

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

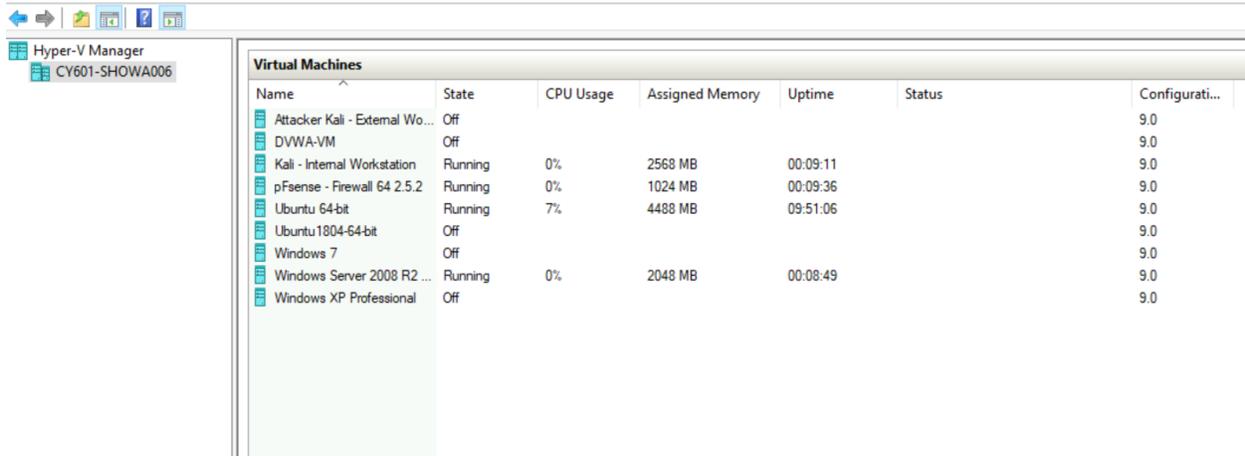
Assignment #1 Traffic Tracing and Analysis

