

## Lab 6 – Nmap

### Lab Objectives

Upon completion of this lab, you will be able to perform the following:

- Become familiar with nmap switches;
- Use necessary switches to perform OS fingerprinting;
- Discover target host vulnerabilities.
- Extra miles will test your skills – but not mandatory
  - Point booster

### Lab Materials

- Tools and utilities:
  - Product: nmap
  - Installed on Kali: yes
  - Manufacturer: Gordon Lyon
  - Web site: <https://nmap.org/>

### Lab Instructions

- Complete this lab;
- Answer questions and add screenshots into the corresponding textboxes;
- Submit the submission file in PDF format for grading.

## Introduction

Nmap (**N**etwork **M**apper) is a free, open-source, network scanning software designed to audit a range of hosts or a single host. It attempts to determine what services are running, which OS versions is installed, types of firewalls, and possible vulnerabilities. To find all this information, Nmap sends TCP, UDP, SCTP, and ICMP packets to the target host and examines the response by comparing the result to its database.

Nmap's creator Gordon "Fyodor" Lyon had adopted the pseudonym "Fyodor", which he picked up after reading Russian author Fyodor Dostoevsky.

Initially, Nmap was written in C++ and first introduced, with source code, in Phrack Magazine in September 1997. Later on, it's been extended with C, Perl and Python.

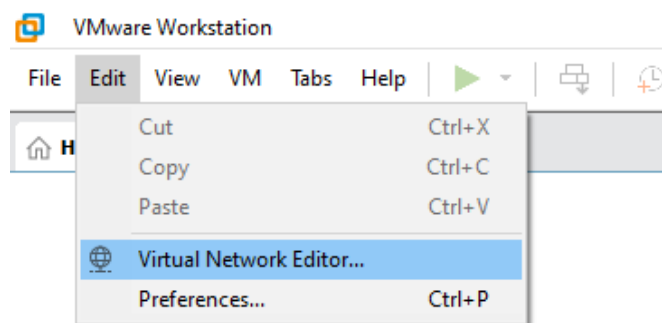
Nmap has achieved a fame in popular culture, becoming the hacking tool featured by directors in at least a dozen movies. Its first break in big-time films came in "The Matrix Reloaded", where the Trinity character showed off her hacking abilities. (You can see her in action in a clip "Trinity uses nmap in The Matrix Reloaded" - <https://www.youtube.com/watch?v=0PxTAn4g20U>).

## Part 1: Connecting your Kali machine to the security lab network:

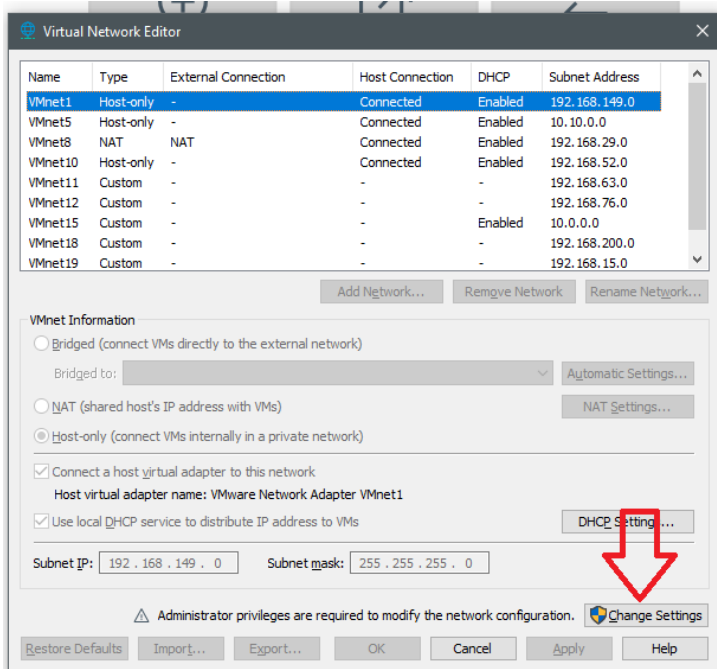
1. The physical machines in the lab are connected to more than one network through more than one NIC card. ? First, you'll need to find which card is "REALTEK" with an IP address in the range 172.16.x.x/28. On your physical machine, goto "start" and search "cmd" and hit Enter.
2. Run the following command:

```
ipconfig /all
```

