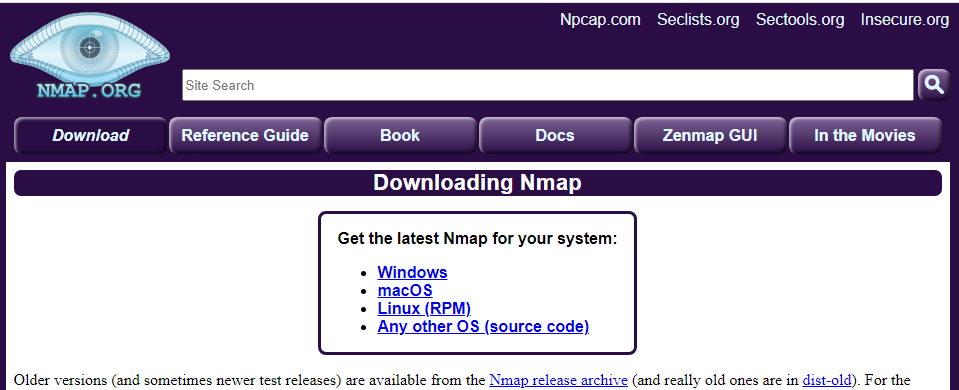
**LAB11 Window Nmap**

Name: Truong Dang Truc Lam Students: ID B2111933 Class: CT201HM01-M04

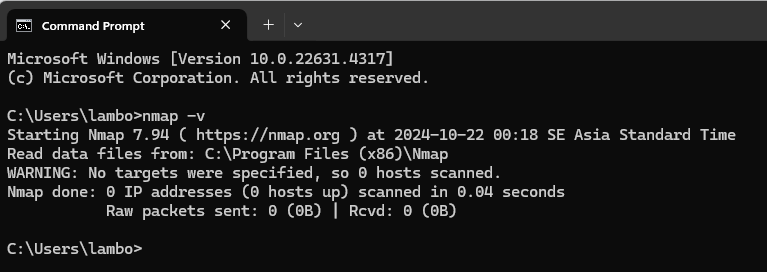
**Its illegal to scan outside network**

1. Install Windows Nmap

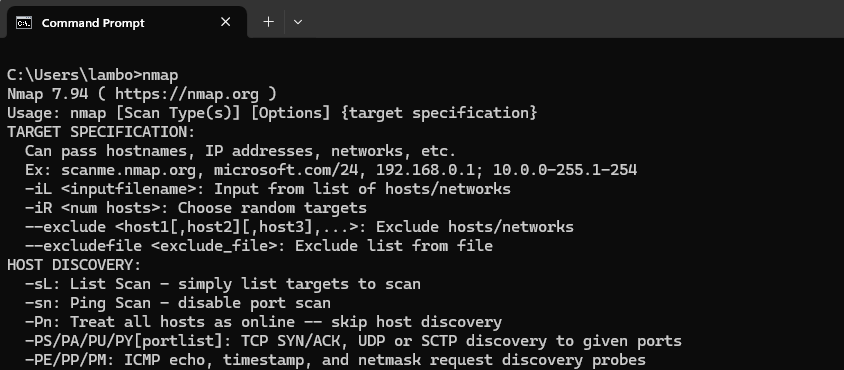


We can download from: <https://nmap.org/download.html>.

