# CYSE 450- Ethical Hacking and Penetration Testing

## Assignment-3

## Total:100 Points

Please complete all the tasks and submit the screenshot for each along with the respective step number in a word or pdf file.

You may refer to the examples demonstrated during the class or go to help/manual page tpo learn about the commands usage for nmap, dig and, host (using –h)

**Task-A: [30 points] Install the following Virtual Machines to complete your lab and submit the screenshots for the IP address displayed in the terminal after using ifconfig (in Linux VM)/ipconfig (in Windows VM) command for all these machines:**

1. Kali Linux
2. Metasploitable2(Source:https://sourceforge.net/projects/metasploitable/files/Metasploitable2/)
3. Windows XP or Windows 7 (Refer to the class recording to install this)

**Task B: [30 points] Perform passive reconnaissance using archive.org and netcraft** (For this task, you can use any browser of your actual computer)

Organizations keep updating their websites from time to time. The archive.org website keeps track of all the updates or changes since the website was launched. An attacker can use this website to determine the changes made on the website. An attacker may use this information to conduct various attacks, such as phishing.

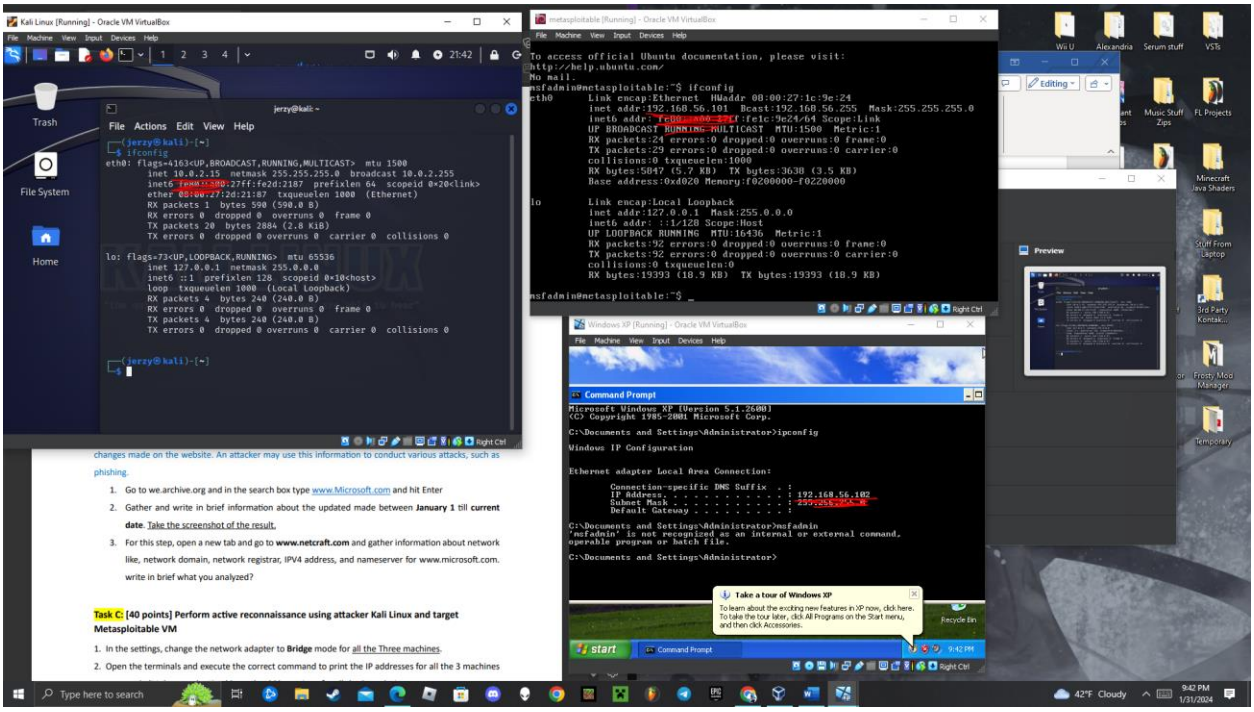
1. Go to we.archive.org and in the search box type www.Microsoft.com and hit Enter
2. Gather and write in brief information about the updated made between **January 1** till **current date**. Take the screenshot of the result.
3. For this step, open a new tab and go to **www.netcraft.com** and gather information about network like, network domain, network registrar, IPV4 address, and nameserver for www.microsoft.com. write in brief what you analyzed?

**Task C: [40 points] Perform active reconnaissance using attacker Kali Linux and target Metasploitable VM**

1. In the settings, change the network adapter to **Bridge** mode for all the Three machines.
2. Open the terminals and execute the correct command to print the IP addresses for all the 3 machines separately (Make sure the IP address should be unique for all the 3 machoines.