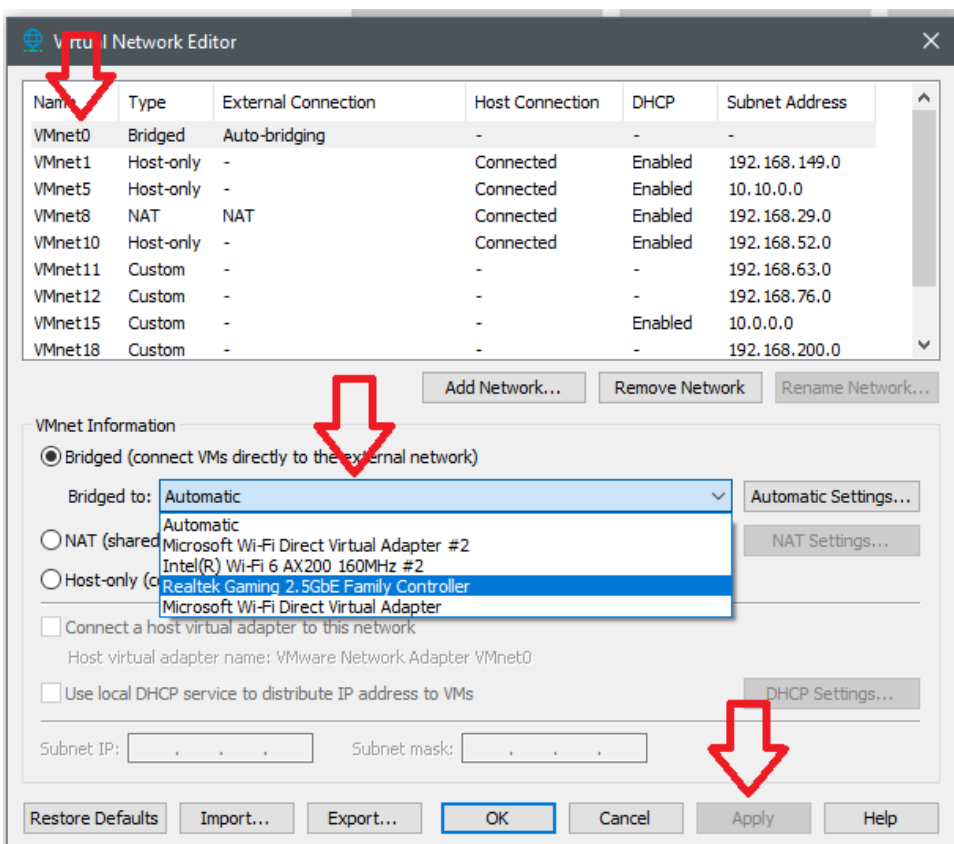
3. Identify which NIC card has the 172.16.x.x IP address.
4. Go to VMWare Workstation. On the top menu, choose "Edit">>"Virtual Network Editor"



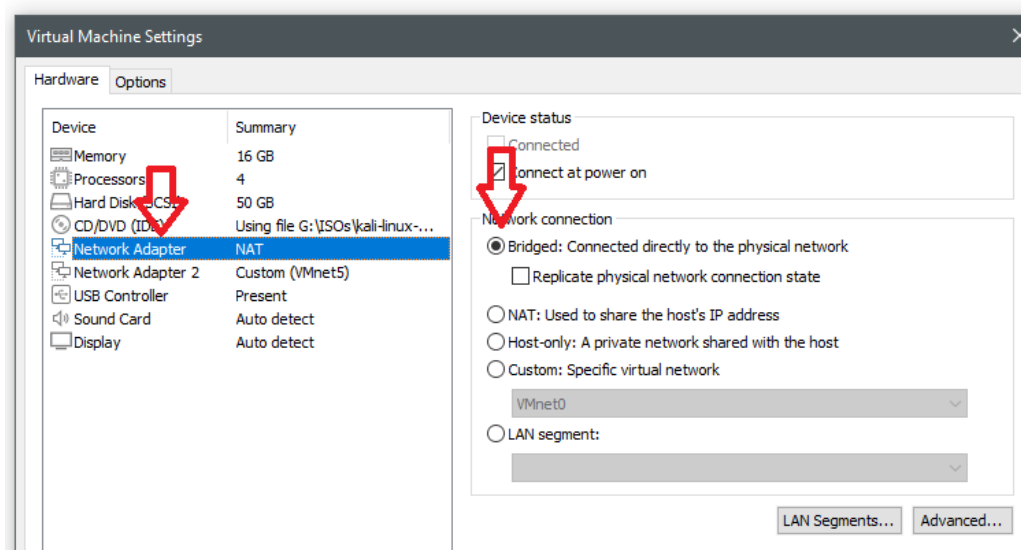
5. Click on "Change settings.."



- Click on the settings of "Vmnet0" which is the bridging network setup, and click on the dropdown menu to choose the NIC card that you have identified in step 3. Then click apply..



- Before starting your Kali VM, change the network connection to “Bridged”.



Check the “Replicate physical network connection state” checkbox.

- Start your Kali VM.
- After booting, run “ifconfig” command.
- The Kali VM IP address should be in the 172.16.x.x range.

