**PART 1**

1.1 Use 'ip a' command to determine the block of IP addresses used by the virtual local network where you run Kali. Write your answer into the lab report. Your answer should be in the form of /<#mask-bits>, e.g., 192.168.221.0/24

**192.168.1.0/24**

1.2 Use n-map with appropriate options to discover which hosts are alive on this local network without scanning ports on these hosts.

a) What is your command line used?

**sudo nmap -sn 192.168.1.0/24**

b) Include the list of discovered active hosts into your lab report.

**192.168.1.1  
192.168.1.101  
192.168.1.102  
192.168.1.103**  
1.3 Find out the IP addresses of the gateway, the Kali VM, the Win7 VM and the Metasploitable2 VM as you did in Lab 1.  
  
a) Write each machine and its IP address into your lab report.  
 **Windows: 192.168.1.101  
Kali: 192.168.1.102  
Met: 192.168.1.103**

b) Check whether these IP addresses appear in the active hosts list above. Simply answer yes or no in your lab report  
  
**Yes.**

1.4 Start Wireshark to capture all traffic on the network. Then, run the command line for task 1.2 again. Observe the Wireshark capture. Based on the observation, explain in your report how nmap discovers active hosts in a local network.

**It has 5 ways to discover hosts on a network.**

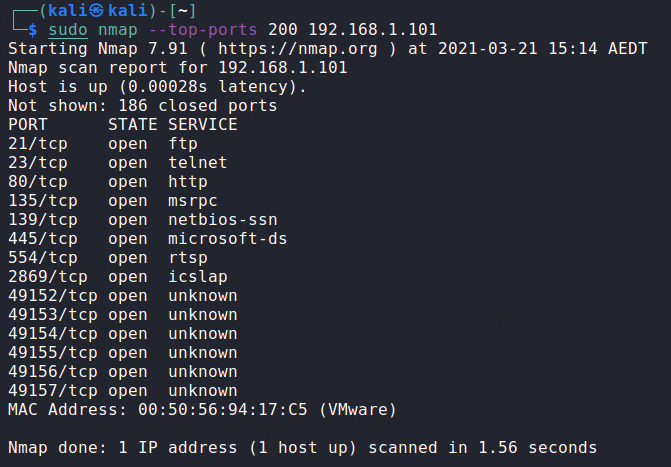
* 1. **Send ARP request (if within the same LAN) the most effective way**
  2. **Send ICMP Echo Request**
  3. **Send TCP SYN to port 443**
  4. **Send TCP ACK to port 80**
  5. **Send ICMP Timestamp Request**

**In this case it does this using ARP requests, if the ARP succeeded, it won’t try the others. The ARP request sends ARP messages through the ARP protocol and the list of addresses according to the subnet group specified gets a message and it responds to see if they are alive.**

**PART 2**

2.1 Use nmap to detect whether the top 200 TCP ports on the WinXP VM are open. Write your command line and the scan results into your lab report.

**sudo nmap --top-ports 200 192.168.1.101 [could add -sS but nmap scans TCP ports by default]**



2.2 Start Wireshark to capture all traffic on the network. Then, use nmap with proper arguments to only detect whether the TCP port 80 on the Metasploitable2 VM is open (Hint: see how to specify ports in our slides).

a) Write your command line into the lab report.

**sudo nmap -p 80 192.168.1.103 [could add -sS but nmap scans TCP ports by default]**

b) Observe the Wireshark capture. Based on the observation, explain in your report how nmap determines whether a port is open or not.   
  
**It establishes a connection using the TCP SYN protocol.**  
  
**1. It sends a SYN  
2. Other side responds with an ACK  
3. After detecting port is open, nmap sends a RST, to reset connection- Prevents connections from being established, thus saving memory resources and being secretive.**



