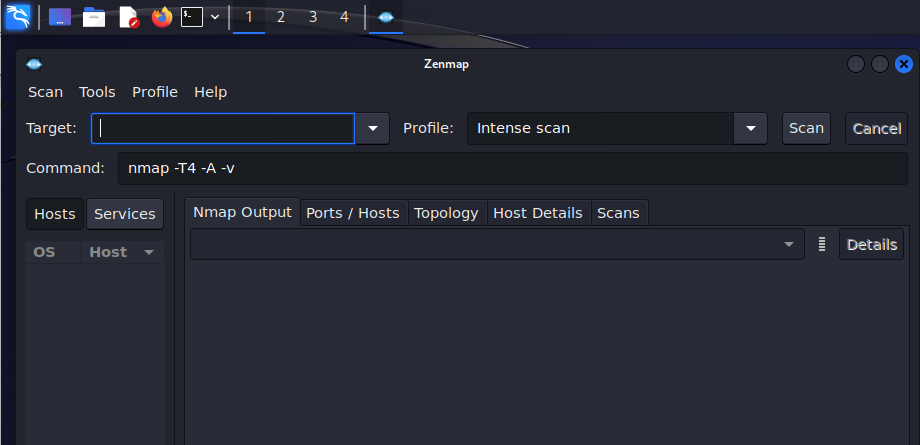
**Class: M04 Name: Truong Dang Truc Lam Student ID: B2111933**

1. **Design Zenmap scanning pen-test scenario**

|  | scanner | target |
| --- | --- | --- |
| OS | Kali Linux | Windows |
| IP address | Test - bed host IP  192.168.1.55 | **Don’t scan other systems(including google.com), instead use test-bed IP**  Localhost:  CTU IP: 123.30.143.225  CICT IP: 123.30.143.202  Neighboring PC IP:  VM IP(Ubuntu, Centos): |
| scanning program | Zenmap Linux |
| scanning types | scanin profile field  scan in command field  scan inmenu bar |

1. Install Zenmap on Window or on Ubuntu (select one)

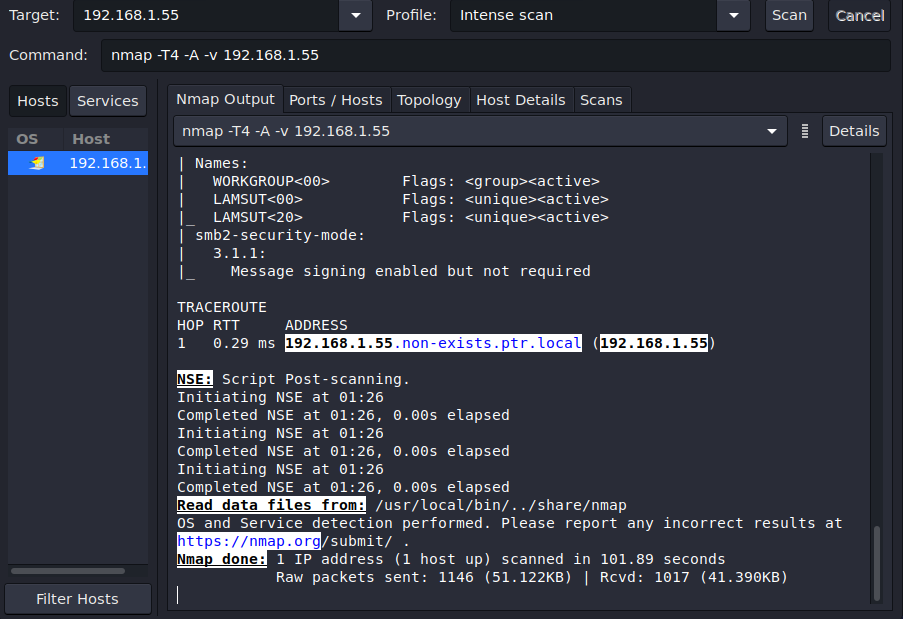
I will install Zenmap on Kali Linux instead



