

Using nmap for network discovery

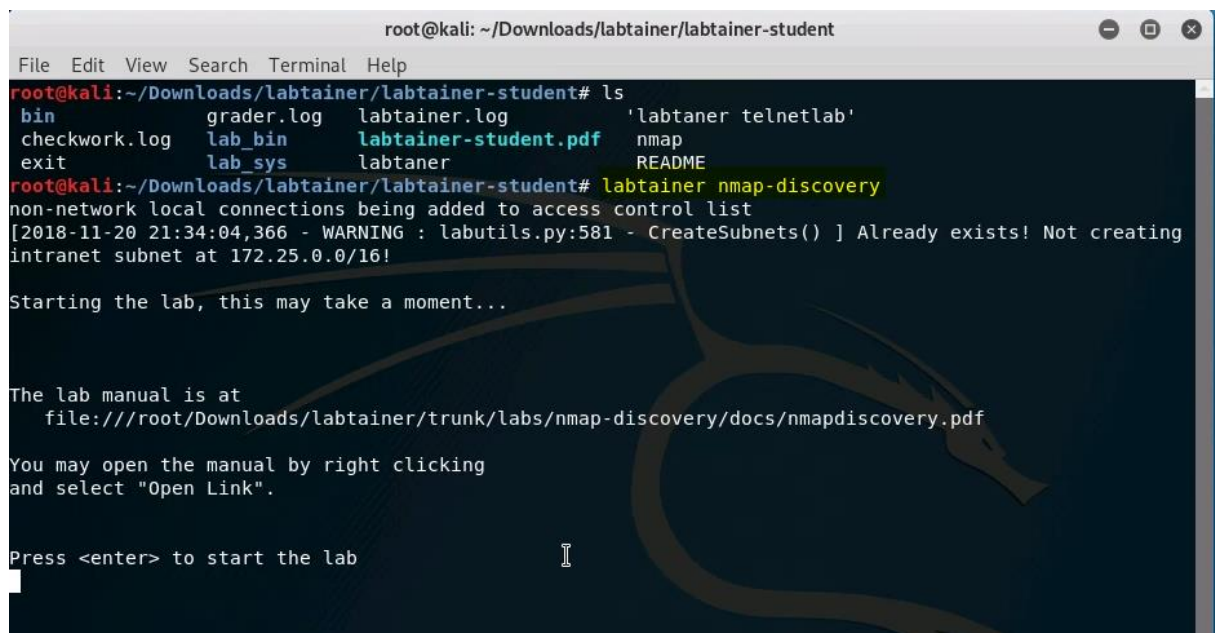
Overview

This Labtainer exercise explores the use of the nmap utility to discover computers and services on networks.

Beginning the lab

The lab is started from the labtainer working directory on your Linux host, e.g. , a Linux VM. From there, issue the command:

```
labtainer nmap-discovery
```

