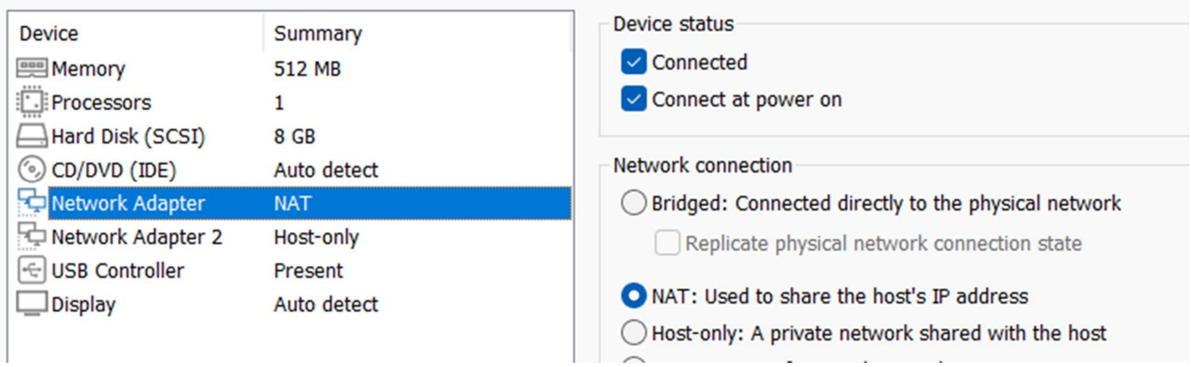
Midterm At-home section (Total point: 30 points)

(In screenshot, you need to show YOUR NAME next to the host clock to get the full point)

For the midterm lab portion, you will use YOUR **Kali**, **Windows XP**, and **Ubuntu** VMware installation in your computer. Check out if they are all in the same NAT network setting in your VMware.



Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Network Adapter 2	Host-only
USB Controller	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

● NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

If you want to download Windows XP for this section, use this Google Drive link (https://drive.google.com/drive/u/0/folders/1iJ-773pEs3FRhnjbwDFWyxUmUBvRmPKz). Please use UCMO ID to access this folder.

*After Windows XP installation, sometimes the firewall is ON. In this case, go to “Control Panel” -> “Windows Firewall” -> turn it off

You need to complete the following tasks. Please provide screenshot for each task to **highlight the commands you use and the results you obtain with red box**. **Brief explanations on what you have done and what you have observed for each task are required for the report**.

0. **(2 point)** To begin this task, check out the IP addresses of each machine and provide them like this example, and they should be in the same subnet to get a point.

- Kali’s IP address: 192.168.84.160
- Windows XP’s IP address: 192.168.84.164
- Ubuntu’s IP address: 192.168.84.162

1. **(3 points)** Run a port scan on Windows XP and report **ALL** open ports

2. **(5 points)** With the port information gathered from task 1, conduct the research on vulnerabilities and

identify a Metasploit module to exploit the Windows XP machine (**you cannot use the admin credential georgia: password, secret: Password123 for this task**). Our goal for this task is to have a **Meterpreter shell** on Windows XP so that we can perform other remaining tasks.

Put the Meterpreter session in background after you finish this task by applying the right option. **Don't kill the meterpreter shell until the end of this report.**

a) Find vulnerabilities and briefly explain the vulnerability you'll use to exploit the system (3 points)

b) Identify the MSF module you want to use (1 points)

c) Show 'pwd' & 'sysinfo' result screen from the meterpreter shell you opened (1 points)

3. **(3 points)** Do screenshot of Windows XP using the Meterpreter shell from task 2. Save the image file using your name (ex. danieltiger.jpg). Show the command and screenshot.

4. **(3 points)** Conduct a ping sweep on your subnet from the Windows XP (you cannot login in Windows XP to perform the task). List all the hosts identified through the ping sweep
(Ubuntu's IP address needs to be in this host list)

5. **(3 points)** Without logging in Windows XP, create a folder '**more'** under the C drive on Windows XP. Upload the nc.exe from Kali's /usr/share/windows-binaries folder to the newly created **C:\more** folder. You need to show the nc.exe file exists in 'more' folder.

6. **(3 points)** Use the uploaded Netcat from task 5 to run a port scan on Ubuntu (You still cannot login in Windows XP to perform the task and need to open a new shell from Kali to do this). To save the time, limit the ports from 1 to 1000. Don't kill this session until the end of this report ad report all the open ports.

7. **(3 points)** Login in Ubuntu directly and use iptables firewall to block any incoming traffic from Kali. Ping Ubuntu from Kali to verify that the traffic is blocked.

8. **(3 points)** Now that you cannot directly access Ubuntu from Kali while Windows XP has the direct connection with the Ubuntu. Please use Windows XP as a pivot to connect to the FTP server on Ubuntu. On your Kali, please verify that you can successfully ftp to Ubuntu by issuing **ftp localhost port_of_your_choice**

(*if your connection to ftp is not working well, provide screenshots for every command and reasons why it didn't work)

9. **(2 points)** Show the sessions information from MSF which shows the meterpreter session from task 2 and shell session from task 6. You need to show that there are 2 sessions in MSF. Use "sessions -l" command to show this

Report

- please include your name and 700# at the beginning of your report.
- please upload your report to the Blackboard by the due date.
- You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed.
- Only word or pdf format is acceptable.
- you must show all the necessary commands associated with each task in order to receive credits.
- your screenshots size must be appropriate to provide the visible details.