Zenmap on Kali Linux

**2. in profile field, scan and explain the result**

1. Intense Scan Command: nmap -T4 -A -v *<target>*

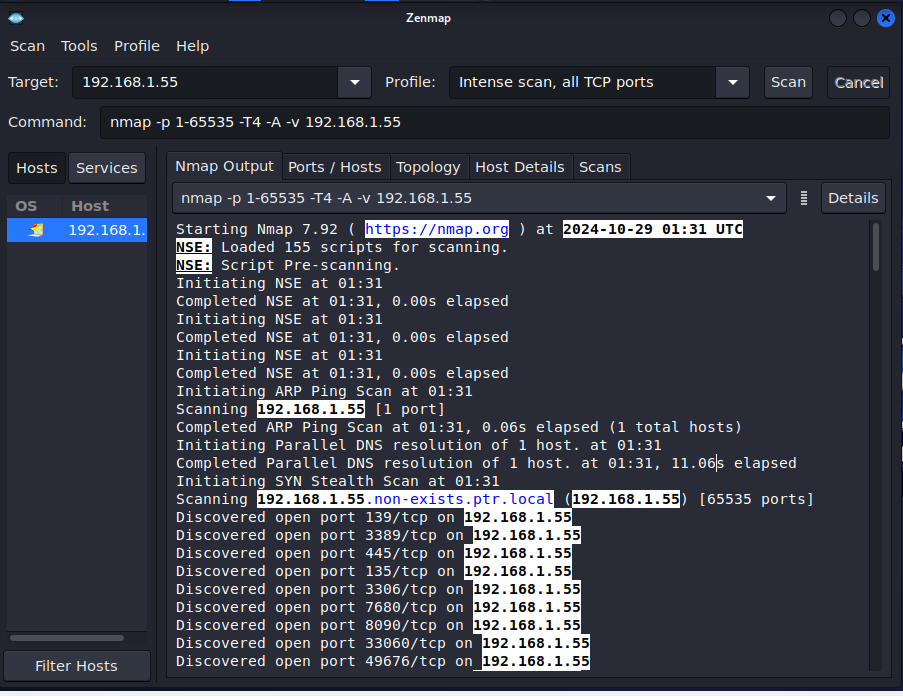


nmap -T4 -A -v 192.168.1.55

An Nmap scan was run on 192.168.1.55 with aggressive timing (T4), scanned all ports (1-65535), performed extensive operating system detection with version enumeration (-v), and ran additional scripts to identify services and vulnerabilities (-A).

The scan revealed several open ports commonly used for services like MySQL, Microsoft Remote Desktop, a basic web server, and PostgreSQL. The device was identified as Microsoft Windows 10 (version 1703) with the hostname LAMSUT. SMB is enabled with message signing but not required for security.