Stuart N. Howard

01241576

Task A. Get ready with VMs

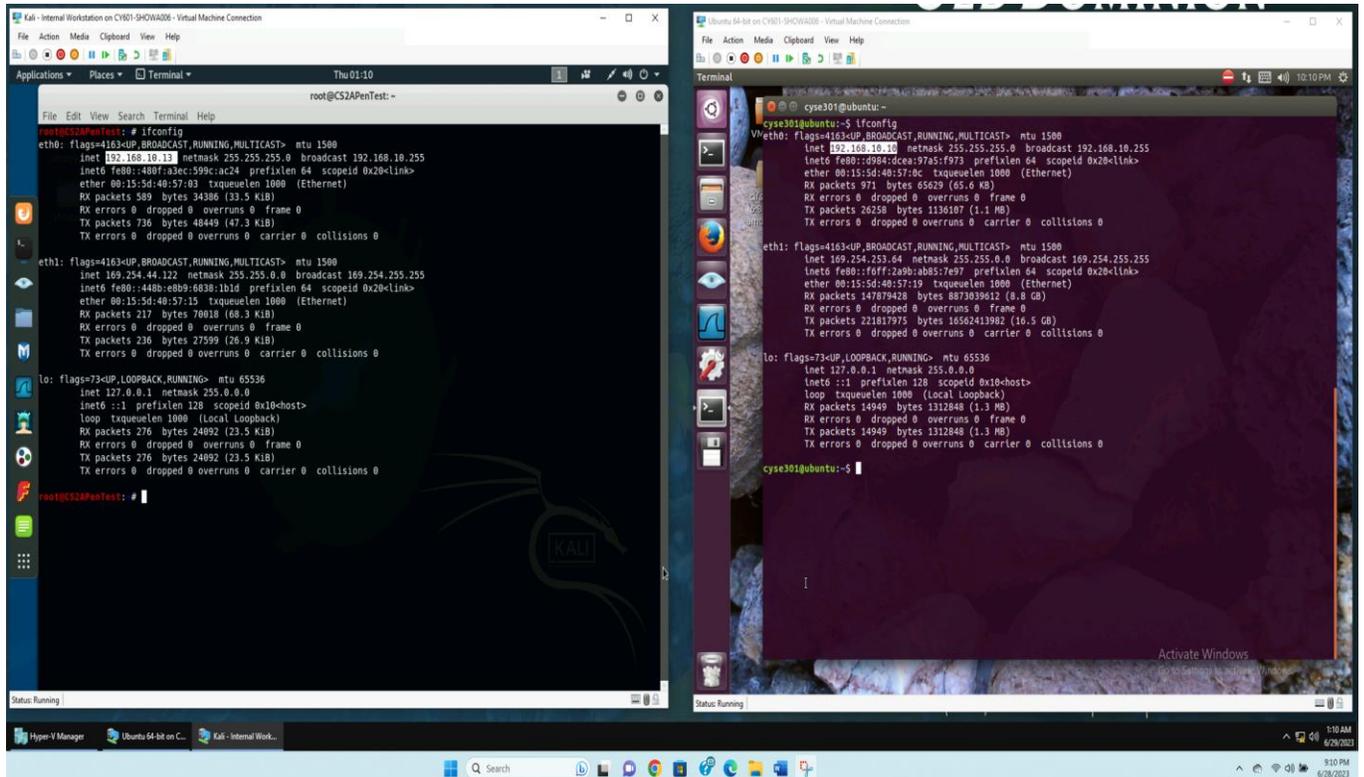
1. Power on the following VMs



Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
Attacker Kali - External Wo...	Off					9.0
DVWA-VM	Off					9.0
Kali - Internal Workstation	Running	0%	2568 MB	00:09:11		9.0
pFense - Firewall 64 2.5.2	Running	0%	1024 MB	00:09:36		9.0
Ubuntu 64-bit	Running	7%	4488 MB	09:51:06		9.0
Ubuntu1804-64-bit	Off					9.0
Windows 7	Off					9.0
Windows Server 2008 R2 ...	Running	0%	2048 MB	00:08:49		9.0
Windows XP Professional	Off					9.0

