Design of Secure Computer Systems

Lab 06

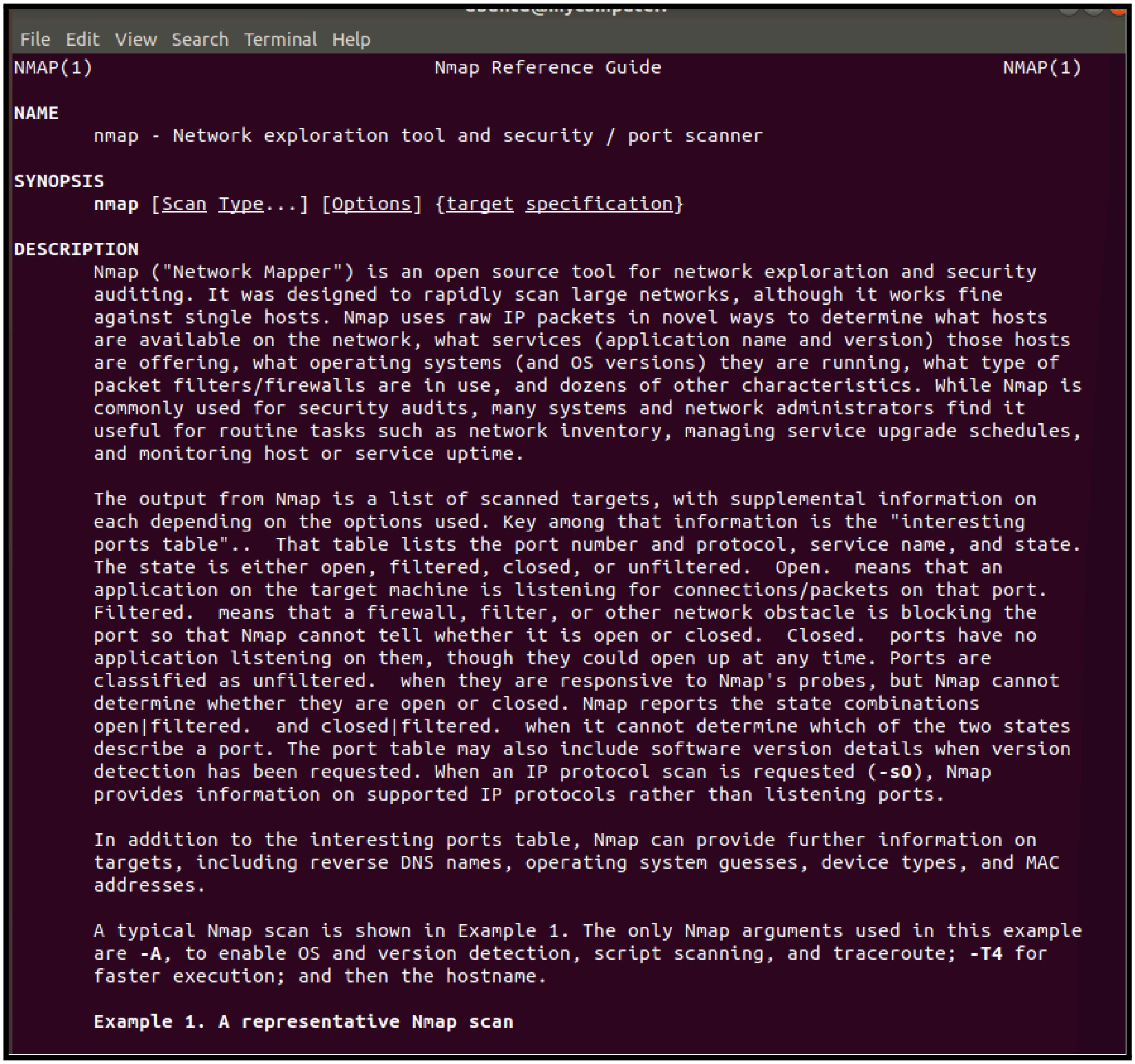
NMAPDISCOVERY

This Lab will explore the use of the Nmap utility to discover computers and services on networks.