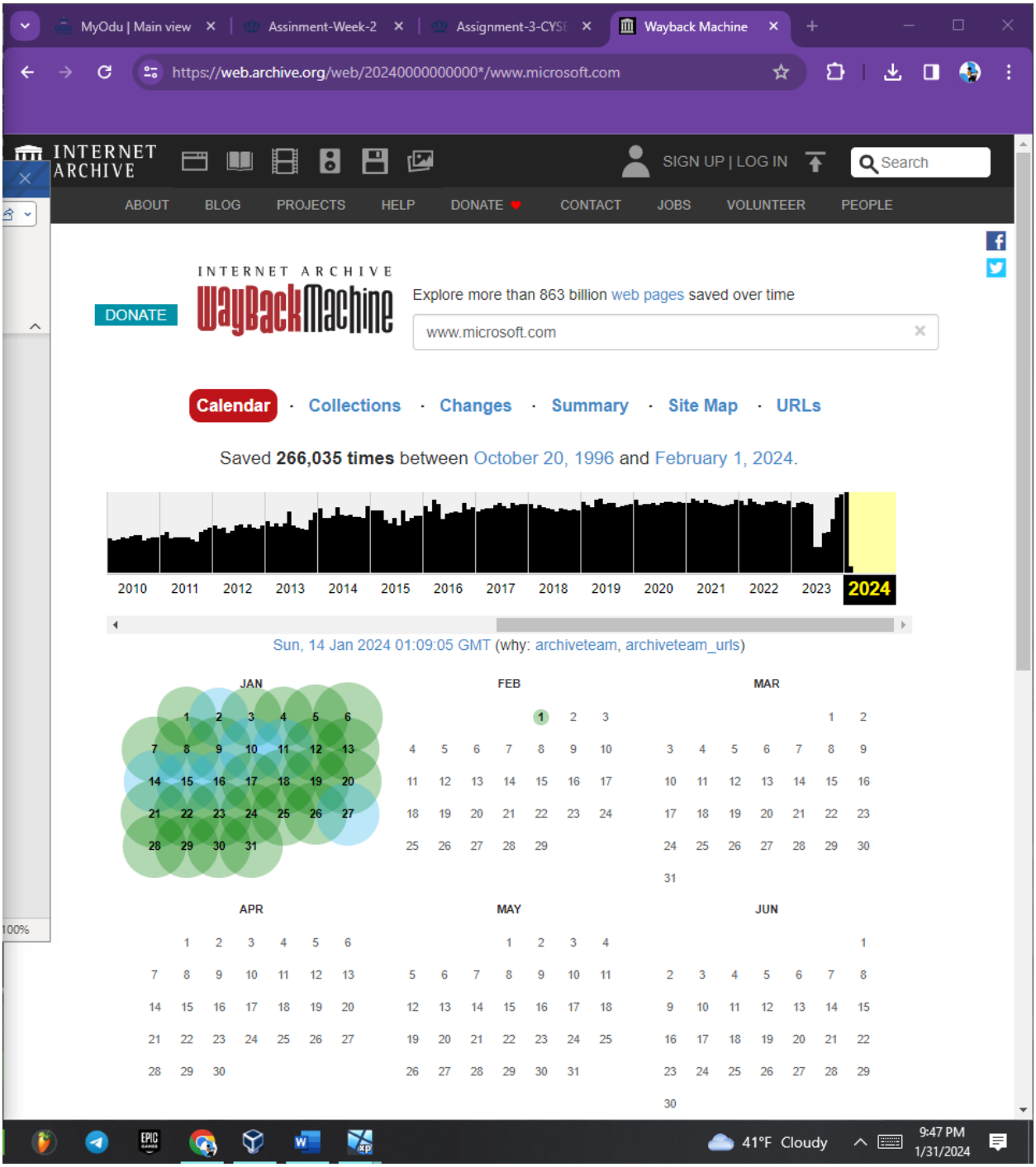
3. In Kali Linux terminal, execute the command (host/dig) to demonstrate whether the host (www.odu.edu or www.amazon.com) is live/UP or not. **Also provide the reason if the host is live /UP by using the option - -reason**.
4. Using terminal in Kali Linux, perform **DNS enumeration** using dnsenum command for www.odu.edu or www.google.com (Please refer to the slide for using dnsenum)
5. In kali Linux, perform **ICMP Sweep scan** to gather information about the target machine (Metasploitable Linux) by sending **ICMP echo request** to target machine (using its ip address), using **nmap** command with correct options. Highlight the line indicating whether the ICMP reply has been received or not. [Do not forget to disable the arp-ping]
6. In kali Linux, perform **ICMP Sweep scan** to gather information about the target machine (Windows Xp/7) by sending **ICMP echo request,** using **nmap** command with correct options. (Make sure the firewall is turned on in windows machine)