1. Confirm Windows Nmap installation



Confirm Windows Nmap installation

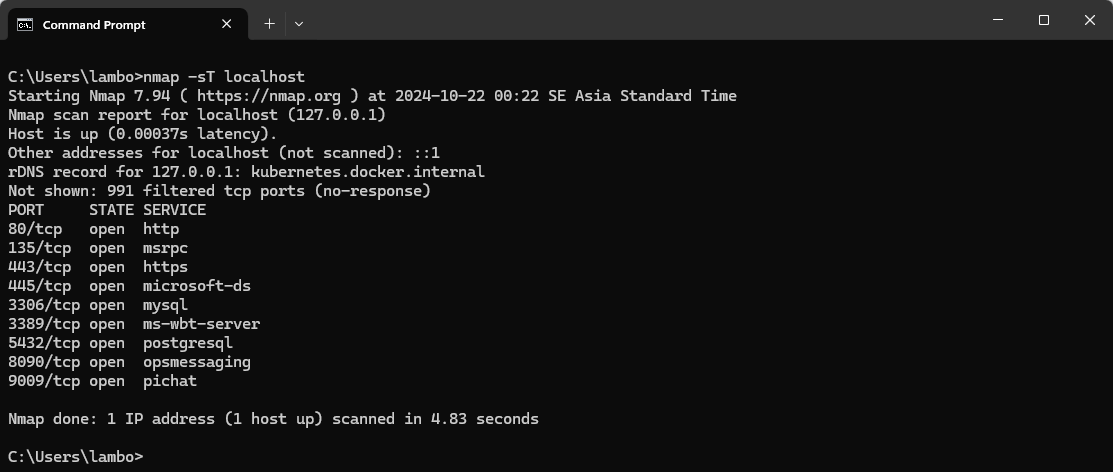


CMD nmap-h

1. Design [**Nmap**](https://nmap.en.lo4d.com/windows)scanning pen-test

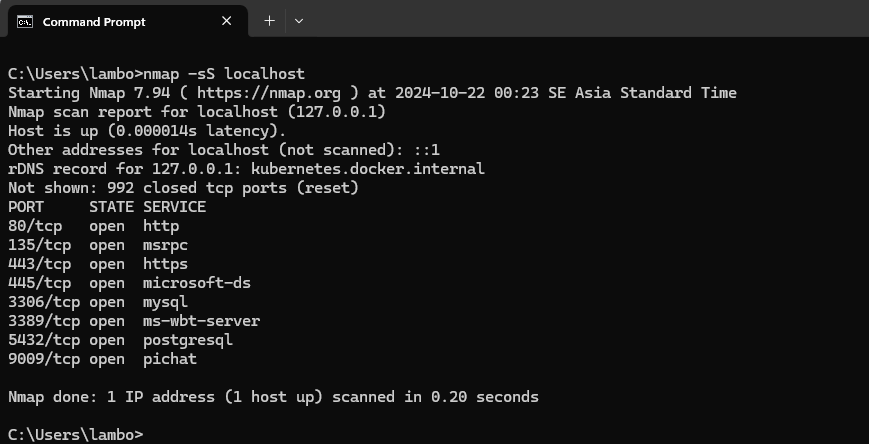
|  | scanner | target |
| --- | --- | --- |
| OS | Windows | Windows, Linux |
| IP address | Test - bed host IP | * Localhost * CICT IP * Neighboring PC IP * VM IP(Ubuntu, Centos) |
| scanning program | Windows [**Nmap**](https://nmap.en.lo4d.com/windows) |
| scanning types | -sT: -sS: -sP:  -sU: -sF -P-PB  -O -PS |

1. Execute Windows Nmap based on slide (screenshot and explain the scanning result)
2. nmap –sT CTU or localhost



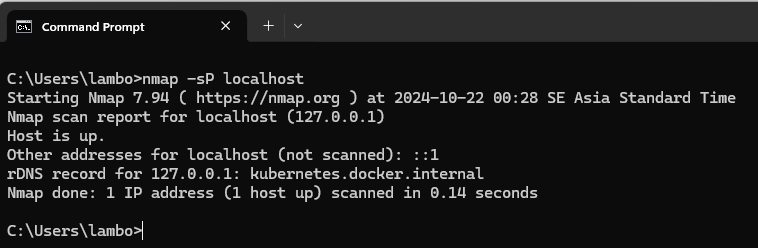
The nmap -sT command performs a TCP SYN scan, which sends a SYN packet to each port on a target host to determine if the port is open and listening. This scan is often used for initial reconnaissance to identify active hosts and open services on a network.

1. nmap –sS CTU or localhost



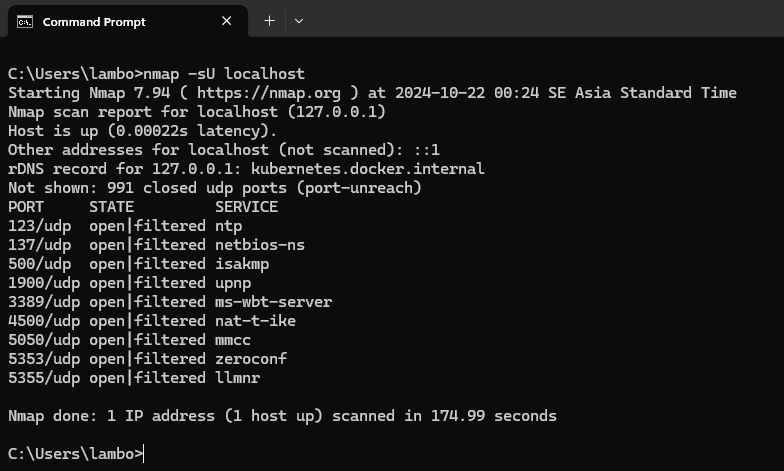
The nmap -sS command performs a TCP SYN Stealth scan, which sends a SYN packet to each port on a target host but doesn't wait for a response before sending the next packet. This scan is less likely to be detected by intrusion detection systems (IDS) compared to a regular SYN scan.