Name: Rakshita Mathur

Nmap-discovery

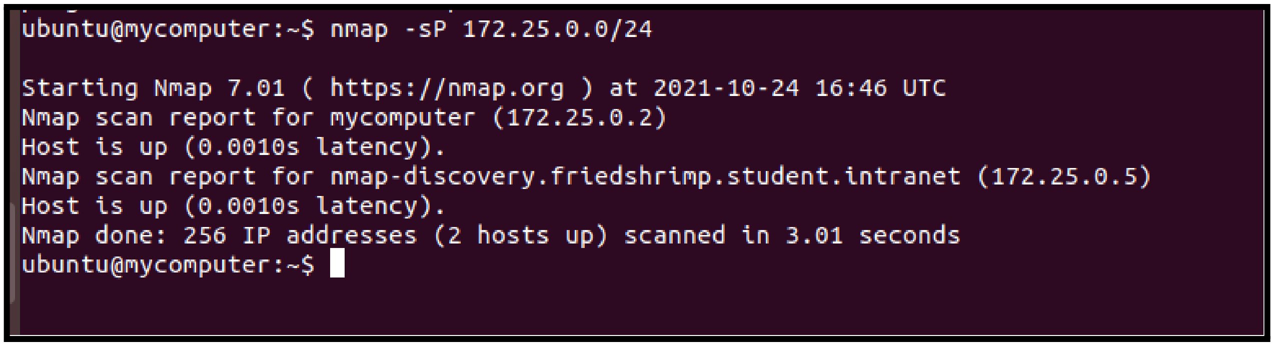
The first command used: **man nmap** to see the manual of nmap



```
NMAP(1)                          Nmap Reference Guide                          NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
       Nmap ("Network Mapper") is an open source tool for network exploration and security
       auditing. It was designed to rapidly scan large networks, although it works fine
       against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts
       are available on the network, what services (application name and version) those hosts
       are offering, what operating systems (and OS versions) they are running, what type of
       packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is
       commonly used for security audits, many systems and network administrators find it
       useful for routine tasks such as network inventory, managing service upgrade schedules,
       and monitoring host or service uptime.

       The output from Nmap is a list of scanned targets, with supplemental information on
       each depending on the options used. Key among that information is the "interesting
       ports table"..  That table lists the port number and protocol, service name, and state.
       The state is either open, filtered, closed, or unfiltered.  Open.  means that an
       application on the target machine is listening for connections/packets on that port.
       Filtered.  means that a firewall, filter, or other network obstacle is blocking the
       port so that Nmap cannot tell whether it is open or closed.  Closed.  ports have no
       application listening on them, though they could open up at any time. Ports are
       classified as unfiltered.  when they are responsive to Nmap's probes, but Nmap cannot
       determine whether they are open or closed. Nmap reports the state combinations
       open|filtered.  and closed|filtered.  when it cannot determine which of the two states
       describe a port. The port table may also include software version details when version
       detection has been requested. When an IP protocol scan is requested (-sO), Nmap
       provides information on supported IP protocols rather than listening ports.

       In addition to the interesting ports table, Nmap can provide further information on
       targets, including reverse DNS names, operating system guesses, device types, and MAC
       addresses.

       A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this example
       are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for
       faster execution; and then the hostname.

       Example 1. A representative Nmap scan
```

We can see all the commands here.