**PART 3**

3.1 Use nmap with proper arguments to detect services possibly provided by the top 200 TCP ports on the WinXP VM.

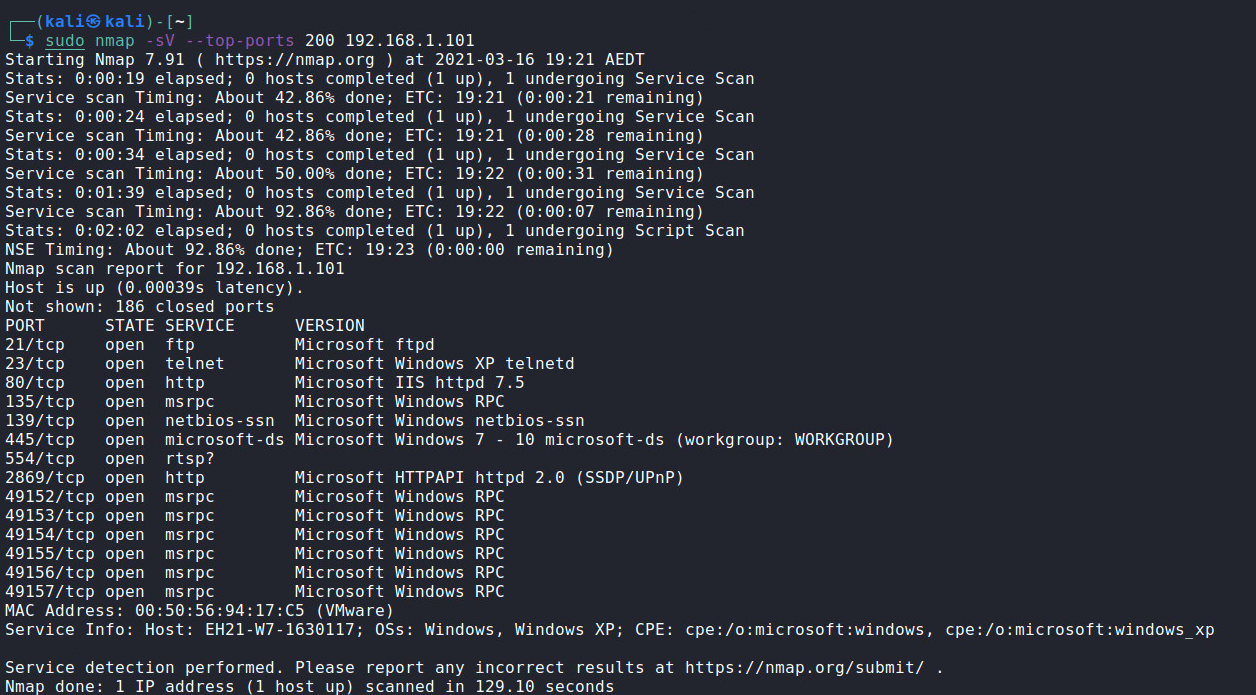
a) Write your command line and the scan results into your lab report.

**sudo nmap -sV --top-ports 200 192.168.1.101 [could add -sS but nmap scans TCP ports by default]**

b) Compare the output with the one from Task 2.1. What are the differences?

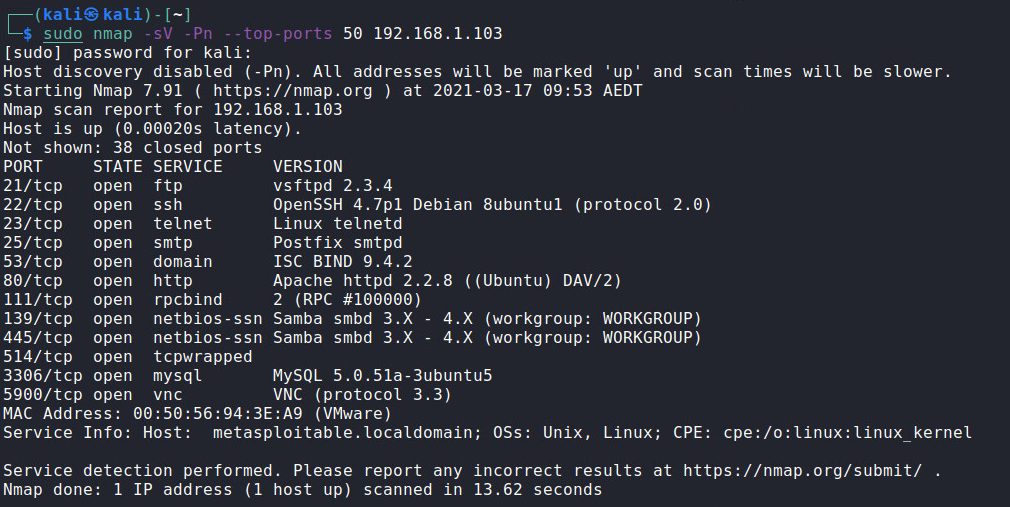
**There is extra information about the service and the versions of those services by providing a name for those services that are supported by TCP, It also provides extra information like**

1. **- Hostname**
2. **- Deduced OS:**
3. **- Common Platform Enumeration (CPE) representation:   
     
   this is other service information [host,CPE, OS], essentially you can learn about the OS and programs that are operating on the ports in greater detail that is running on the other end.**



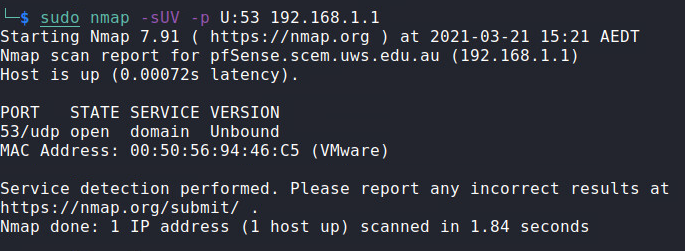
3.2 Use nmap with proper arguments to detect services possibly provided by the top 50 TCP ports on Metasploitable2 VM and skip host discovery as you already know that it is running. Write your command line and the scan results into your lab report.