2. Find the IP address of the following VMs by using command:

Entered "ifconfig" in the terminal window of Ubuntu and Kali



```
root@CS2APenTest:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.10.13  netmask 255.255.255.0  broadcast 192.168.10.255
    inet6 fe80::480f:a3ec:599c:ac24  prefixlen 64  scopeid 0x20<link>
    ether 08:15:5d:48:57:03  txqueuelen 1000  (Ethernet)
    RX packets 489  bytes 34386 (33.5 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 736  bytes 48449 (47.3 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 169.254.44.122  netmask 255.255.0.0  broadcast 169.254.255.255
    inet6 fe80::448b:e8b9:6838:1bd1  prefixlen 64  scopeid 0x20<link>
    ether 08:15:5d:48:57:15  txqueuelen 1000  (Ethernet)
    RX packets 217  bytes 70818 (68.3 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 236  bytes 27599 (26.9 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 276  bytes 24092 (23.5 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 276  bytes 24092 (23.5 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

root@CS2APenTest:~#
```

```
cyse301@ubuntu:~$ ifconfig
vetho: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.10.10  netmask 255.255.255.0  broadcast 192.168.10.255
    inet6 fe80::6984:dcea:97a5:f973  prefixlen 64  scopeid 0x20<link>
    ether 08:15:5d:48:57:0c  txqueuelen 1000  (Ethernet)
    RX packets 971  bytes 65629 (65.6 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 26258  bytes 1136107 (1.1 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 169.254.253.64  netmask 255.255.0.0  broadcast 169.254.255.255
    inet6 fe80::f0ff:2a9b:ab85:7e97  prefixlen 64  scopeid 0x20<link>
    ether 08:15:5d:48:57:19  txqueuelen 1000  (Ethernet)
    RX packets 147879428  bytes 8873839612 (8.8 GiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 221817975  bytes 16562413982 (16.5 GiB)
    TX errors 0  dropped 0  overruns 0  carrier 0
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

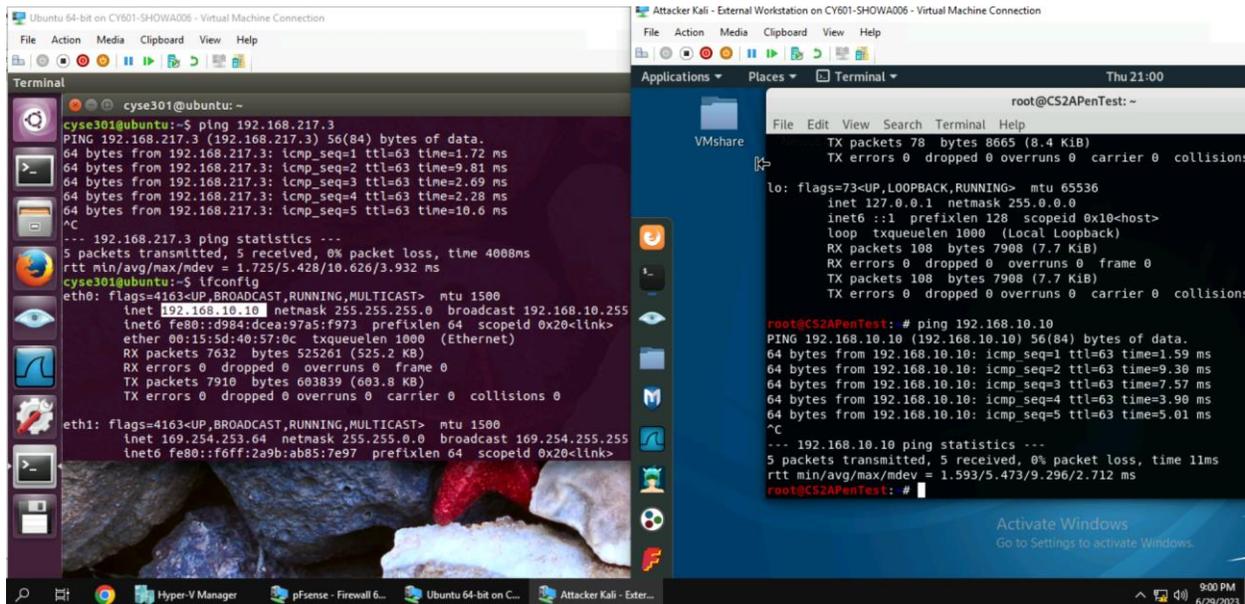
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 14949  bytes 1312848 (1.3 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 14949  bytes 1312848 (1.3 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

cyse301@ubuntu:~$
```

3. Verify the connection between Kali Linux VM and Ubuntu VM using the ping command.

Once the IP address was located above.