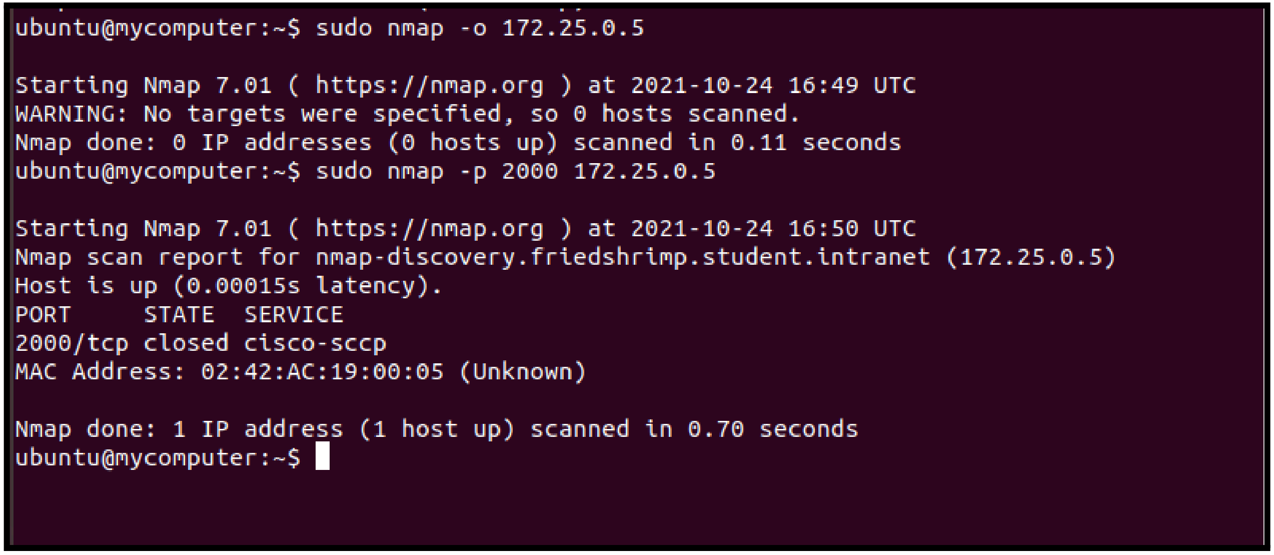
For finding the IP address we use the command **nmap -sP 172.24.0.0/24**



```
ubuntu@mycomputer:~$ nmap -sP 172.25.0.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2021-10-24 16:46 UTC
Nmap scan report for mycomputer (172.25.0.2)
Host is up (0.0010s latency).
Nmap scan report for nmap-discovery.friedshrimp.student.intranet (172.25.0.5)
Host is up (0.0010s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.01 seconds
ubuntu@mycomputer:~$ 
```

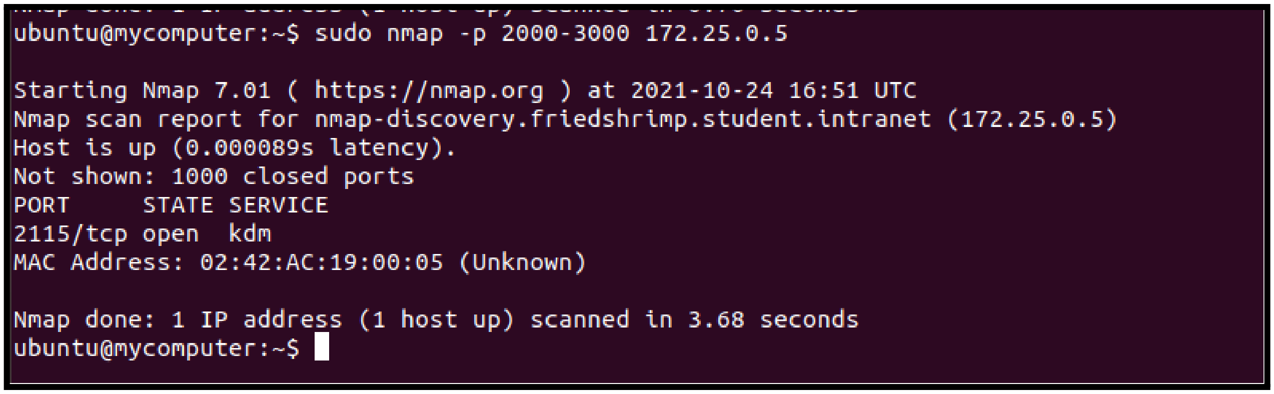
And found the IP address to be 172.25.0.2

Now we run the port from 2000



```
ubuntu@mycomputer:~$ sudo nmap -o 172.25.0.5

Starting Nmap 7.01 ( https://nmap.org ) at 2021-10-24 16:49 UTC
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.11 seconds
ubuntu@mycomputer:~$ sudo nmap -p 2000 172.25.0.5

Starting Nmap 7.01 ( https://nmap.org ) at 2021-10-24 16:50 UTC
Nmap scan report for nmap-discovery.friedshrimp.student.intranet (172.25.0.5)
Host is up (0.00015s latency).
PORT     STATE  SERVICE
2000/tcp closed cisco-sccp
MAC Address: 02:42:AC:19:00:05 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
ubuntu@mycomputer:~$ 
```