1. Intense Scan, all TCP Ports Command: nmap -p 1-65535 -T4 -A -v <target>

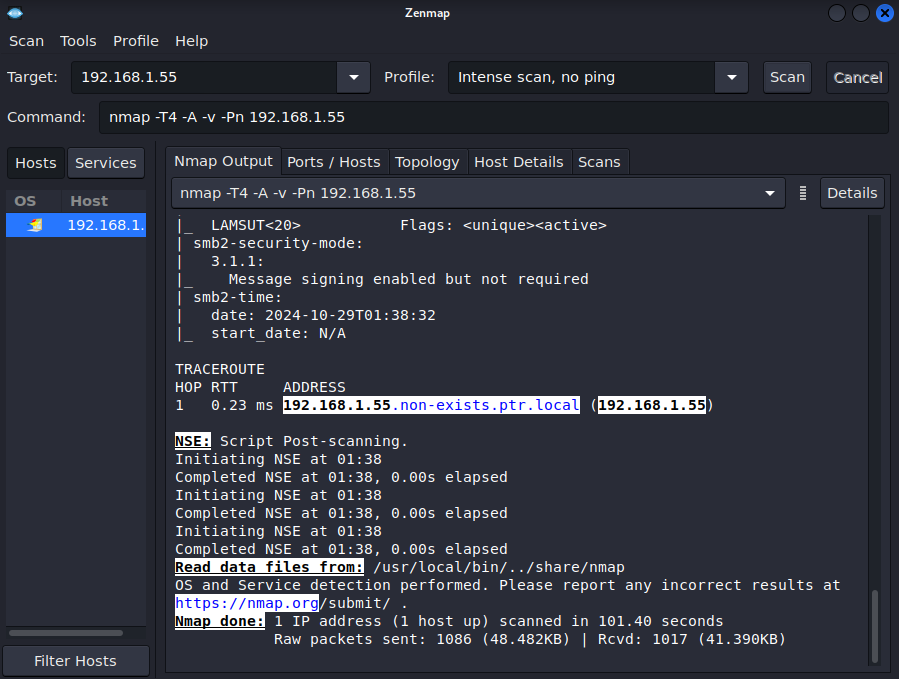


nmap -p 1-65535 -T4 -A -v 192.168.1.55

An Nmap scan was performed on the device 192.168.1.55. The scan identified several open ports including those commonly used for services like MySQL, Microsoft Remote Desktop, and a basic web server. The operating system was identified as Microsoft Windows 10 (version 1703) and the hostname is LAMSUT. The device also has SMB enabled with security mode 3.1.1, which means message signing is enabled but not required.

This scan used aggressive timing (-T4), scanned all ports (1-65535), performed a comprehensive operating system detection (-O) with version detection (-v), and ran additional scripts to identify specific services and vulnerabilities (-A)

1. Intense Scan, no ping Command: nmap -T4 -A -v -Pn <target>



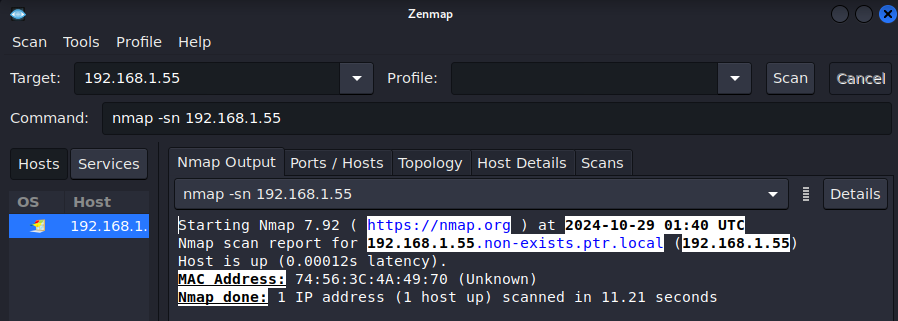
nmap -T4 -A -v -Pn 192.168.1.55

This Nmap scan (Nmap -T4 -A -v -Pn) targeted 192.168.1.55. It skipped host discovery (-Pn) assuming the device was alive. The scan aggressively timed responses (T4), scanned all ports (1-65535), performed detailed OS detection with version enumeration (-v), and ran additional scripts to identify services and vulnerabilities (-A).

The scan revealed several open ports commonly used for services like MySQL, Microsoft Remote Desktop, a basic web server, and PostgreSQL. The device was identified as Microsoft Windows 10 (version 1703) with the hostname LAMSUT. SMB is enabled with message signing but not required for security.

