LAB03 Zenmap

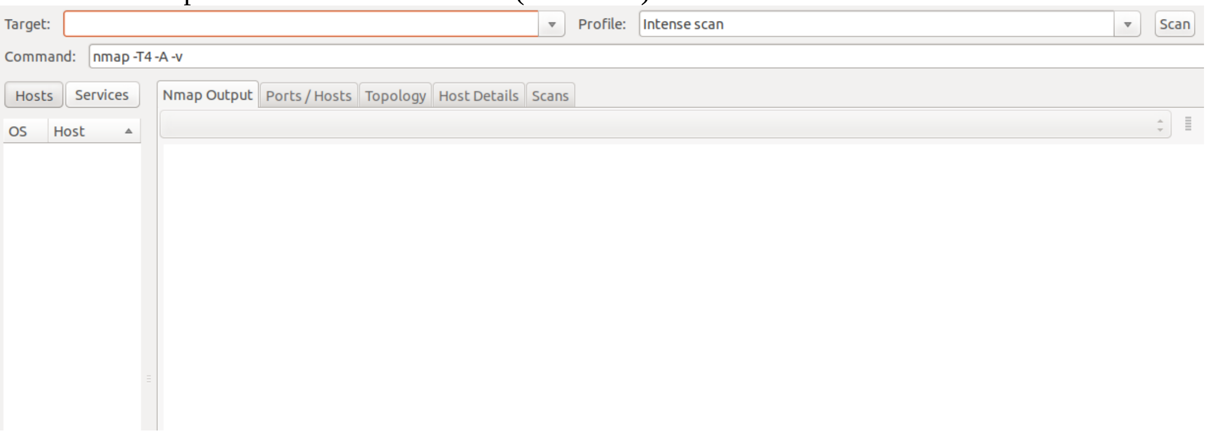
Class	CT201H
Student ID	B2014926
Name	Tran Dang Khoa
Email address	B2014926
Class	
Browser	Safari, Chrome, IE, Firefox

1. Design Zenmap scanning pen-test scenario under Windows

	scanner	target
OS	Windows Ubuntu	Windows, Linux
IP address	Test - bed host IP	Localhost CTU IP CICT IP Neighboring PC IP VM IP(Ubuntu, Centos)
scanning program	Zenmap Windows Zenmap Ubuntu	
scanning types	scan in profile field scan in command field scan in menu bar	

If you find error message, capture it on LAB report and explain

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



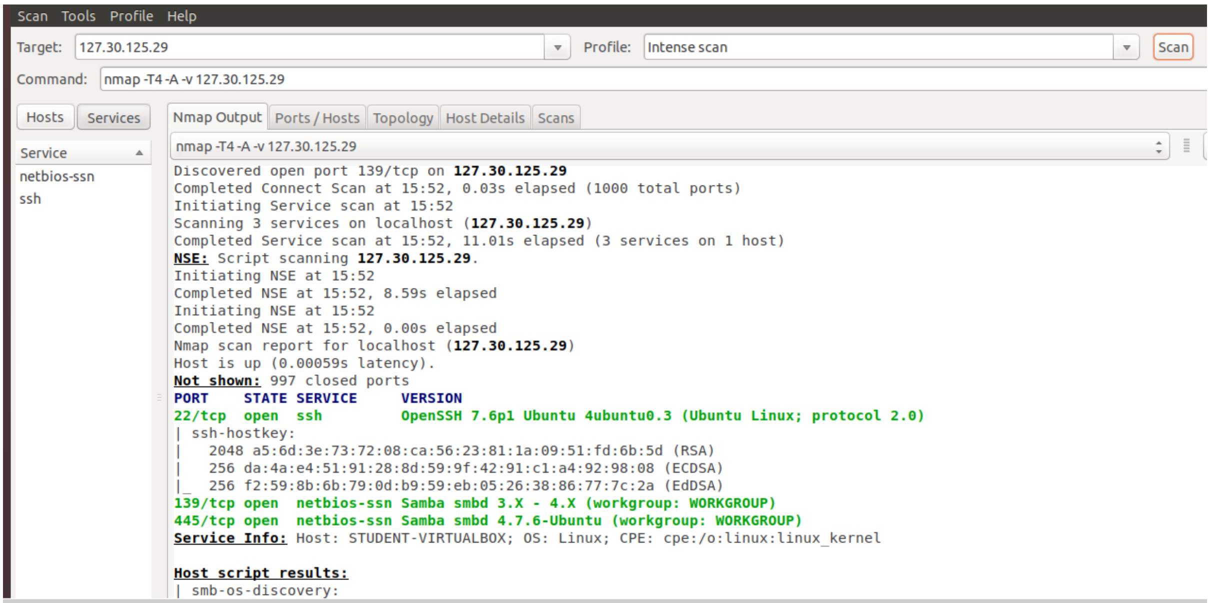
Target:

Profile: Intense scan

Command: nmap -T4 -A -v

3. scan in profile field and explain the scan command

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



Target: 127.30.125.29

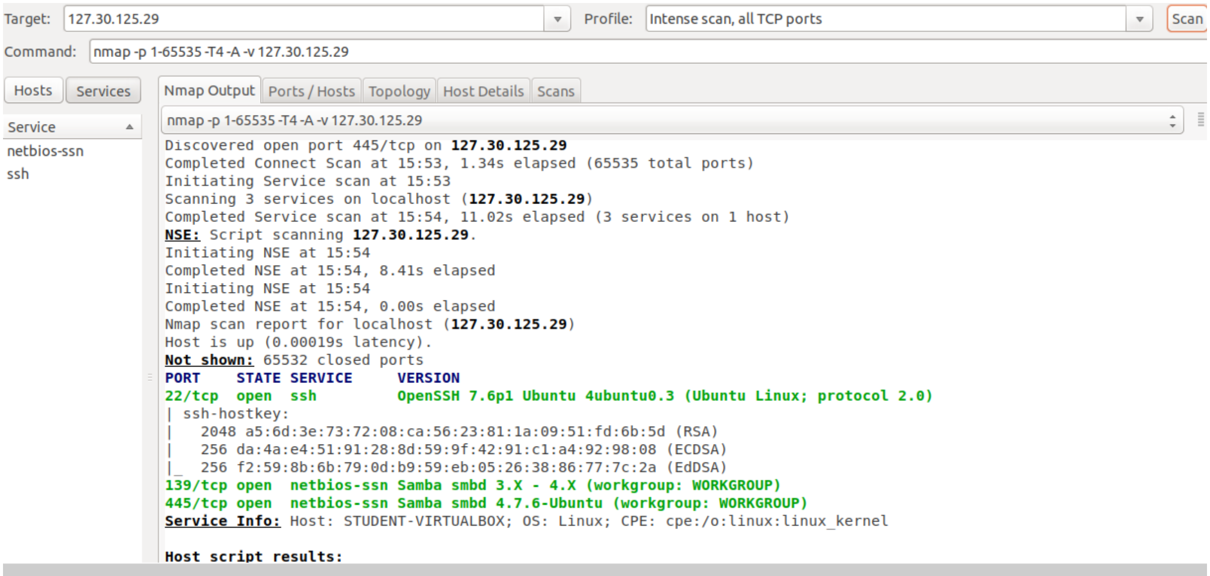
Profile: Intense scan

Command: nmap -T4 -A -v 127.30.125.29

Service: netbios-ssn, ssh

```
nmap -T4 -A -v 127.30.125.29
Discovered open port 139/tcp on 127.30.125.29
Completed Connect Scan at 15:52, 0.03s elapsed (1000 total ports)
Initiating Service scan at 15:52
Scanning 3 services on localhost (127.30.125.29)
Completed Service scan at 15:52, 11.01s elapsed (3 services on 1 host)
NSE: Script scanning 127.30.125.29.
Initiating NSE at 15:52
Completed NSE at 15:52, 8.59s elapsed
Initiating NSE at 15:52
Completed NSE at 15:52, 0.00s elapsed
Nmap scan report for localhost (127.30.125.29)
Host is up (0.00059s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a5:6d:3e:73:72:08:ca:56:23:81:1a:09:51:fd:6b:5d (RSA)
|   256 da:4a:e4:51:91:28:8d:59:9f:42:91:c1:a4:92:98:08 (ECDSA)
|_  256 f2:59:8b:6b:79:0d:b9:59:eb:05:26:38:86:77:7c:2a (EdDSA)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: STUDENT-VIRTUALBOX; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
```