1. nmap – sP CTU or localhost



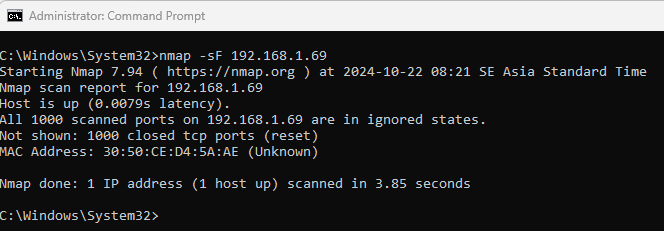
The nmap -sP command is a basic and useful command in Nmap, used for network discovery. This command will send ICMP Echo Request (ping) packets to all IP addresses in a specified network range, to determine which hosts are active and responding.

1. nmap -sU CICT or localhost



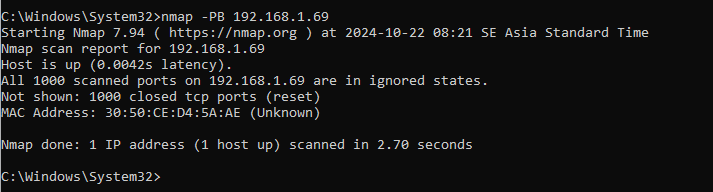
The nmap -sU command is used to scan UDP ports on a host or network. UDP (User Datagram Protocol) is a network protocol that does not guarantee packet delivery, unlike TCP.

1. nmap -sF VM IP



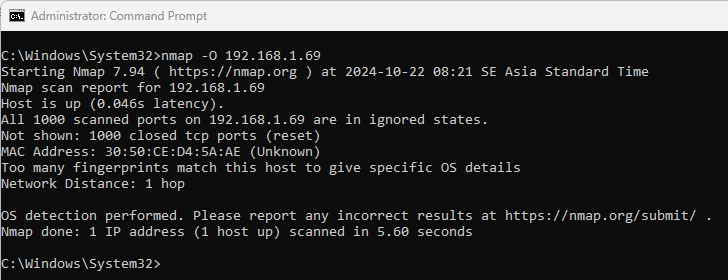
The nmap -sF command performs a fast scan using Nmap, a network scanning tool. It sends a single TCP packet to each port on the target host, attempting to determine if the port is open or closed. This is a quick and efficient way to get a basic overview of the open ports on a system.

1. nmap -PB VM IP



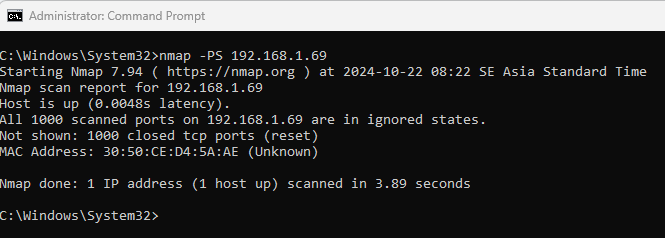
The nmap -PB command performs a ping scan and a basic port scan on one or more hosts. It first sends a ping to the target host to determine if it is online, and then scans a predefined set of common ports (known as "basic ports"). This is a quick and efficient way to get a basic overview of the status of a host and the services running on it.

1. nmap -O VM IP IP



The nmap -O command attempts to identify the operating system and version of a target host by analyzing the responses to various probes sent during the scan. This technique, known as operating system fingerprinting, leverages known characteristics of different operating systems to make educated guesses about the system in use.

1. nmap -PS VM IP



The nmap -PS command performs a SYN ping scan using Nmap. It sends a single TCP SYN packet to each port on the target host, attempting to determine if the port is open or closed based on the response received. This scan is often used to quickly identify live hosts on a network and gather basic information about open services.

<https://nmap.org/download.html>

<http://www.insecure.org/nmap/>