Task A

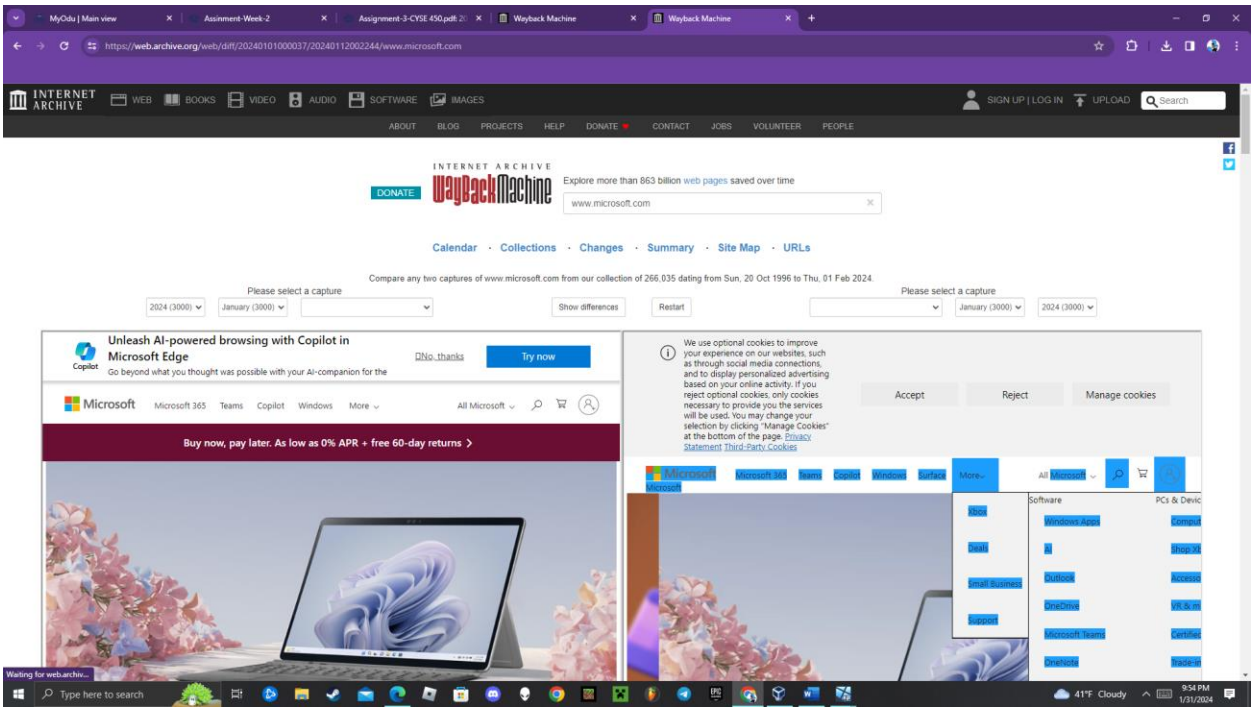



I have shown all three IP addresses in the screenshot. Kali is 10.0.2.15, metasploitable is 192.168.56.101, and windows XP is 192.168.56.102.