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



Target: 127.30.125.29

Profile: Intense scan, all TCP ports

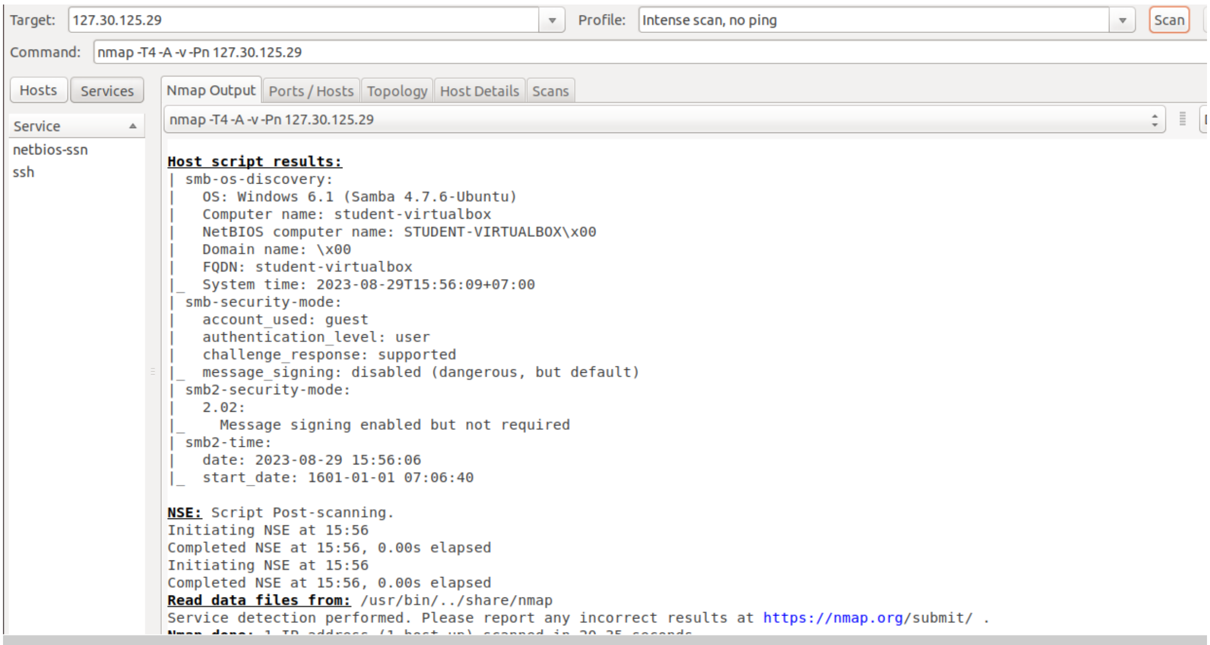
Command: nmap -p 1-65535 -T4 -A -v 127.30.125.29

Service: netbios-ssn, ssh

```
nmap -p 1-65535 -T4 -A -v 127.30.125.29
Discovered open port 445/tcp on 127.30.125.29
Completed Connect Scan at 15:53, 1.34s elapsed (65535 total ports)
Initiating Service scan at 15:53
Scanning 3 services on localhost (127.30.125.29)
Completed Service scan at 15:54, 11.02s elapsed (3 services on 1 host)
NSE: Script scanning 127.30.125.29.
Initiating NSE at 15:54
Completed NSE at 15:54, 8.41s elapsed
Initiating NSE at 15:54
Completed NSE at 15:54, 0.00s elapsed
Nmap scan report for localhost (127.30.125.29)
Host is up (0.00019s latency).
Not shown: 65532 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a5:6d:3e:73:72:08:ca:56:23:81:1a:09:51:fd:6b:5d (RSA)
|   256 da:4a:e4:51:91:28:8d:59:9f:42:91:c1:a4:92:98:08 (ECDSA)
|_  256 f2:59:8b:6b:79:0d:b9:59:eb:05:26:38:86:77:7c:2a (EdDSA)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: STUDENT-VIRTUALBOX; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
```

⇨Nmap -p 1-65535 -T4 -A -v is an Namp command that performs an extensive and aggressive scan of all possible ports on the target systems, while also attempting to identify the operating system and service versions. The use of '-v' provides detailed output, and '- T4' sets the timing template for the scan to be faster but less stealthy. This command is useful when you want to thoroughly inspect a target system's services and are willing to accpect the increased scan time and potentially less stealthy approach.