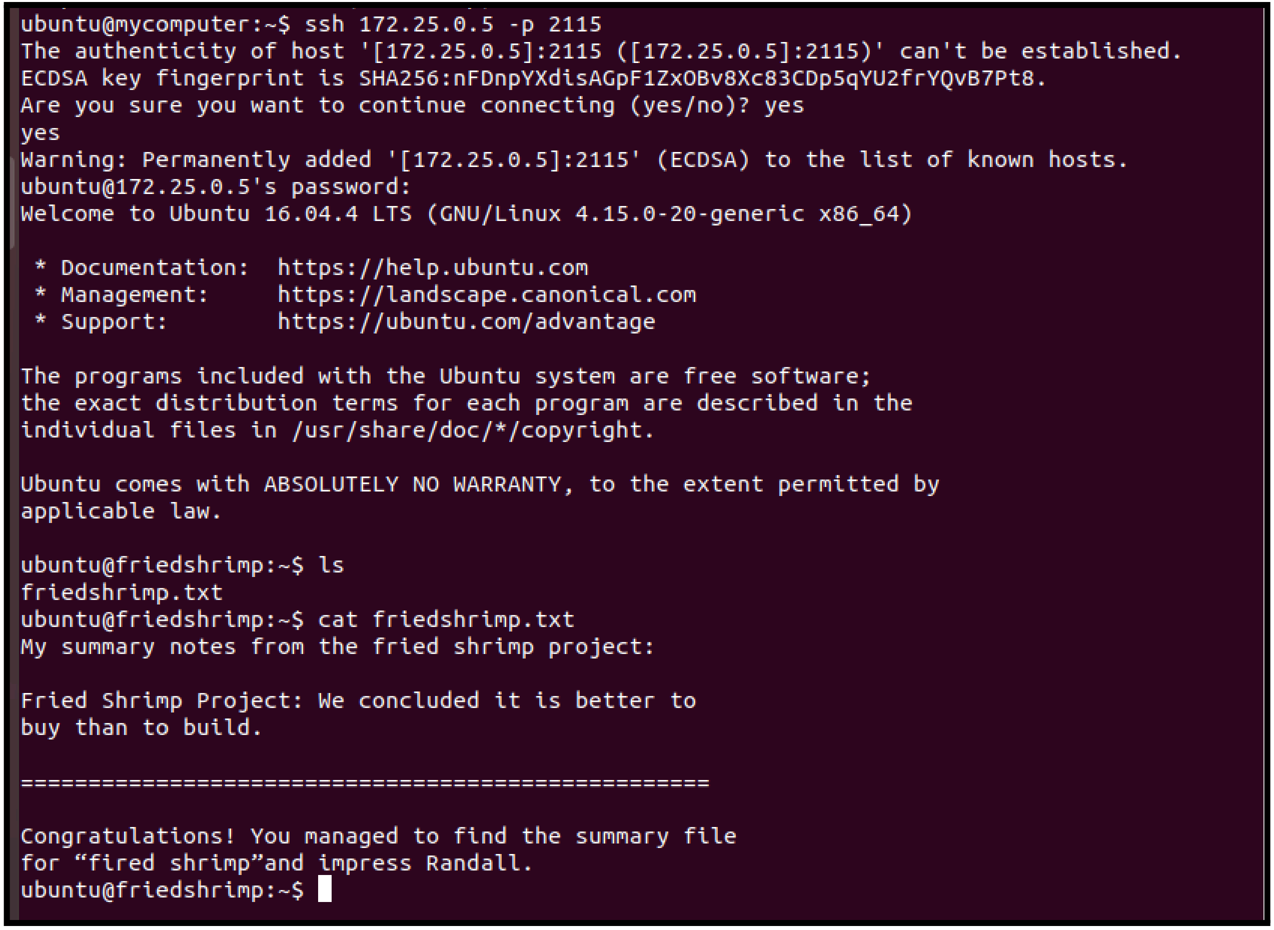
And when we want to run every port from 2000-3000 we use the command **sudo nmap -o 2000-3000 172.25.0.5**



```
ubuntu@mycomputer:~$ sudo nmap -p 2000-3000 172.25.0.5

Starting Nmap 7.01 ( https://nmap.org ) at 2021-10-24 16:51 UTC
Nmap scan report for nmap-discovery.friedshrimp.student.intranet (172.25.0.5)
Host is up (0.000089s latency).
Not shown: 1000 closed ports
PORT     STATE SERVICE
2115/tcp open  kdm
MAC Address: 02:42:AC:19:00:05 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.68 seconds
ubuntu@mycomputer:~$ 
```