**3. Scan in command field, scan and explain the result**

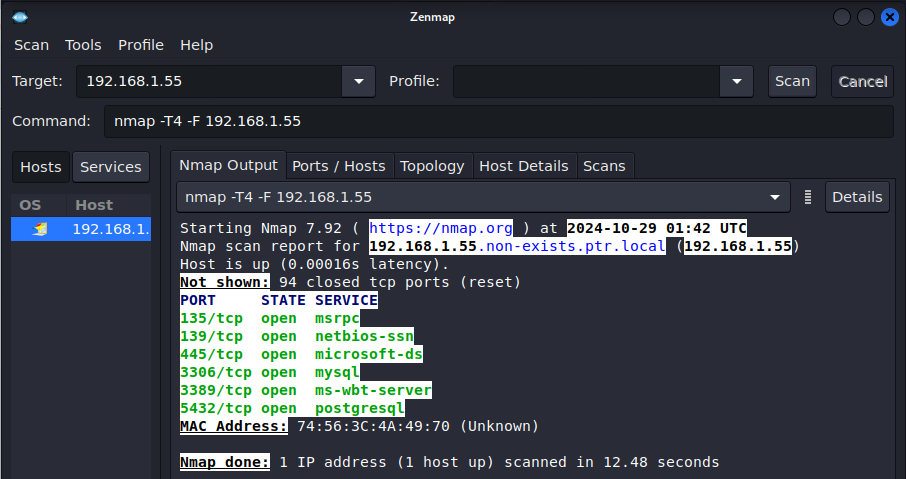
1. Ping Scan Command: nmap -sn <target>



nmap -sn 192.168.1.55

This Nmap scan (nmap -sn) focused solely on host discovery for 192.168.1.55. It skipped port scanning and service detection entirely with the "-sn" flag. The scan confirmed the device is up and responsive, reporting its MAC address (74:56:3C:4A:49:70) but not identifying any open ports or running services.

1. Quick Scan Command: nmap -T4 -F <target>

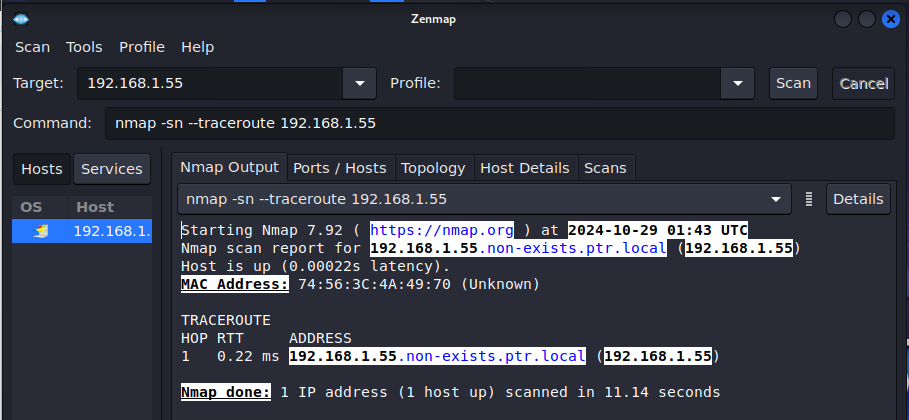


nmap -T4 -F 192.168.1.55

This Nmap scan (Nmap -T4 -F) focused on 192.168.1.55. It used aggressive timing (T4) to speed up the scan and scanned only the most common ports (F) associated with well-known services.

The scan identified several open ports including those commonly used for MySQL, Microsoft Remote Desktop, and PostgreSQL. The device's MAC address was also discovered. It did not perform any detailed OS detection or vulnerability checks.

1. Quick Trace Route Command: nmap -sn --traceroute <target>

****

nmap -sn --traceroute 192.168.1.55

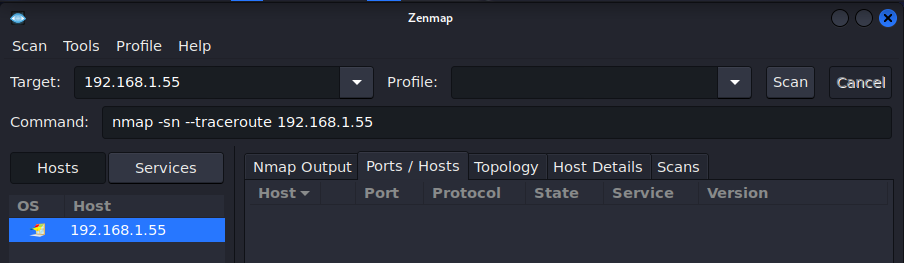
This Nmap scan (nmap -sn --traceroute) focused on determining if the device at 192.168.1.55 was reachable and the path packets take to get there. It achieved this by:

* Using the -sn flag to perform a SYN scan (ping sweep) without port scanning.
* Using the --traceroute flag to map the route packets take to reach the target.