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



Target: 127.30.125.29 Profile: Intense scan, no ping

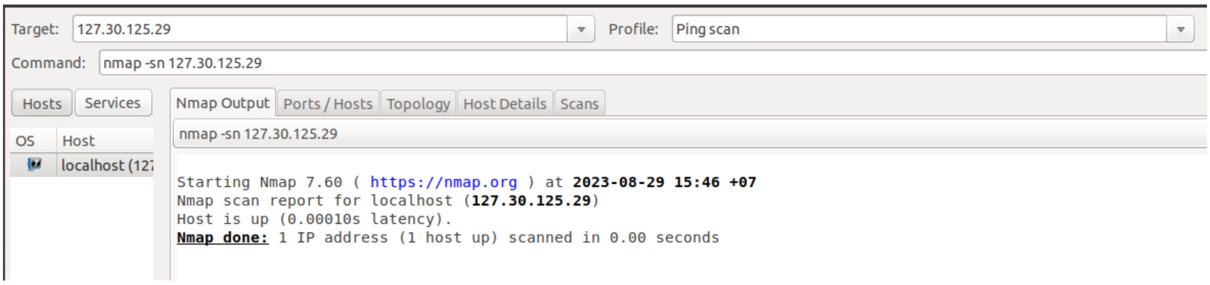
Command: nmap -T4 -A -v -Pn 127.30.125.29

```
Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: student-virtualbox
|   NetBIOS computer name: STUDENT-VIRTUALBOX\x00
|   Domain name: \x00
|   FQDN: student-virtualbox
|_  System time: 2023-08-29T15:56:09+07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-08-29 15:56:06
|_  start_date: 1601-01-01 07:06:40

NSE: Script Post-scanning.
Initiating NSE at 15:56
Completed NSE at 15:56, 0.00s elapsed
Initiating NSE at 15:56
Completed NSE at 15:56, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.25 seconds
```

⇨namp -T4 -A -v -Pn' is an namp command that performs an aggressive and thorough scan of a target host or network. It attempts to identify the operating system and service version, provides detailed output, and skips the host discovery phase to save time when you are sure about the target's online status. This command is useful for in-depth network reconnaissance when speed is a priority and stealthiness is not a major concern.

4. Scan in command field and explain the scan command

4 Ping Scan Command: nmap -sn <target>



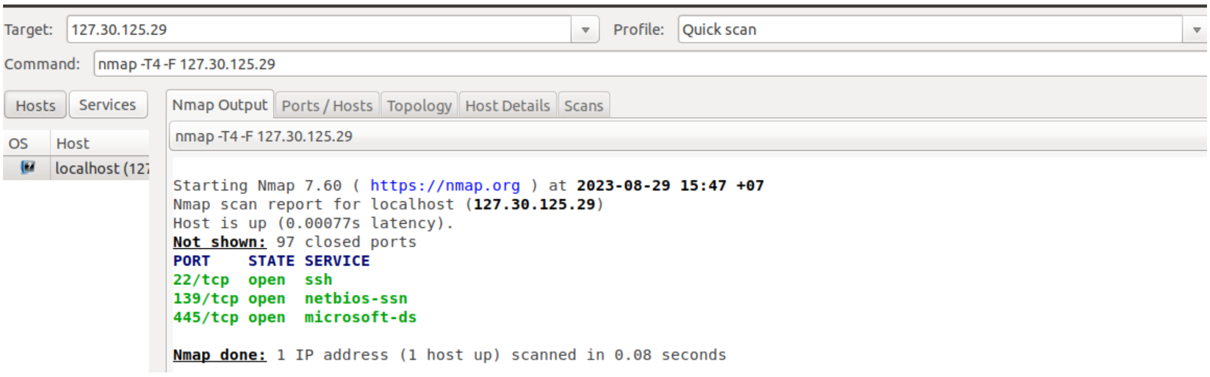
Target: 127.30.125.29 Profile: Ping scan