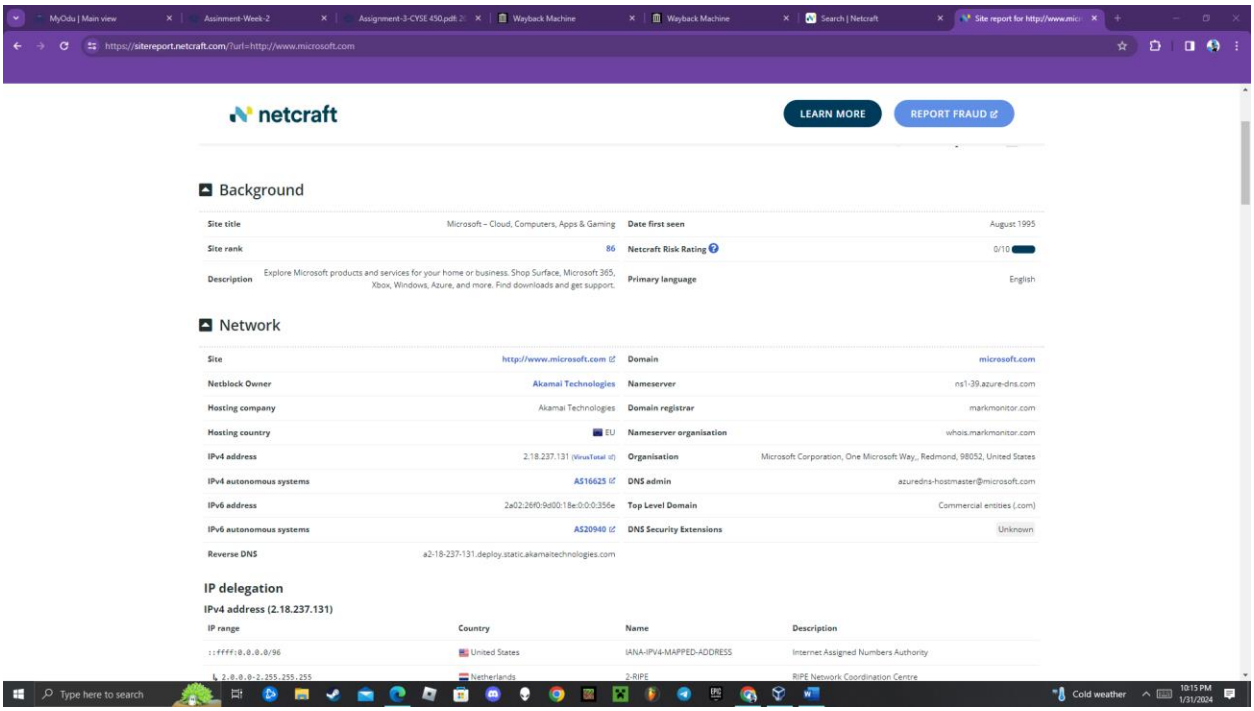
Task B




1. Here I took a screenshot of me looking up [www.microsoft.com](http://www.microsoft.com) on the website. (Sorry its only half the screen. I have the instructions for the homework taking up the other side and I figured you didn't want to see that.)

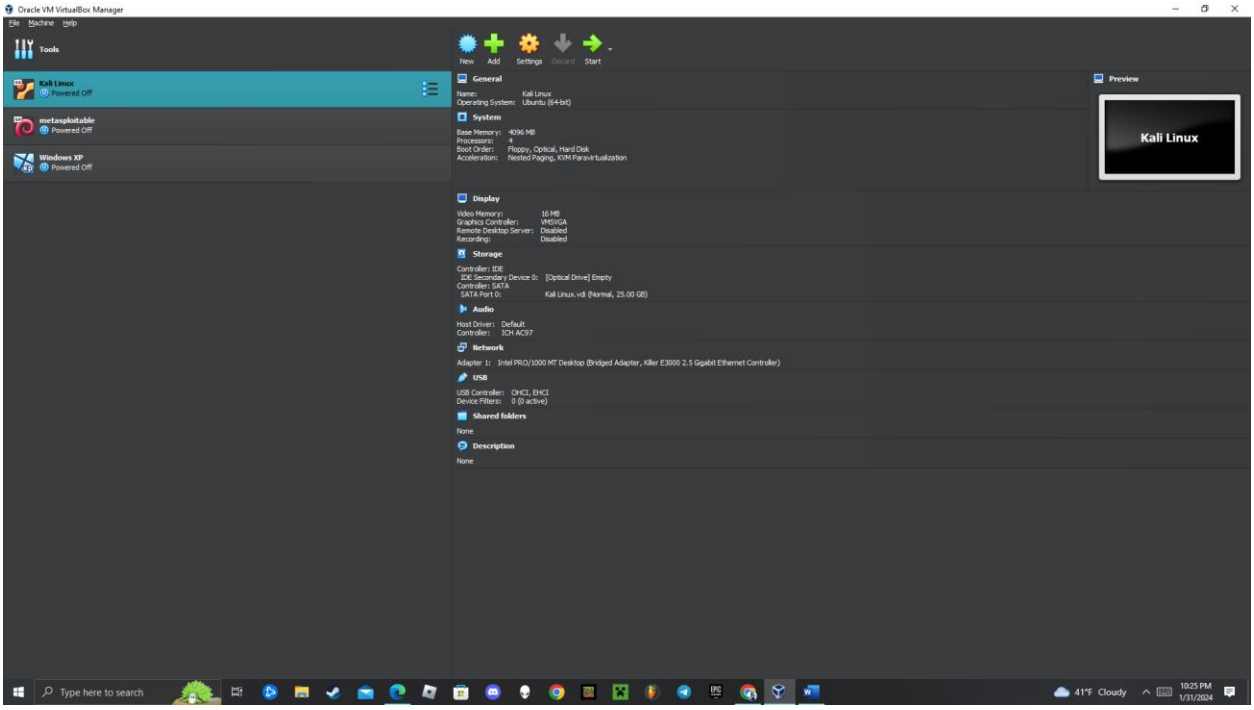



2. Here I took a screenshot of me looking at the difference between January 1st and January 10th(the latest they had data for). Im not sure how or if I can directly assess differences in specific backend or vulnerabilities through this so ill just describe the differences I can physically see with my eyes. On January 1st the top of the screen includes an ad/deal saying “buy now, pay later” that is not included on the January 10th version. When I scroll down, the content is the same, but the design is slightly different with the older version having links in two separate columns while the updated site only has one column. When I scroll down even further, the old site was advertising a special deal on Xbox and PC games that has since disappeared. The final difference I see on the homepage is that the bottom section previously advertised physical products while the new version seems to be advertising subscription services.