The scan successfully identified the device as alive (0.00022s latency) and retrieved its MAC address (74:56:3C:4A:49:70). The traceroute revealed it took one hop to reach the device (192.168.1.55). This suggests the target device is directly connected to your network.

**4. Scan in menu bar explain the result**

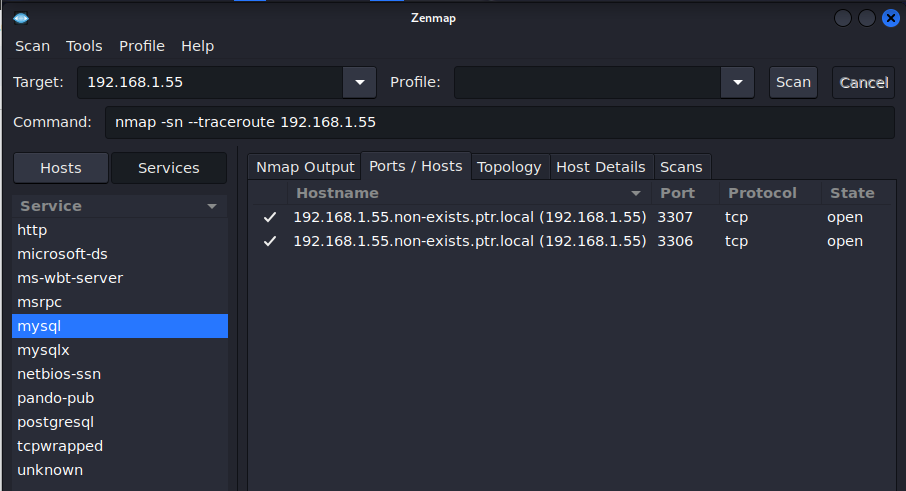
1. Press Hosts button & explain



Host

In Zenmap, a "host" refers to a specific device or computer connected to a network. It's represented by an IP address, such as 192.168.1.55 in the image. Zenmap uses this information to identify and gather details about the devices on the network, including their operating systems, open ports, and services running. This knowledge helps in network administration, troubleshooting, and security assessments.

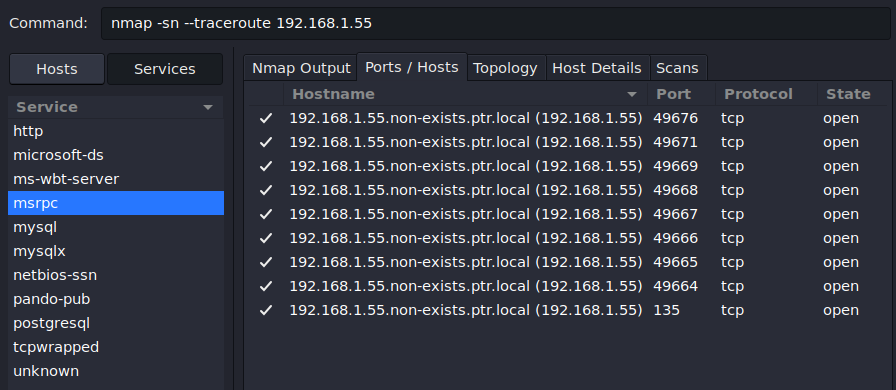
1. Press Services button & explain



Services

In Zenmap, "Services" refers to the applications or processes running on a host that are accessible over the network. It displays a list of open ports on the target host and the services associated with those ports. This information is crucial for understanding the host's functionality, potential vulnerabilities, and for making informed decisions about network security and administration.