**sudo nmap -sV -Pn --top-ports 50 192.168.1.103 [could add -sS but nmap scans TCP ports by default]**



3.3 Use nmap with proper arguments to detect service on UDP port 53 on the gateway. (Hint: see service detection part in our slides). Write your command line and the scan results into your lab report.

**sudo nmap -sUV -p U:53 192.168.1.1**



**Part 4**

4.1 Use nmap with proper arguments to detect OS on the Metasploitable2 VM.

a) Write your command line into your lab report.

**sudo nmap -O 192.168.1.103**

b) What OS does nmap thinks the Metasploitable2 VM is running?

**Running: Linux 2.6.X**

c) If it is Linux, what is the kernel version number believed by nmap?

**OS CPE: cpe:/o:linux:linux\_kernel:2.6**

4.2 Use nmap with proper arguments to detect OS on the WinXP VM.

a) Write your command line into your lab report.

**sudo nmap -O 192.168.1.101**

b) What OS does nmap thinks the WinXP VM is running?

**Running: Microsoft Windows 7|2008|8.1**

c) If it is WinXP, can nmap be sure that it is XP SP3?

**Yes it is in the OS details. OS details: Microsoft Windows 7 SP0 - SP1. The windows 7 that we are using is actually running service pack 1.**

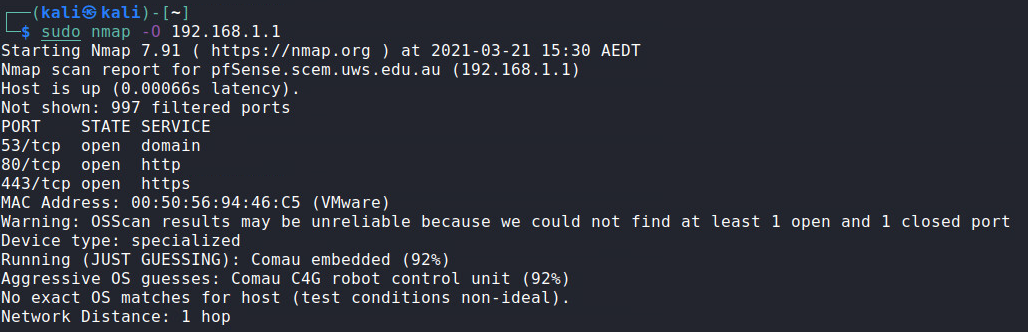
4.3 Use nmap with proper arguments to detect OS on the gateway (which is your virtual NAT box).

a) Write your command line into your lab report.

**sudo nmap -O 192.168.1.1**

b) What OS does nmap thinks the gateway device is running?

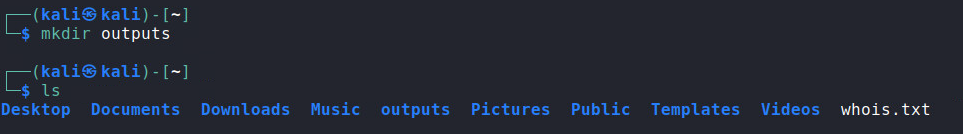
**It appears as if it is uncertain or that it is guessing. It specified that it guesses “Comau embedded)”; “No exact OS matches for host (test conditions non-ideal).”**

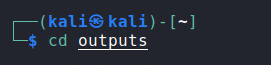


**PART 5**

5.1 Make sure you are currently in the directory of "/home/kali".

a) Create a new directory under it called "outputs" using command "mkdir". If you are unsure how to use "mkdir", do "man mkdir".



b) Execute "cd outputs".   
  


c) Execute "pwd". What's the result of this command?

**/home/kali/outputs**

5.2 Use nmap with proper arguments to detect whether the TCP ports in the range of 8001-8010 on Metasploitable2 VM are open, and output in all three formats of Normal, XML, and Grepable. The output file names without the suffix part should use "ports8001-8010". Write your command line into your lab report.