A screenshot of a terminal window titled 'root@kali: ~/Downloads/labtainer/labtainer-student'. The terminal shows the following commands and output:

```
root@kali:~/Downloads/labtainer/labtainer-student# ls
bin          grader.log   labtainer.log  'labtainer telnetlab'
checkwork.log lab_bin      labtainer-student.pdf nmap
exit         lab_sys     labtainer      README

root@kali:~/Downloads/labtainer/labtainer-student# labtainer nmap-discovery
non-network local connections being added to access control list
[2018-11-20 21:34:04,366 - WARNING : labutils.py:581 - CreateSubnets() ] Already exists! Not creating
intranet subnet at 172.25.0.0/16!

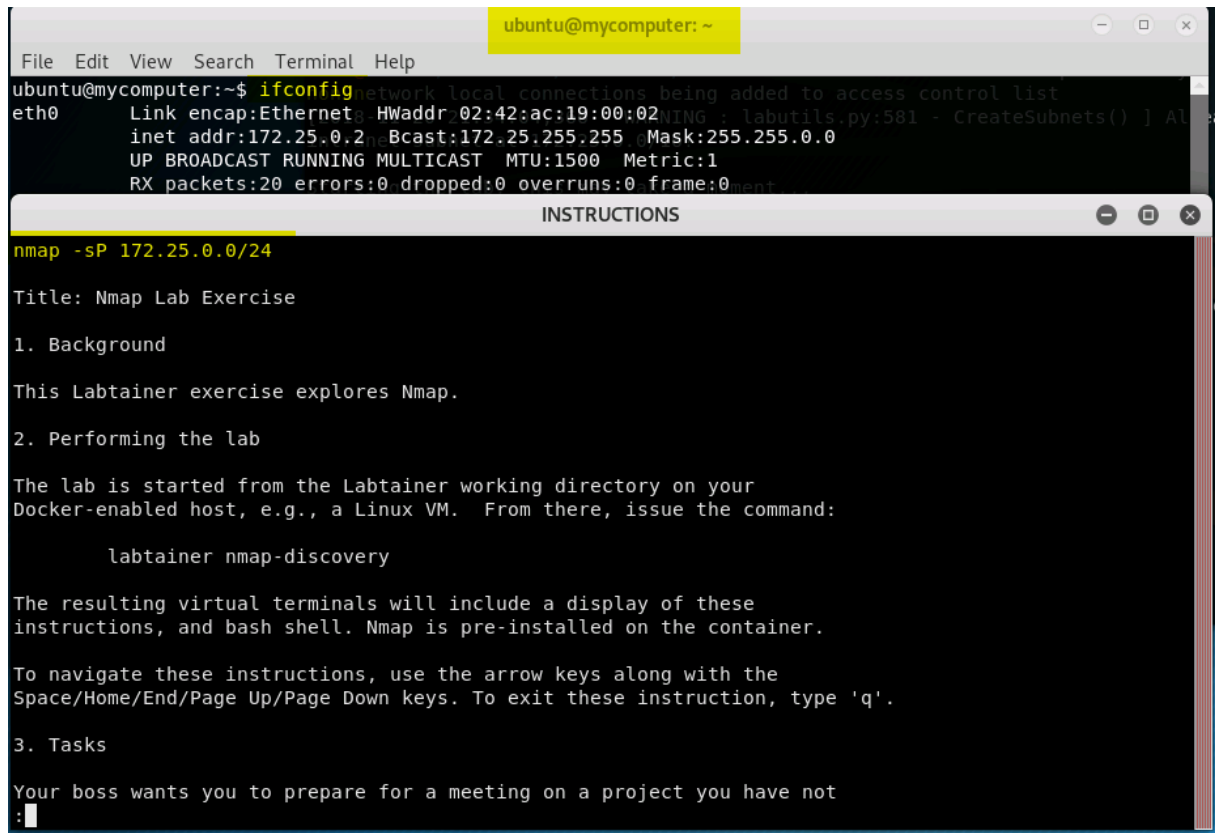
Starting the lab, this may take a moment...

The lab manual is at
  file:///root/Downloads/labtainer/trunk/labs/nmap-discovery/docs/nmapdiscovery.pdf

You may open the manual by right clicking
and select "Open Link".

Press <enter> to start the lab
```

The resulting virtual terminal will include a bash shell. The nmap utility is pre-installed on the computer connected to the terminal.



The screenshot shows a terminal window titled 'ubuntu@mycomputer: ~'. The terminal output displays the configuration for the 'eth0' interface, including its MAC address, IP address (172.25.0.2), broadcast address, and subnet mask. Below this, an 'nmap' command is entered: 'nmap -sP 172.25.0.0/24'. A second window titled 'INSTRUCTIONS' is overlaid on the terminal, providing a guide for the Nmap lab exercise. It includes sections for background, performing the lab, and tasks. The tasks section mentions a meeting preparation and a search for a server named 'friedshrimp'.

```
File Edit View Search Terminal Help
ubuntu@mycomputer:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    link/ether 02:42:ac:19:00:02 brd ff:ff:ff:ff:ff:ff
    inet addr:172.25.0.2 netmask 255.255.255.0
    RX packets:20 errors:0 dropped:0 overruns:0 frame:0
    TX packets:0 errors:0 dropped:0 overruns:0 frame:0
    devices:0
ubuntu@mycomputer:~$ nmap -sP 172.25.0.0/24

INSTRUCTIONS

Title: Nmap Lab Exercise

1. Background

This Labtainer exercise explores Nmap.

2. Performing the lab

The lab is started from the Labtainer working directory on your
Docker-enabled host, e.g., a Linux VM. From there, issue the command:

    labtainer nmap-discovery

The resulting virtual terminals will include a display of these
instructions, and bash shell. Nmap is pre-installed on the container.

To navigate these instructions, use the arrow keys along with the
Space/Home/End/Page Up/Page Down keys. To exit these instruction, type 'q'.

3. Tasks

Your boss wants you to prepare for a meeting on a project you have not
:

```

Tasks

Your boss Randall wants you to prepare for a meeting on a project you have not worked on in months. You have a summary file on the “friedshrimp” server that you previously accessed via ssh; however, you cannot remember the IP address of “friedshrimp”, and you also forgot which port the pesky IT staff assigned for ssh on that server. You know it’s somewhere in between 2000 and 3000. The one thing you most certainly know is that your password is the usual one used in these labs. You are left with only one option: use the nmap command to find the IP address and and port number used by the ssh service. After finding that information review the contents of the “friedshrimp.txt” file from an ssh session.