Command: nmap -sn 127.30.125.29

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-29 15:46 +07
Nmap scan report for localhost (127.30.125.29)
Host is up (0.00010s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
```

⇨It simply sends ping requests to the target host to check if the target host is alive or not. As the example below, I use a ping scan to check if the target host is alive or not and, as the result, it seems alive.

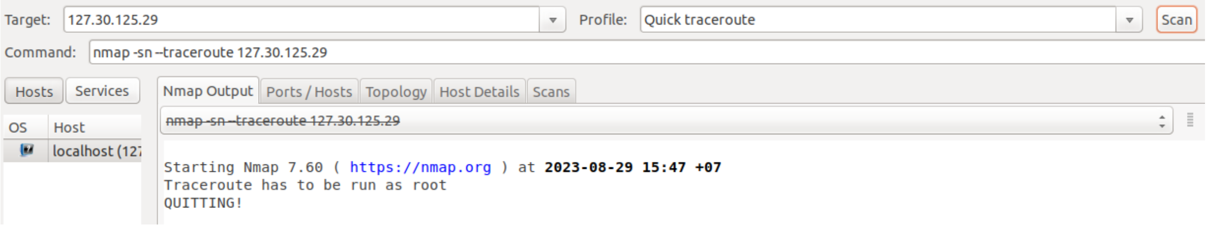
5 Quick Scan Command: nmap -T4 -F <target>



```
nmap -T4 -F 127.30.125.29

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-29 15:47 +07
Nmap scan report for localhost (127.30.125.29)
Host is up (0.00077s latency).
Not shown: 97 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

⇨ Quick scan simply scan faster than the intense scan and limit the number of ports scanned to only 100 most common TCP ports.

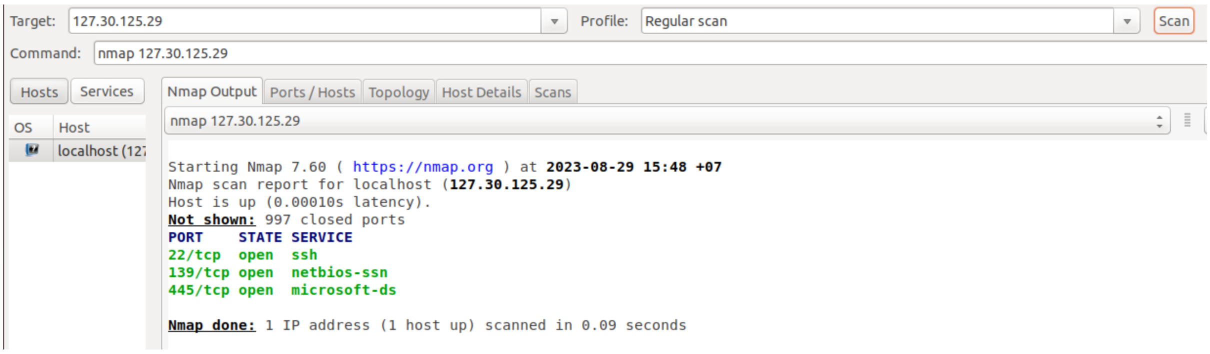
6 Quick Trace Route Command: nmap -sn --traceroute <target>



```
~~nmap -sn --traceroute 127.30.125.29~~

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-29 15:47 +07
Traceroute has to be run as root
QUITTING!
```

⇨ This scan means traceroute and ping all hosts defined in the target. 7 Regular
Scan Command: nmap *<127.30.125.29>*