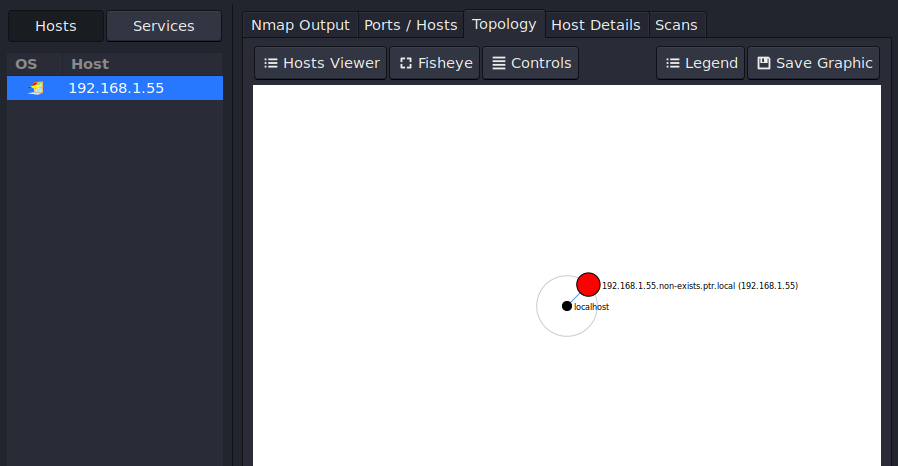
1. Press Ports / Hosts button & explain



Ports / Hosts

In Zenmap, the "Ports/Hosts" tab displays a list of open ports on the target host (identified by its IP address or hostname) and the associated services running on those ports. This information is essential for understanding the host's functionality, potential vulnerabilities, and for making informed decisions about network security and administration.

1. Press Topology button & explain

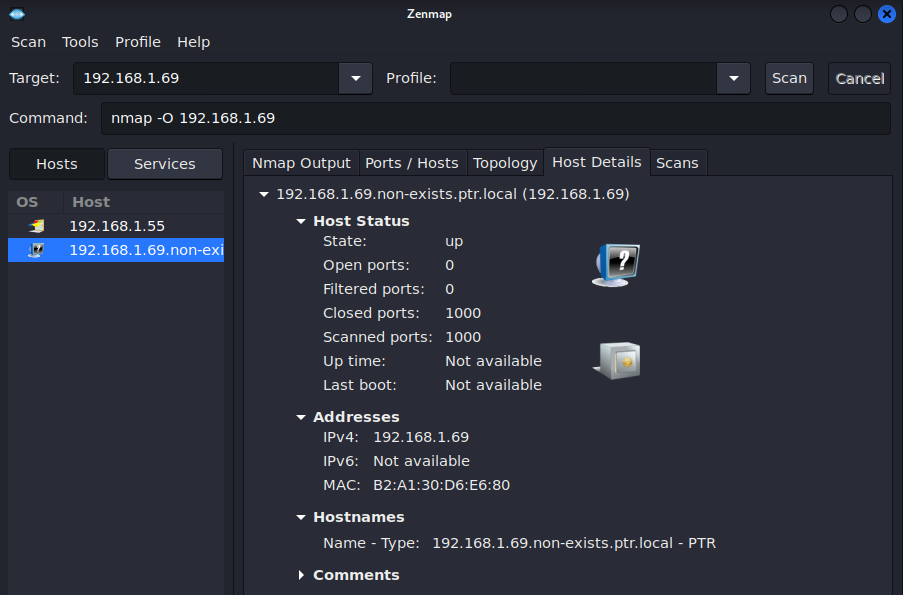


Topology

In Zenmap, the "Topology" tab provides a graphical representation of the network, showing the interconnected devices and their relationships. This visual representation helps you understand the network layout, identify potential bottlenecks, and visualize the flow of traffic. It's particularly useful for larger networks where it might be difficult to grasp the overall structure from a list of devices and connections.

1. Press Host details button & explain

In this exercise, I will scan my phone instead (192.168.1.69), as my PC has security rules preventing detailed scans.



Host details

In Zenmap, the "Host Details" tab provides a comprehensive view of information about a specific host, including its IP address, hostname, operating system (if detected), and other details discovered during the scan. This includes open ports, associated services, and potentially vulnerabilities found. It's a valuable tool for understanding the security posture of a host and identifying potential risks

<https://linuxhint.com/zenmap_ubuntu_nmap/>