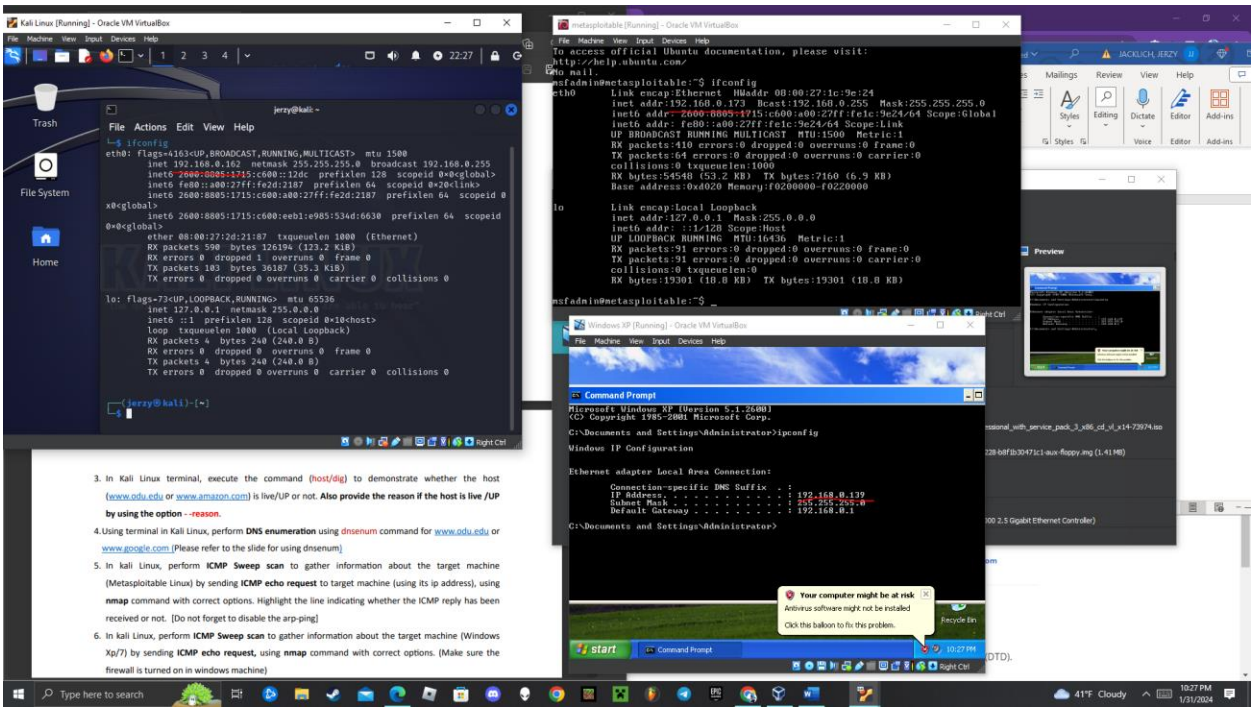



3. This is the screenshot for netcraft. The domain is microsoft.com, the registrar is markmonitor.com, IPv4 is 2.18.237.131, and nameserver is ns1-39.azure-dns.com. Netcraft also listed an address for the company as well as the hosting country for the webpage. Surprisingly is was hosted in the EU. Netcraft also lists site technology such as SSL, Javascript, UTF8, HTML5 in addition to a lot more.