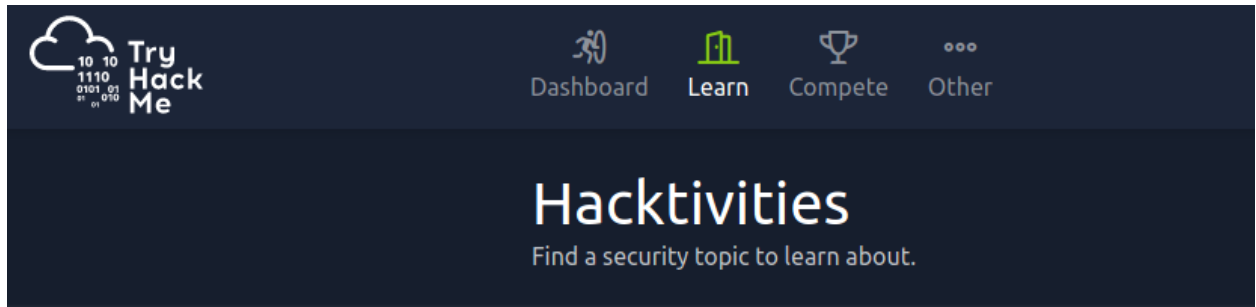
## Part 2: Scanning

Use the IP range 172.16.11.0/26 as your target range.

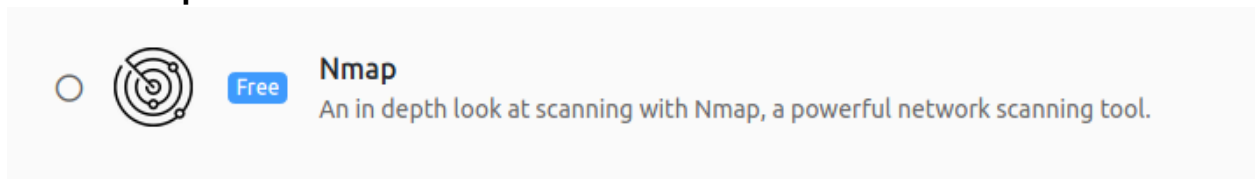
- What is NMAP switch to detect active IP addresses?**  
Include a screenshot for detecting active hosts within the target range.
- What is NMAP switch to detect running service version on open port?**  
Include one screenshot for each target found in the range with the results of service versions.
- What is NMAP switch to scan ALL ports?**  
Include a screenshot for running this command on one of the targets found in the range.
- What is the NMAP switch to detect the operating system?**  
Include one screenshots showing the operating system detected for each target found within the range.
- Vulnerability Scanning:** Use “nikto” web vulnerability scanner to scan one target host running web services. Include screenshots showing the command used and the results of the scan.

### Extra Mile – not mandatory

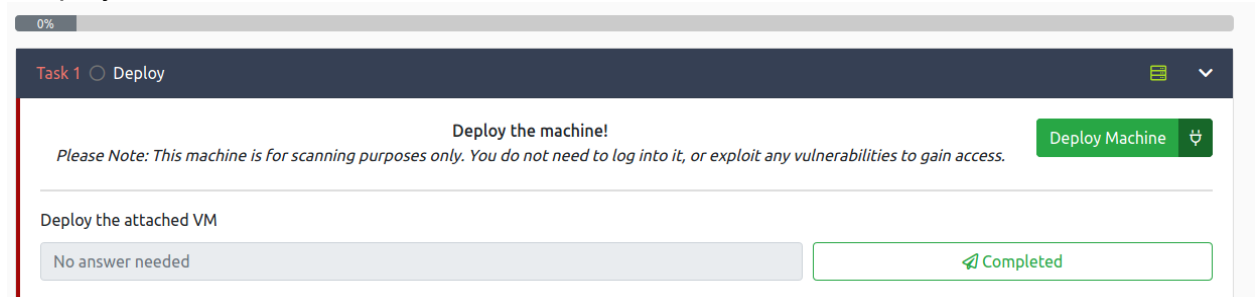
1. Sign up to Try hack me <https://tryhackme.com/>
2. Download openvpn on your kali “**sudo apt install openvpn**”
3. Download openvpn settings from your **tryhackme.com** profile
4. Connect to the downloaded vpn: “**sudo openvpn <downloaded>.ovpn**”
5. Go to “learn”




6. Navigate to “**Networking Fundamentals**”
7. Select “**nmap**”



8. “Deploy machine”



1615



# Nmap

An in depth look at scanning with Nmap, a powerful network scanning tool.

[Room Tutorial](#)[Start AttackBox](#)[Help](#)[Options](#)

Active Machine Information

Title	IP Address	Expires	
Further Nmap	10.10.168.172	57m 25s	<a href="#">Add 1 hour</a> <a href="#">Terminate</a>

0%

Task 1 ☐ Deploy

Deploy the machine!

*Please Note: This machine is for scanning purposes only. You do not need to log into it, or exploit any vulnerabilities to gain access.*

[Deploy Machine](#)

Deploy the attached VM

No answer needed

Completed

9. Scan the provided IP address with nmap and provide screenshot:
- All TCP ports and treat host as "online"
  - Top 100 UDP ports
  - List Open TCP ports (if any)
  - List open UDP ports (if any)

## Part 2: Submit your lab submission file



- Doublecheck all your answers.
- Save the file on your computer for future reference.
- Save the file again as a ".pdf" file.
- Submit the PDF file for grading.