7 Regular Scan Command: nmap <target>

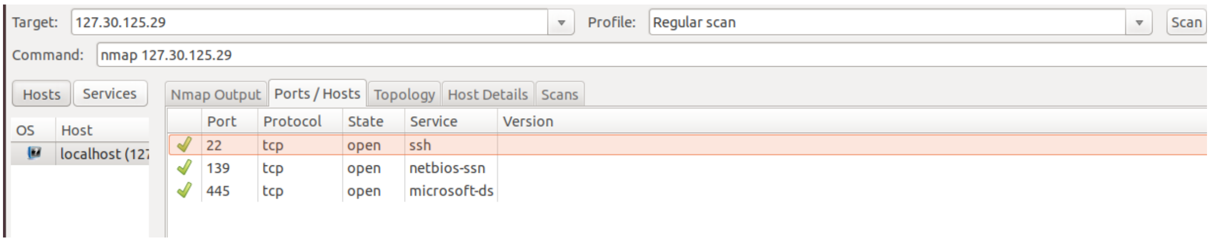


```
nmap 127.30.125.29

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-29 15:48 +07
Nmap scan report for localhost (127.30.125.29)
Host is up (0.00010s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

⇨ The regular scan is the default scanning, TCP scanning, it simply scans and shows open services or ports on the target host, usually scans the 1000 most common ports. The scan below scanned 998 filtered ports and only two are open.

5. Scan **in menu bar and** explain scan command

8 Press <u>Hosts</u> button & explain



Target: 127.30.125.29 Profile: Regular scan

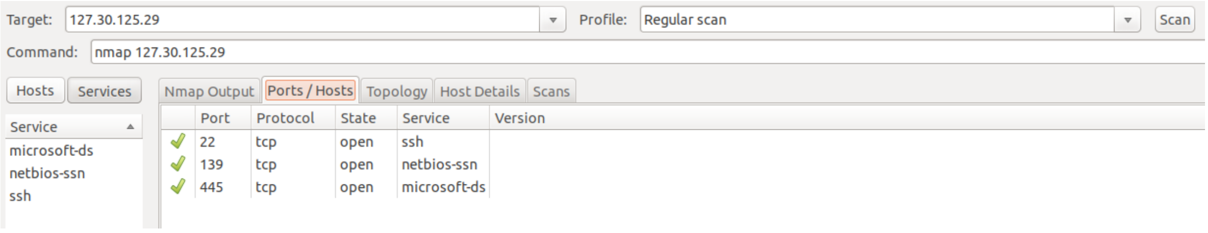
Command: nmap 127.30.125.29

OS	Host
	localhost (127

	Port	Protocol	State	Service	Version
✓	22	tcp	open	ssh	
✓	139	tcp	open	netbios-ssn	
✓	445	tcp	open	microsoft-ds	

⇨ It simply displays all hosts that were scanned. Each host is labeled with its hostname or domain name, IP address and has an icon indicating the OS that was detected for that host. The figure below shows only no specific OS or OS detection not performed on that hosts.

9 Press Services button & explain



Target: 127.30.125.29 Profile: Regular scan

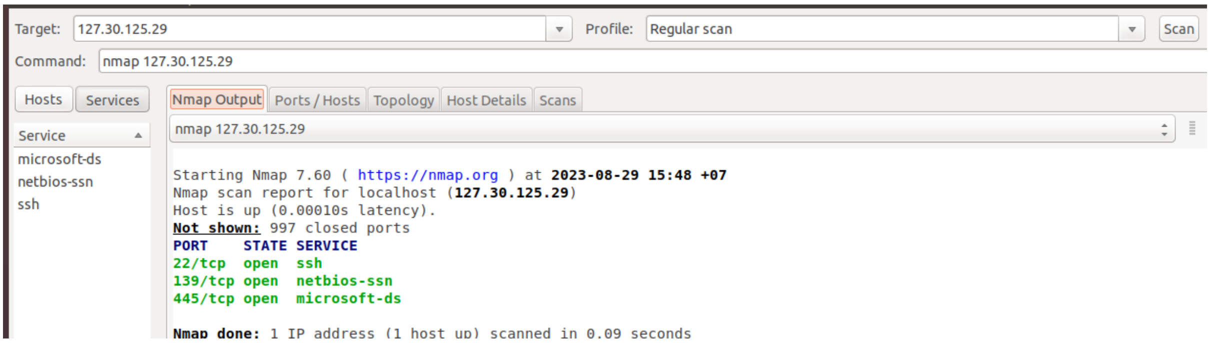
Command: nmap 127.30.125.29

Service
microsoft-ds
netbios-ssn
ssh

	Port	Protocol	State	Service	Version
✓	22	tcp	open	ssh	
✓	139	tcp	open	netbios-ssn	
✓	445	tcp	open	microsoft-ds	

⇨ It displays all services that were scanned and which ports or hosts use that service. 10 Press Nanmap output button & explain

