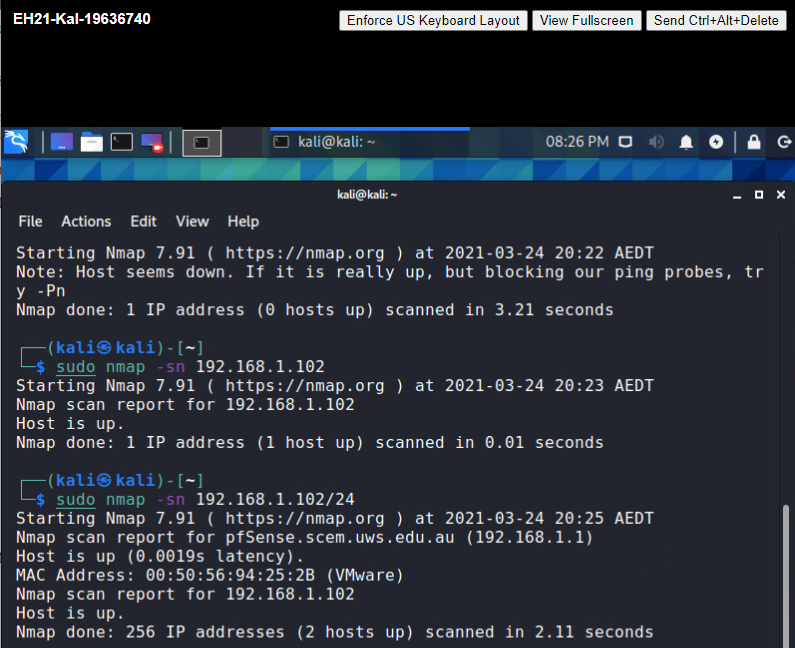
**Question 1**

**1.1** 192.168.1.102/24

**1.2**

**a)** sudo nmap –sn 192.168.1.102

**b)** 

**1.3**

**a)** Kali VM IP address: 192.168.1.102

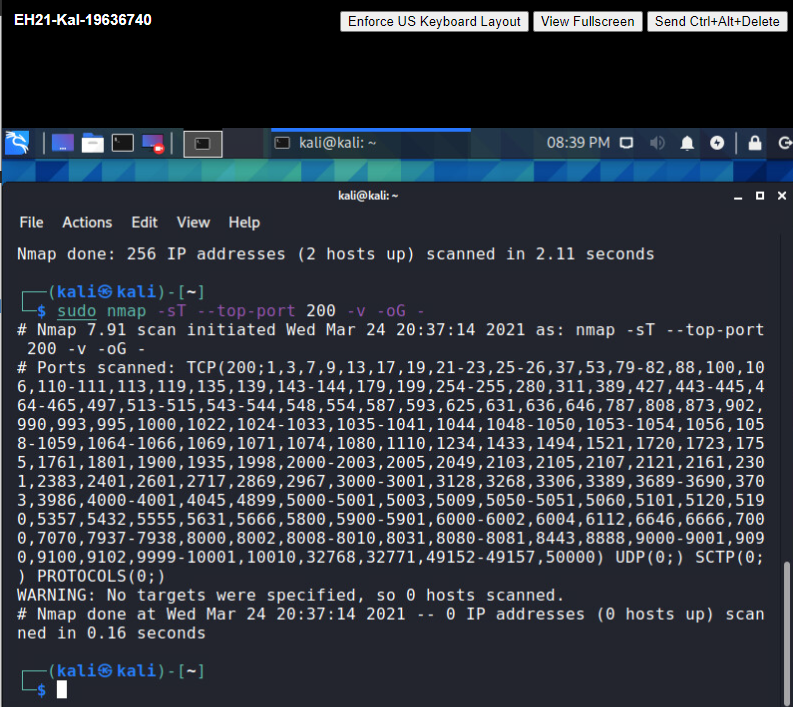
Win7 VM IP address: 192.168.1.101

Metasploitable2 VM IP address: 192.168.1.103

**b)** yes

**1.4** The first two ARP packets are to detect whether the host is alive. First, we choose init seq num: x; then Send SYN packet to server side. Then server Choose init seq num: y and send SYN + ACK packet to our (Client) side. Finally, we send ‘RST = 1’ to let server discard this connection.