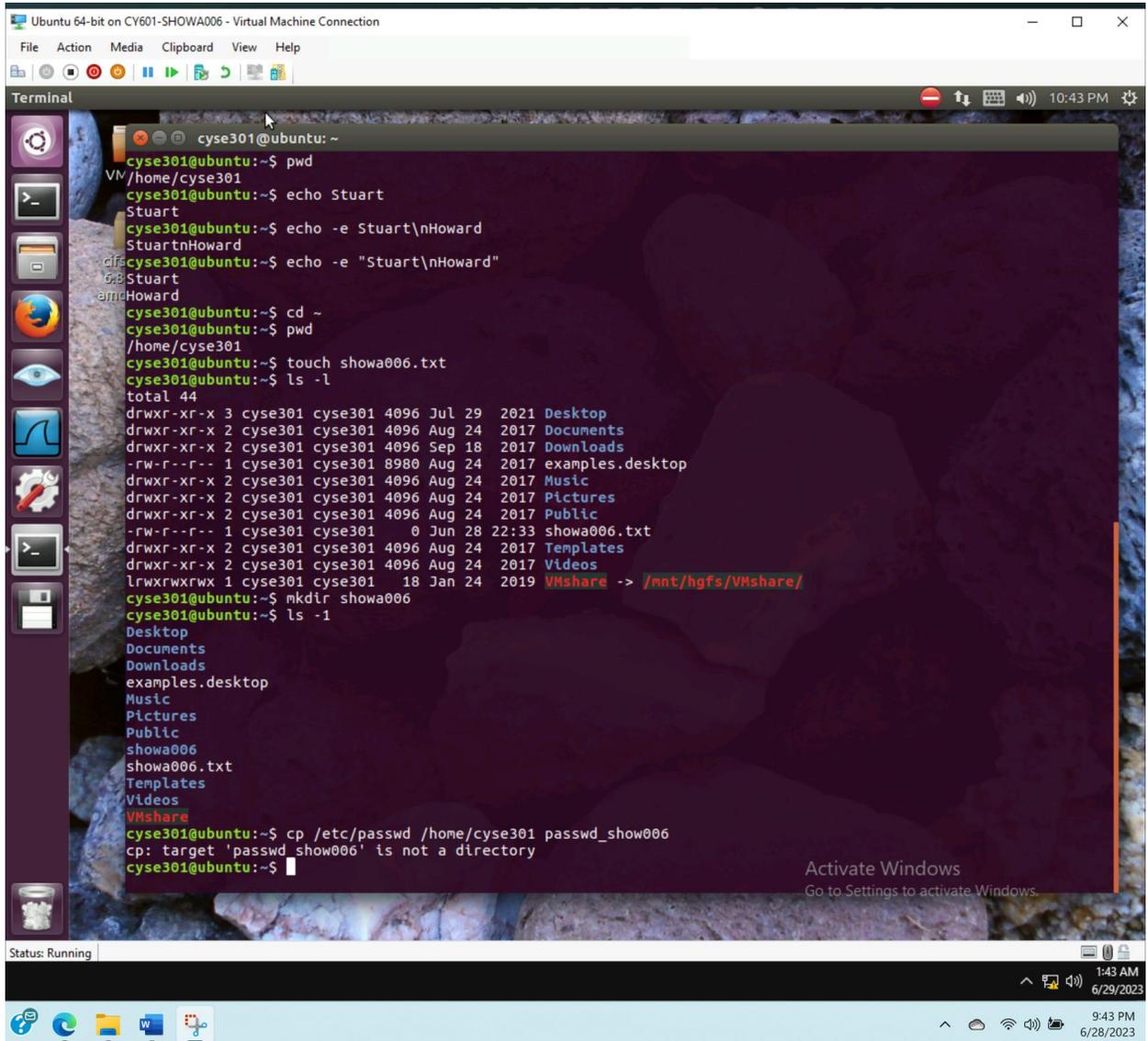
Entered “ping” command and the IP address for Ubuntu into Kali terminal and Kali IP address into Ubuntu terminal.



Task B: Practice with Linux Commands (Complete the following tasks in the Ubuntu VM)

- Display your current directory in a terminal.**
 - Entered print working directory command “PWD”
- Use the **echo** command to print your name to the console.**
 - Entered command “echo” and my name
- Display your first and last names in two separate lines using a **single echo command****
 - Entered command echo -e “first name\nlastname”
- Execute the command to return to your **home** directory.**
 - Entered the change directory command “cd” and the “~”
- Create a new file named “forXXXX.txt” in your **home** directory (replace “XXXX” with your own MIDAS).**
 - To create a new file I entered the “touch” command and created the file with my midas ID.txt
 - Then enter the long display command “ls -l” to display the content in the home directory files
- Create a new directory named “XXXX” in your home directory (replace “XXXX” with your own MIDAS). Then, use the long listing format to display the contents in your home directory. What is the size of the file you just created?**

- In the home directory, I entered the command to make a new directory, “mkdir” and Then enter the long display command “ls -l” to display the content in the home directory files



7. Copy /etc/passwd file to your home directory and rename the file to “passwd_XXXX” (replace “XXXX” with your own MIDAS). Then, complete the following two subtasks:

- Use the proper command to display the first six lines in this file.
- Search keyword “www” in this file.

- Ran the command to copy “cp” the file, use the “~” for the location and renamed the file
- To display the first six lines of the file, I use the ”head” command with the -n6 option.
- To search for the keyword "www" in the file, I used the “grep” command with “www” and the directory name I wanted to search .