10 Press Nanmap output button & explain



Target: 127.30.125.29 Profile: Regular scan

Command: nmap 127.30.125.29

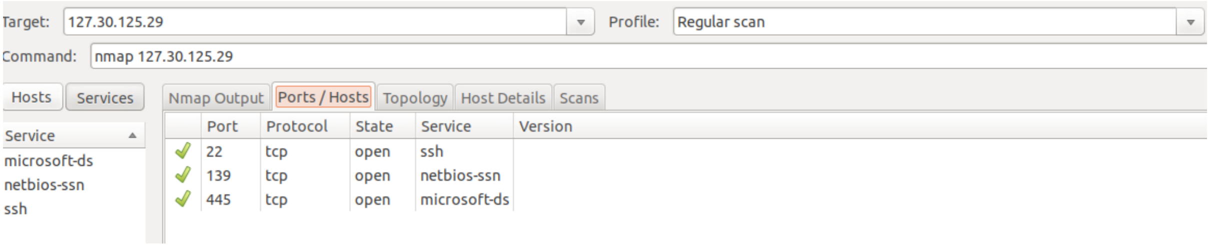
Service
microsoft-ds
netbios-ssn
ssh

nmap 127.30.125.29

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-29 15:48 +07
Nmap scan report for localhost (127.30.125.29)
Host is up (0.00010s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

⇨ It simply shows the results scan of nmap commands.

11 Press Ports / Hosts button & explain



Target: 127.30.125.29 Profile: Regular scan

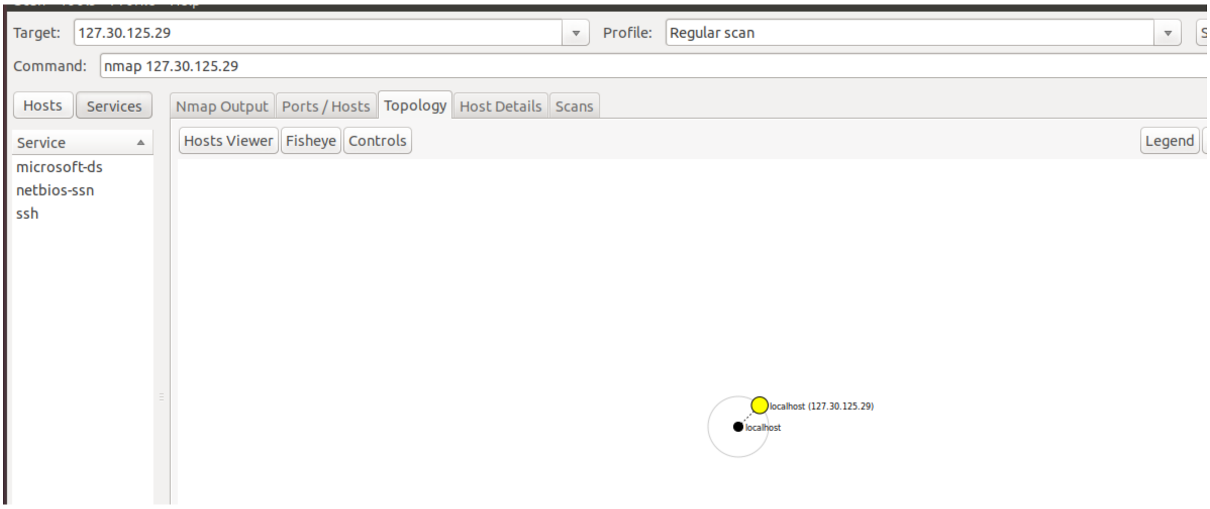
Command: nmap 127.30.125.29

Service
microsoft-ds
netbios-ssn
ssh

	Port	Protocol	State	Service	Version
✓	22	tcp	open	ssh	
✓	139	tcp	open	netbios-ssn	
✓	445	tcp	open	microsoft-ds	

⇨ The “Ports / Hosts” tab's display differs depending on whether a host or a service is currently selected. When a host is selected, it shows all the interesting ports on that host, along with version information when available. When a service is selected, the “Ports / Hosts” tab shows all the hosts which have that port open or filtered.

12 Press Topology button & explain



Target: 127.30.125.29

Profile: Regular scan

Command: nmap 127.30.125.29

Service

microsoft-ds

netbios-ssn

ssh

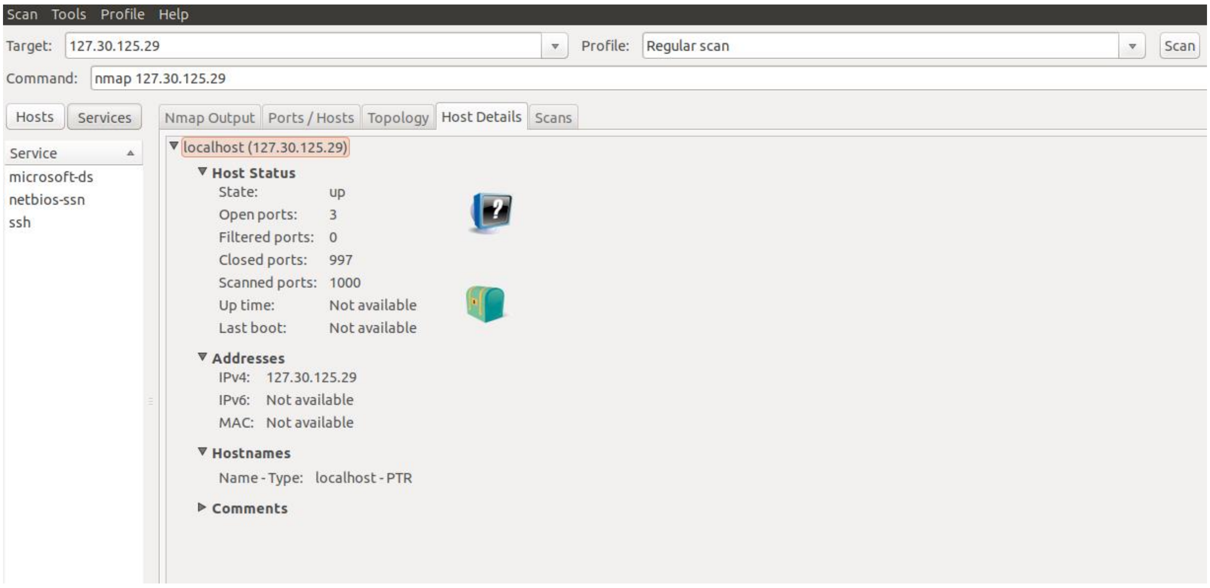
⇨ The “Topology” tab shows the connections between hosts in a network. It is a visual view of the traceroute. From the figure below, I can see, the black circle is my local host.

⇨ It has some green circle (because that has fewer than 3 open ports) clustered around localhost and has connected with a dashed black line (seems that with no traceroute information).