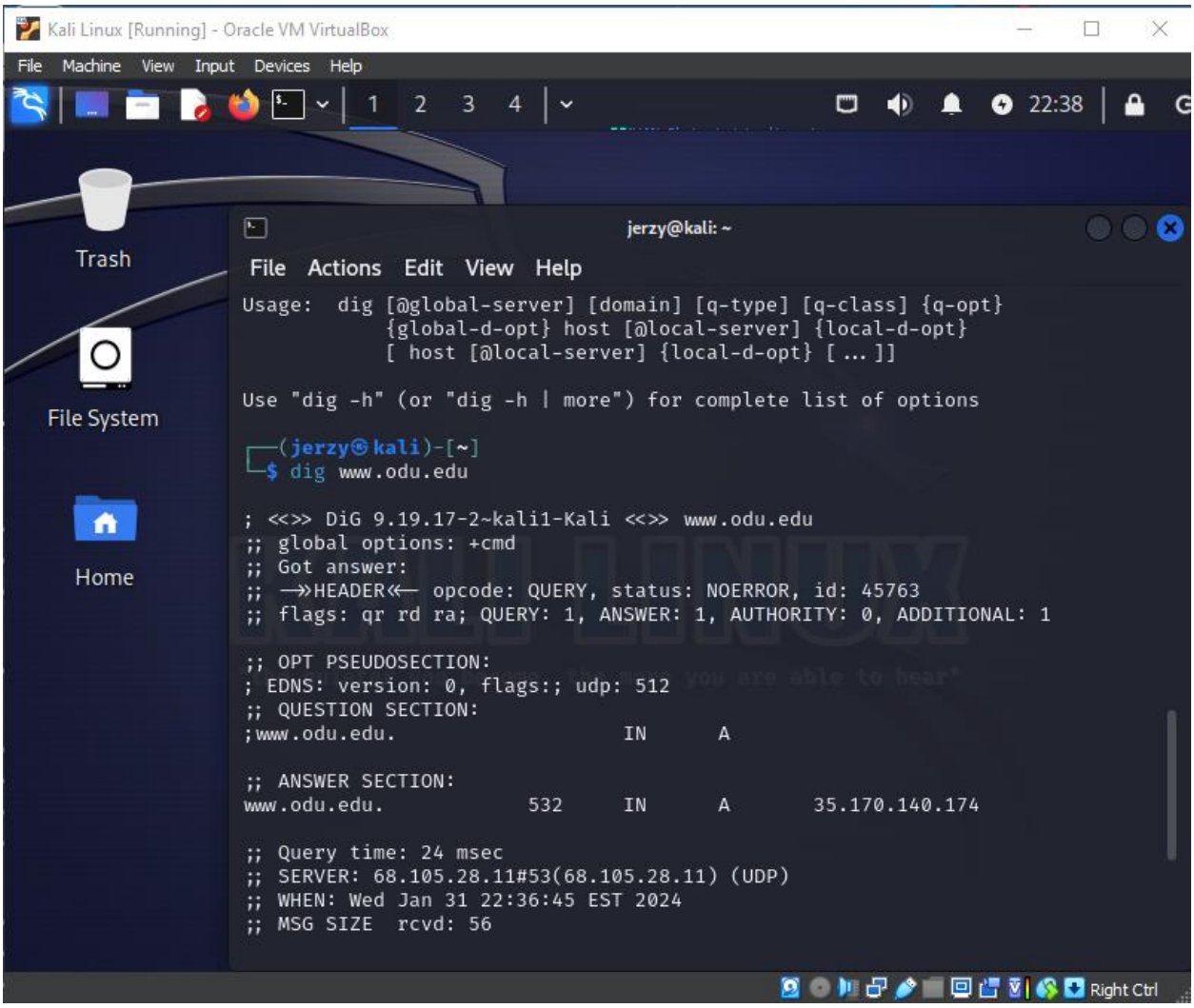
Task C



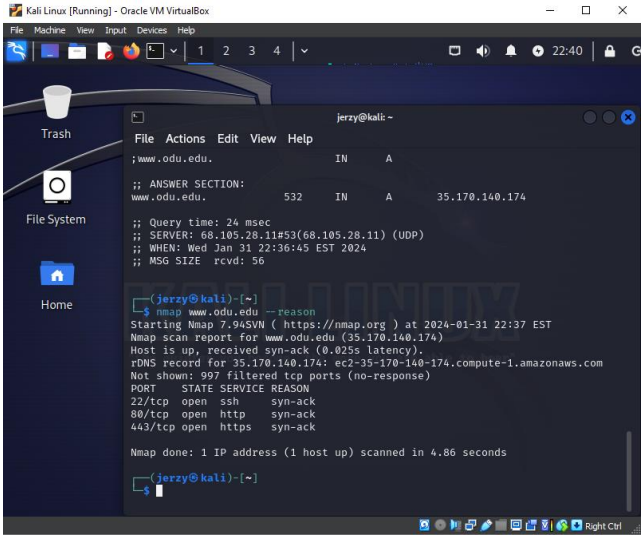

1. All three of the virtual machines I will be using have been changed to bridged mode.