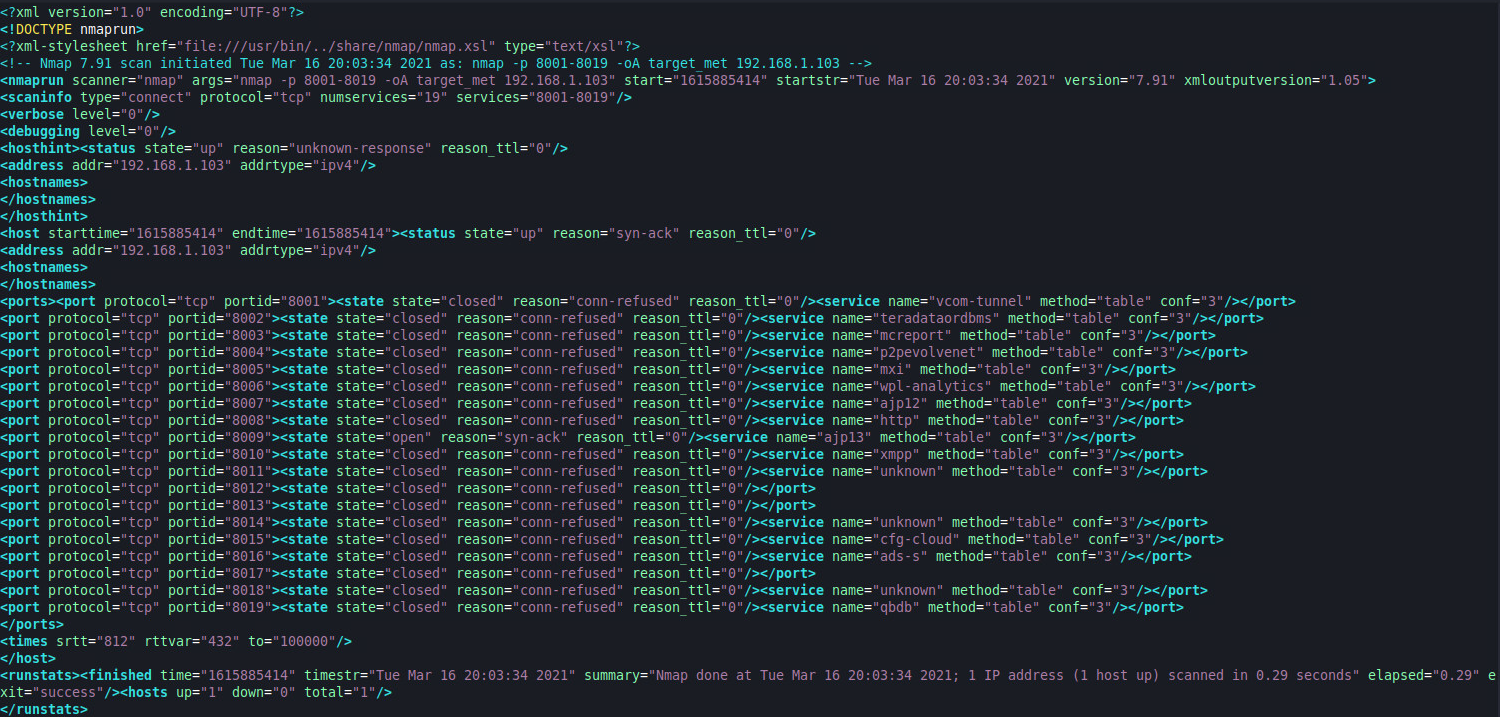
**sudo nmap -p 8001-8019 -oA ports8001-8010 192.168.1.103 [could add -sS but nmap scans TCP ports by default]**

5.3 What are the full file names of the three output files from Task 5.2?

**1. ports8001-8010.gnmap [Greppable]  
2. ports8001-8010.nmap [normal]  
3. ports8001-8010.xml [XML output]**

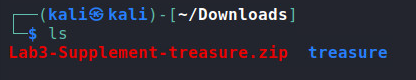
5.4 Examine the contents of the XML output file, which is convenient for exporting nmap output to other programs. An XML file typically includes a hierarchy of tags. For example, you'll notice that the <scaninfo> tag is nested inside the <nmaprun> tag in XML output file. Similarly, which tag is the <port> tag nested in?

**It’s nested in the “<ports>” tag**



PART 6

6.1 Decompress this file using the ‘unzip’ command. Write your command line into the lab report. (If you are unsure how to use ‘unzip’, do a ‘man unzip’.)   
 **unzip /home/kali/Downloads/treasure.zip**



6.2 After decompressing, you should see a directory called “treasure”. Under this directory, you see many further directories and files. Only one of these files contains a line with the following string “Secret:OpenSeseme”. Use ‘grep’ to find out which file it is. (Suppose you are now under the directory “/home/kali/Downloads/treasure”). Write your command line and result into the lab report.

**grep -r "Secret:OpenSeseme"**