⇨ In the figure, I also see a white circle on the effort to connect to the ctu.edu.vn domain, the white circle represents it is an intermediate host in the network path that was not port scanned.

⇨ The bigger circle show that has a more open port on the host, the thickness of the blue line in the figure below shows it is a primary traceroute. As we can see in the figure below, they have two yellow squares, which means that hosts with some ports are filtered.

13 Press Host details button & explain



```
Target: 127.30.125.29        Profile: Regular scan
Command: nmap 127.30.125.29

Service
microsoft-ds
netbios-ssn
ssh

▼ localhost (127.30.125.29)
  ▼ Host Status
     State:          up
     Open ports:     3
     Filtered ports: 0
     Closed ports:   997
     Scanned ports:  1000
     Up time:        Not available
     Last boot:      Not available
  ▼ Addresses
     IPv4:  127.30.125.29
     IPv6:  Not available
     MAC:   Not available
  ▼ Hostnames
     Name - Type:  localhost - PTR
  ▶ Comments
```

- The “Host Details” tab shows pieces of information of host about Host status, Address.
- Hostnames, Operating System, OS class, Ports used by Host.
- Each host has an icon that provides a very rough “vulnerability” estimate, which is based solely on the number of open ports. From the figure below, I can see that host has 1 open port so the host has the icon below (the icon below will be shown if has 0-2 open ports).

https://linuxhint.com/zenmap_ubuntu_nmap/