If you need any help with the nmap commands, you can use “man nmap” to view the manual. Note that in order to ssh to a host via a port other than the default one, use “ssh -p <port> <host>” . Stop the labtainer.

```
ubuntu@mycomputer: ~  
File Edit View Search Terminal Help  
ubuntu@mycomputer:~$ nmap 172.25.0.0/24  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-20 21:38 UTC  
Nmap scan report for mycomputer (172.25.0.2)  
Host is up (0.00022s latency).  
All 1000 scanned ports on mycomputer (172.25.0.2) are closed  
  
Nmap scan report for nmap-discovery.friedshrimp.student.intranet (172.25.0.5)  
Host is up (0.00024s latency).  
All 1000 scanned ports on nmap-discovery.friedshrimp.student.intranet (172.25.0.5) are closed  
  
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.80 seconds  
ubuntu@mycomputer:~$
```

```
ubuntu@mycomputer: ~  
File Edit View Search Terminal Help  
ubuntu@mycomputer:~$ nmap -p 2000-3000 172.25.0.5  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-20 21:58 UTC  
Nmap scan report for nmap-discovery.friedshrimp.student.intranet (172.25.0.5)  
Host is up (0.00019s latency).  
Not shown: 1000 closed ports  
PORT      STATE SERVICE  
2795/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds  
ubuntu@mycomputer:~$
```

```
File Edit View Search Terminal Help
ubuntu@mycomputer:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:ac:19:00:02
          inet addr:172.25.0.2  Bcast:172.25.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3207 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4757 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:191235 (191.2 KB)  TX bytes:313743 (313.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:5362 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5362 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:319830 (319.8 KB)  TX bytes:319830 (319.8 KB)

ubuntu@mycomputer:~$ ssh -p 2795 172.25.0.5
ubuntu@172.25.0.5's password: ubuntu
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.15.0-kali2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Last login: Tue Nov 20 21:52:27 2018 from 172.25.0.2
ubuntu@friedshrimp:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:ac:19:00:05
          inet addr:172.25.0.5  Bcast:172.25.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4819 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3207 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:320588 (320.5 KB)  TX bytes:194304 (194.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

ubuntu@friedshrimp:~$
```

```
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.

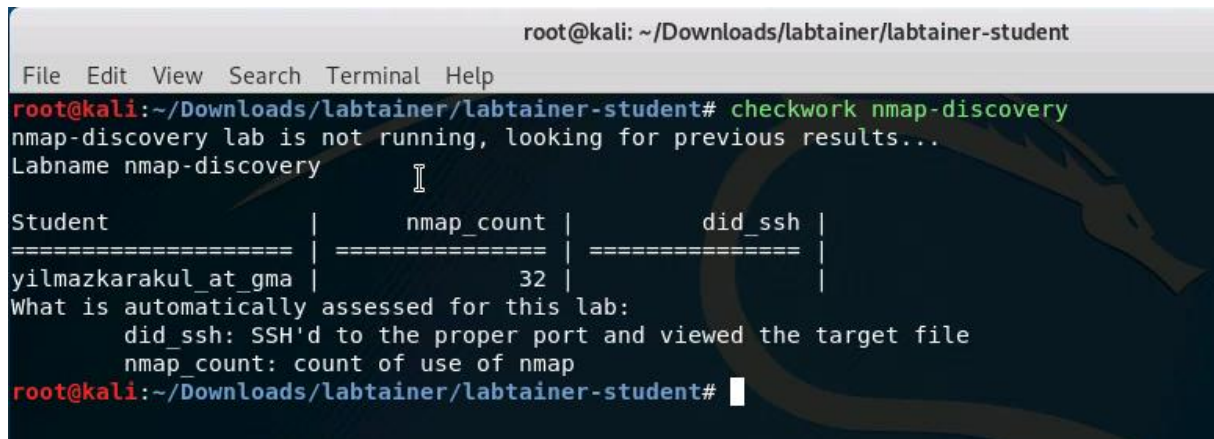
=====

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

When the lab is completed, or you'd like to stop working for a while, run:

stoplab

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



```
root@kali: ~/Downloads/labtainer/labtainer-student
File Edit View Search Terminal Help
root@kali:~/Downloads/labtainer/labtainer-student# checkwork nmap-discovery
nmap-discovery lab is not running, looking for previous results...
Labname nmap-discovery

Student | nmap_count | did_ssh |
=====|=====|=====|
yilmazkarakul_at_gma | 32 | |
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
root@kali:~/Downloads/labtainer/labtainer-student#
```

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. This work is in the public domain, and cannot be copyrighted.

Labtainers

from the host Labtainer working directory (VM). You can always restart the Labtainer and continue your work. When the Labtainer is stopped, a zip file is created and copied to a location displayed by the “stoplab” command. When the lab is completed, send that zip file to the instructor.