**Question 2**

 **2.1** sudo nmap -sT --top-ports 200 -v -oG –

**2.2**

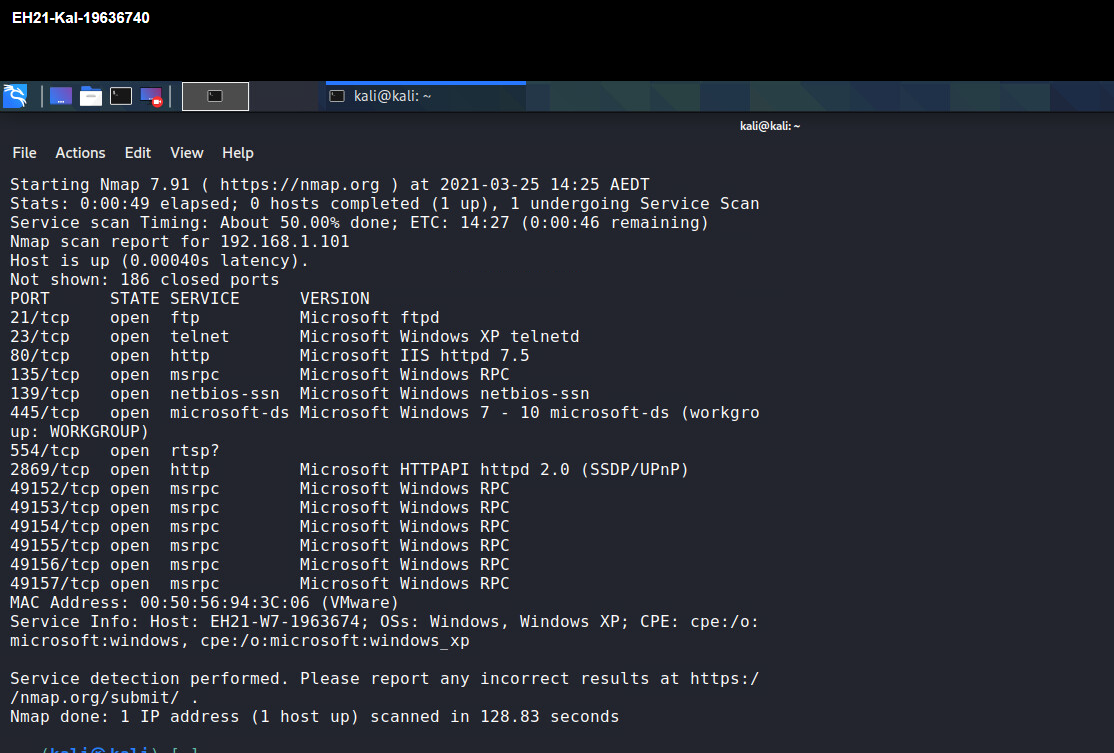
**a)** sudo nmap –p 80 192.168.1.103

**b)** Open port status indicates that those ports actively accept and respond to an incoming connection, and an application is listening to these connections such as TCP, UDP or SCTP. A closed port is like an open port; it is accessible (receives and responds to Nmap probe packets). However, the only difference is that no application is listening on it.