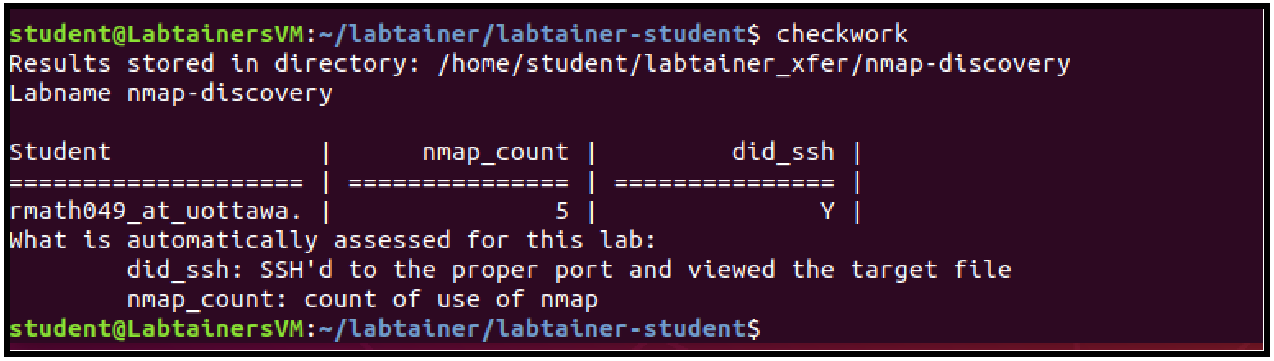
We found that there are 1000 closed ports and only one open port which is 2115, so we consider it to be the desired port for ssh

Now we ssh using port 2115. And ls the file. Then we view the content of the file using cat command.



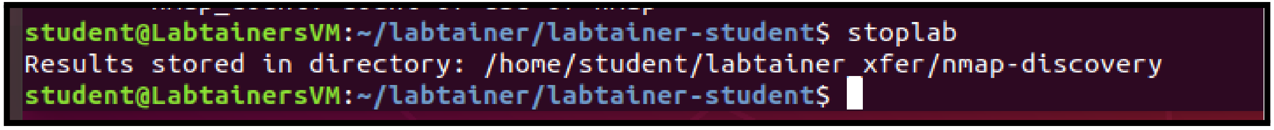
```
ubuntu@mycomputer:~$ ssh 172.25.0.5 -p 2115
The authenticity of host '[172.25.0.5]:2115 ([172.25.0.5]:2115)' can't be established.
ECDSA key fingerprint is SHA256:nFDnpYXdisAGpF1ZxOBv8Xc83CDp5qYU2frYQvB7Pt8.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '[172.25.0.5]:2115' (ECDSA) to the list of known hosts.
ubuntu@172.25.0.5's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ubuntu@friedshrimp:~$ ls
friedshrimp.txt
ubuntu@friedshrimp:~$ cat friedshrimp.txt
My summary notes from the fried shrimp project:

Fried Shrimp Project: We concluded it is better to
buy than to build.

===================================================

Congratulations! You managed to find the summary file
for “fired shrimp”and impress Randall.
ubuntu@friedshrimp:~$
```

Then we check the lab using checkwork command



```
student@LabtainersVM:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/nmap-discovery
Labname nmap-discovery

Student              |      nmap_count |         did_ssh |
==================== | =============== | =============== |
rmath049_at_uottawa. |               5 |               Y |
What is automatically assessed for this lab:
        did_ssh: SSH'd to the proper port and viewed the target file
        nmap_count: count of use of nmap
student@LabtainersVM:~/labtainer/labtainer-student$
```

And stop the lab using the stop lab command



```
student@LabtainersVM:~/labtainer/labtainer-student$ stoplab
Results stored in directory: /home/student/labtainer_xfer/nmap-discovery
student@LabtainersVM:~/labtainer/labtainer-student$
```