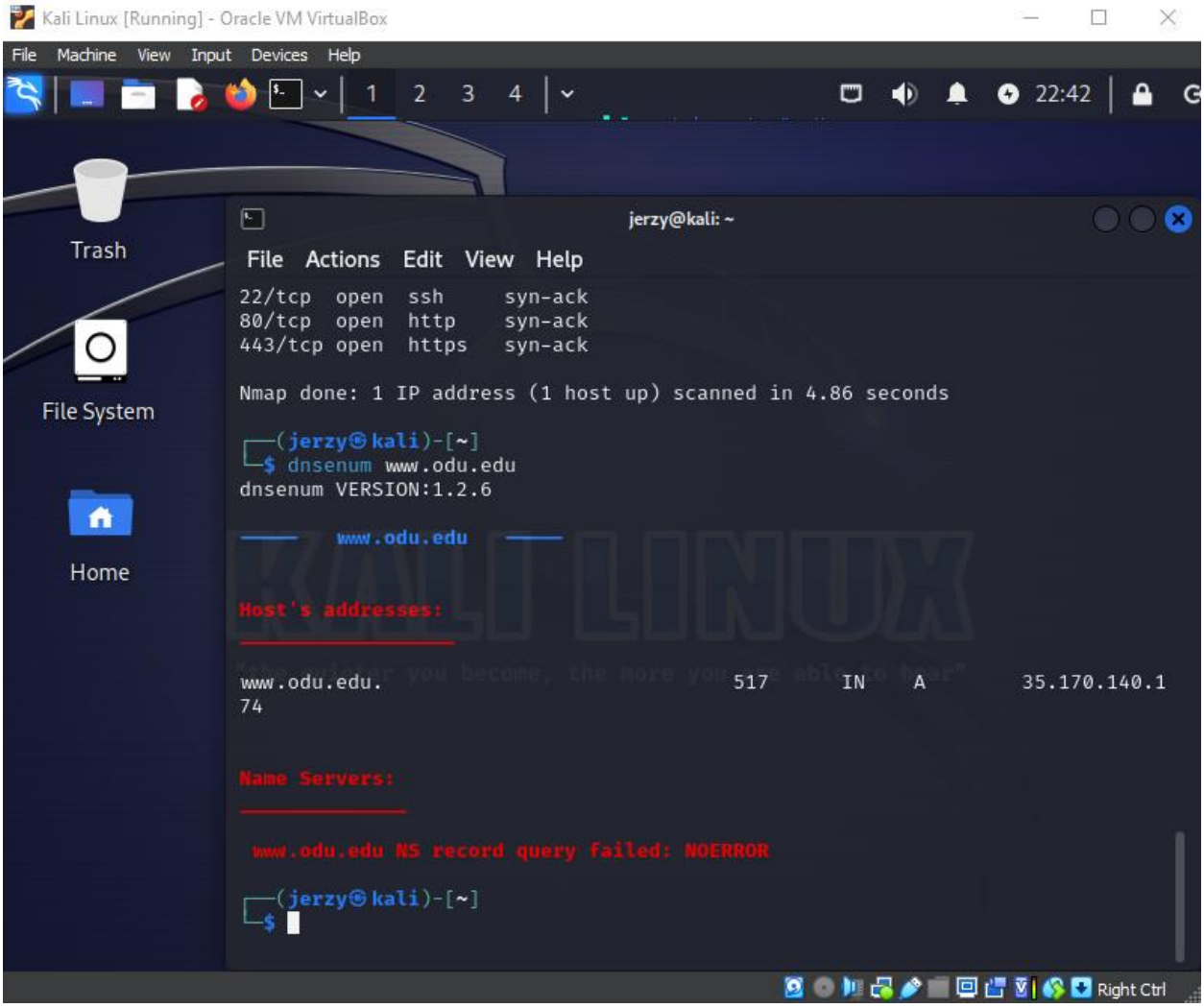



2. Here is the screenshot of me finding the IPs of each machine. Kali is 192.168.0.162, metasploitable is 192.168.0.173, and XP is 192.168.0.139.