**Question 3**

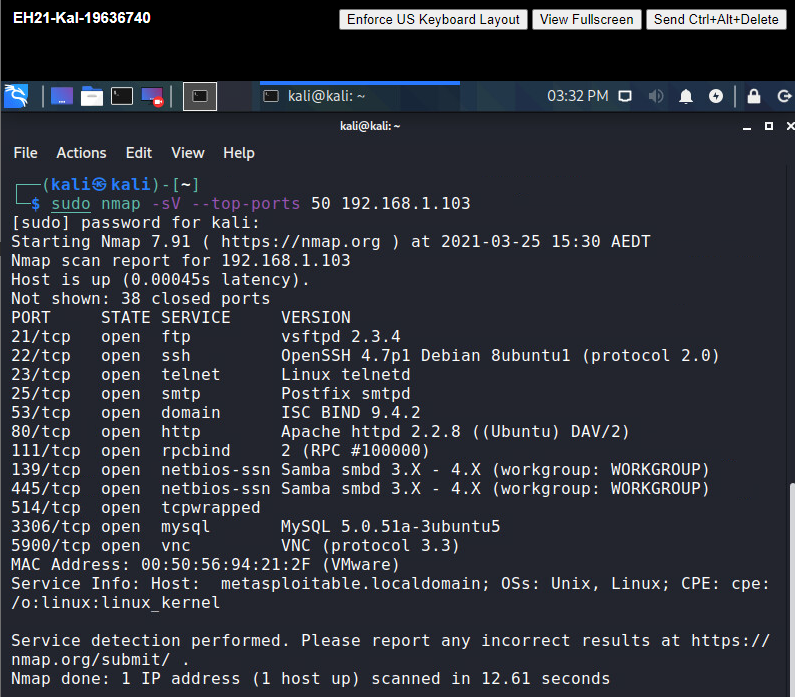
**3.1**

**a)** sudo nmap -sV --top-ports 200 192.168.1.101

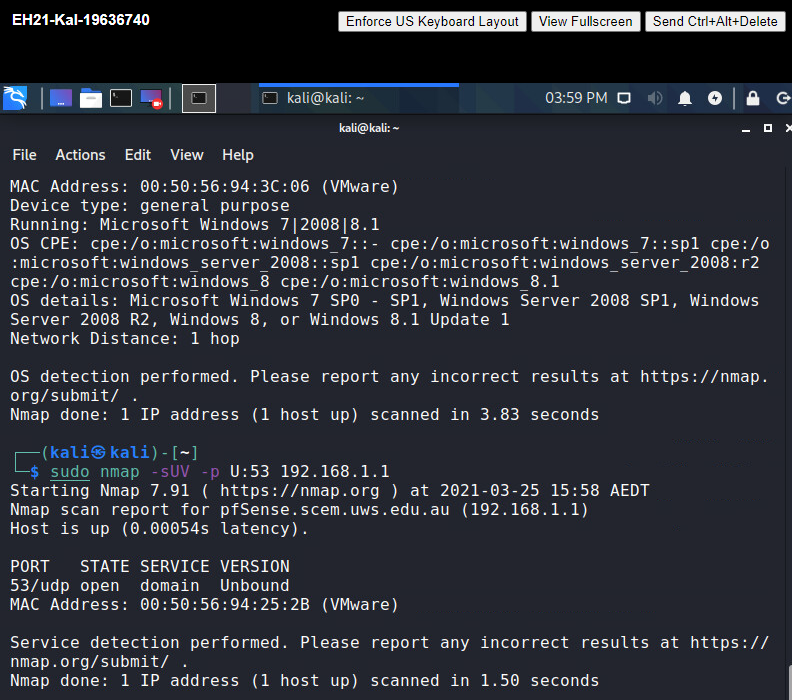


**b)** there are only 14 in 200 TCP ports that are open and possibly provide services.

**3.2** sudo nmap -sV --top-ports 50 192.168.1.103



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



**Question 4**

**4.1**

**a)** sudo nmap -O 192.168.1.103

**b)** Linux 2.6.X

**c)** kernel: 2.6 (2.6.9 – 2.6.33)

**4.2**

**a)** sudo nmap -O 192.168.1.101

**b)** MicrosoftWindows 7|2008|8.1

**c)** No, it is MicrosoftWindows 7 SP0

**4.3**

**a)** sudo nmap -O 192.168.1.1

**b)** It is guessing it is running Comau embedded (92%), OpenBSD 4.X (86%)

**Question 5**

**5.1**

**a)** mkdir outputs

**b)** /home/kali/outputs

**5.2** sudo nmap -oA ports8001- 8010 -p 8001-8010 192.168.1.103

**5.3** ports8001- 8010.nmap

ports8001- 8010.xml

ports8001- 8010.gnmap

**5.4** The XML output, <ports>

**Question 6**

**6.1** assuming we are under /home/kali/Downloads (cd Downloads)

unzip Lab3-Supplement-treasure

**6.2** grep -r “Secret:OpenSeseme” \*