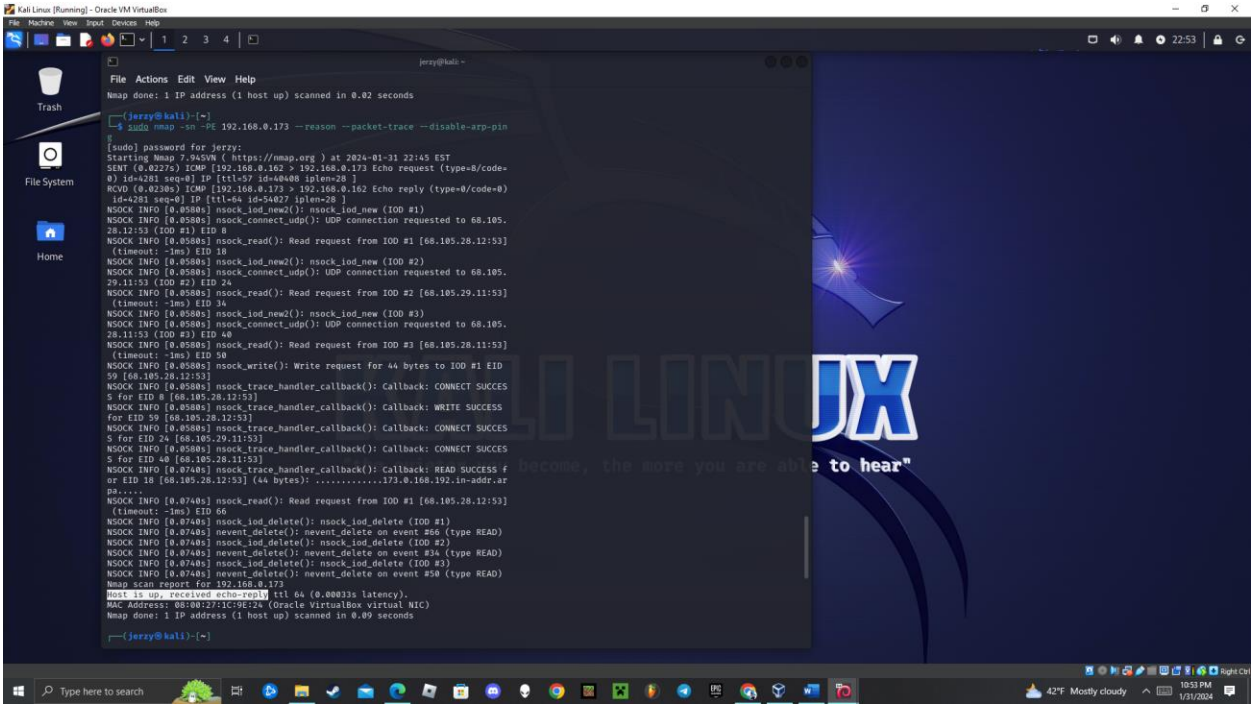



3. Here is me using the dig command to verify that www.odu.edu is up. I wasn't able to use the –reason option with dig specifically, but the powerpoint you made used it with nmap so im going to assume that is what you want for the second half of this question.

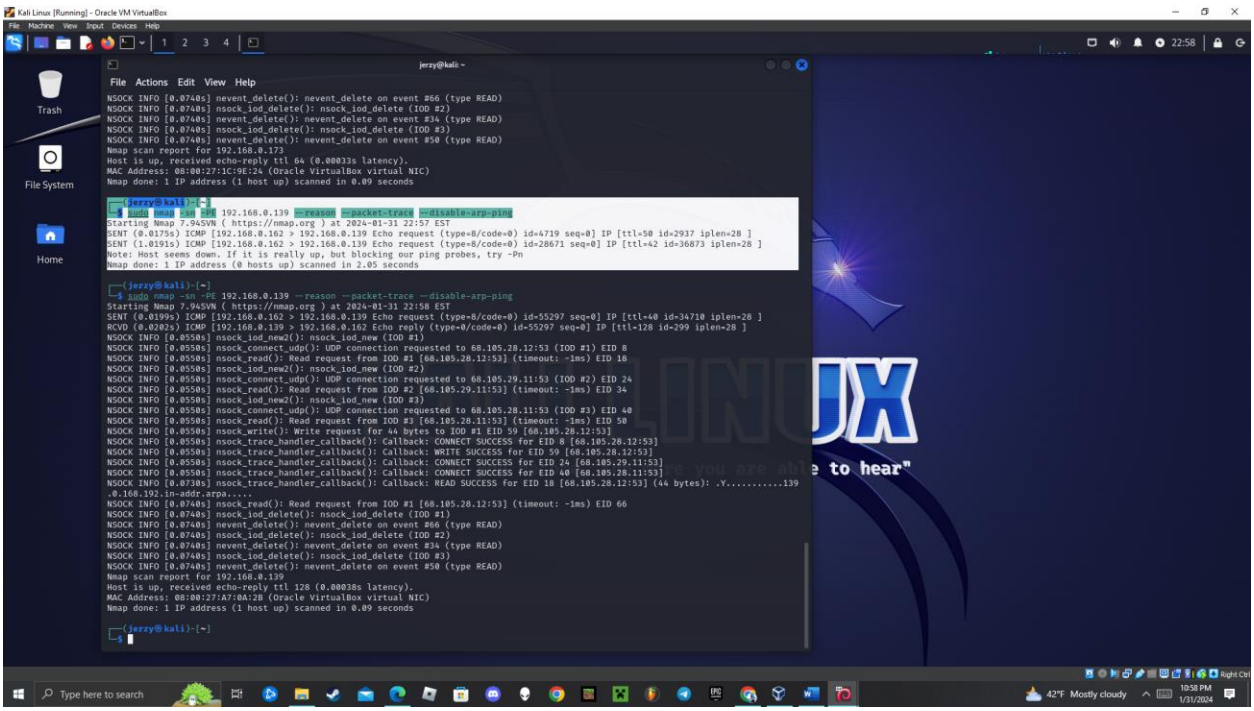





4. Here is use dnsenum to perform DNS enumeration




5. Here I used nmap to ICMP sweep the metasploitable machine. I had to use sudo because without it, my kali was defaulting to a tcp scan.




6. Here I ICMP sweep the windows xp machine. The highlighted portion is with the windows xp firewall on and the portion below is without the firewall on (I wanted to see if it made a difference and it did)