OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

Peter MacMillan

01073897

In this task, you will be acting as an ATTACKER who sniffs the internal communications between peers by using either Wireshark or tShark on Ubuntu VM.

You need to use the following VMs to complete the assignment:

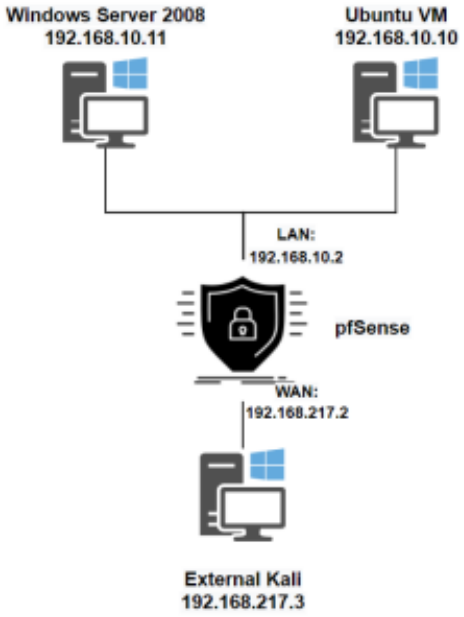


Figure 1 Required VMs for this assignment

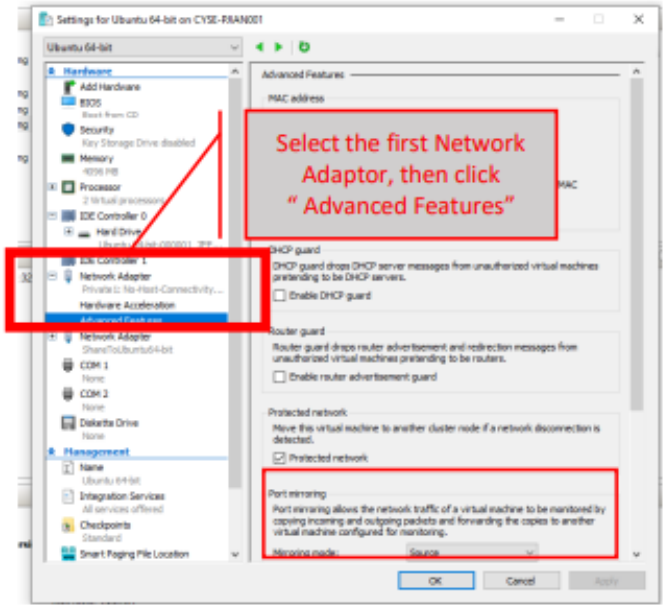


Figure 2 How to configure port mirroring in Hyper-V

IMPORTANT! Due to the different networking configurations in Hyper-V, you need to ***Enable Port Mirroring*** for related VMS accordingly (This is a helpful link to follow)

You need to put the sniffer (Ubuntu VM) as the **mirroring Destination**, and the target VMS are the **mirroring Source**

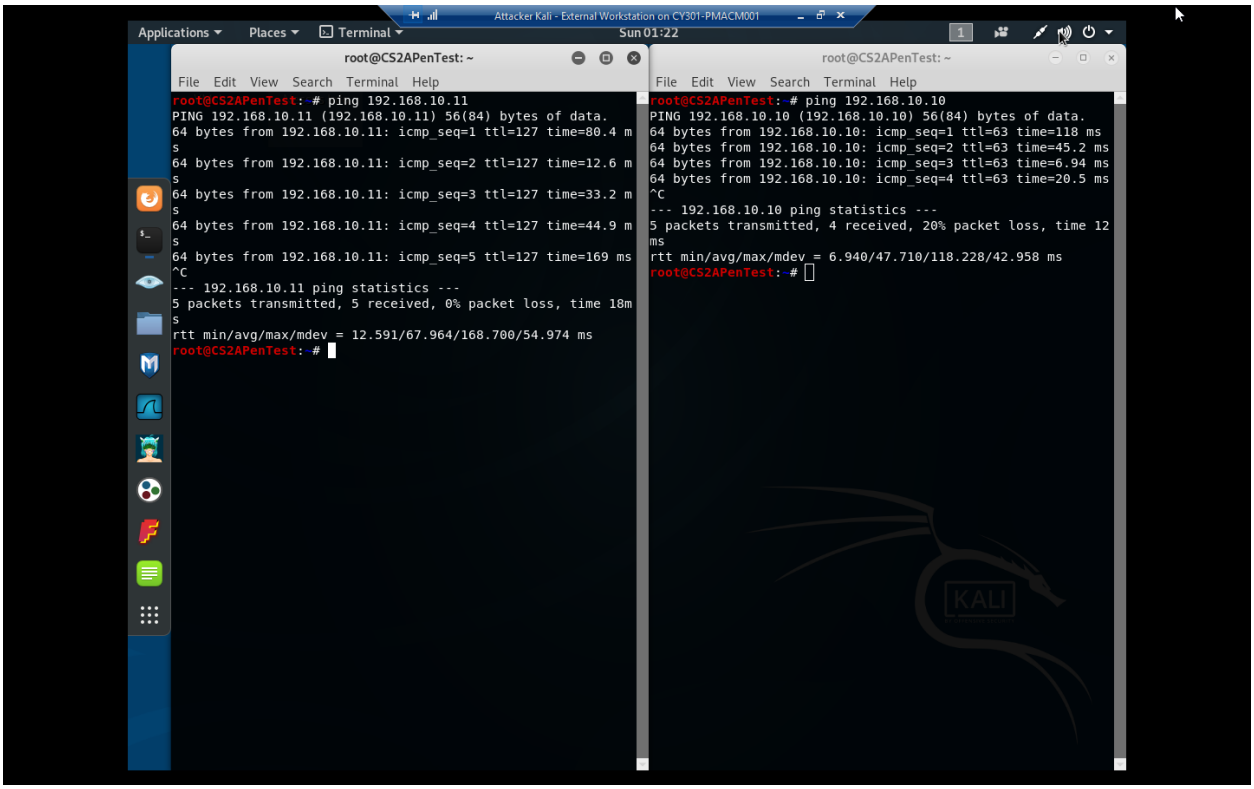
To be specific:

- **Ubuntu VM**: Set Mirroring mode to "**Destination**" in the "Port Mirroring"
- **Windows Server 2008**: Set mirroring mode to "**Source**" in the "Port Mirroring"
- **External Kali**: Set Mirroring mode to "**Source**" in the "Port Mirroring"

TASK A: SNIFF LAN TRAFFIC

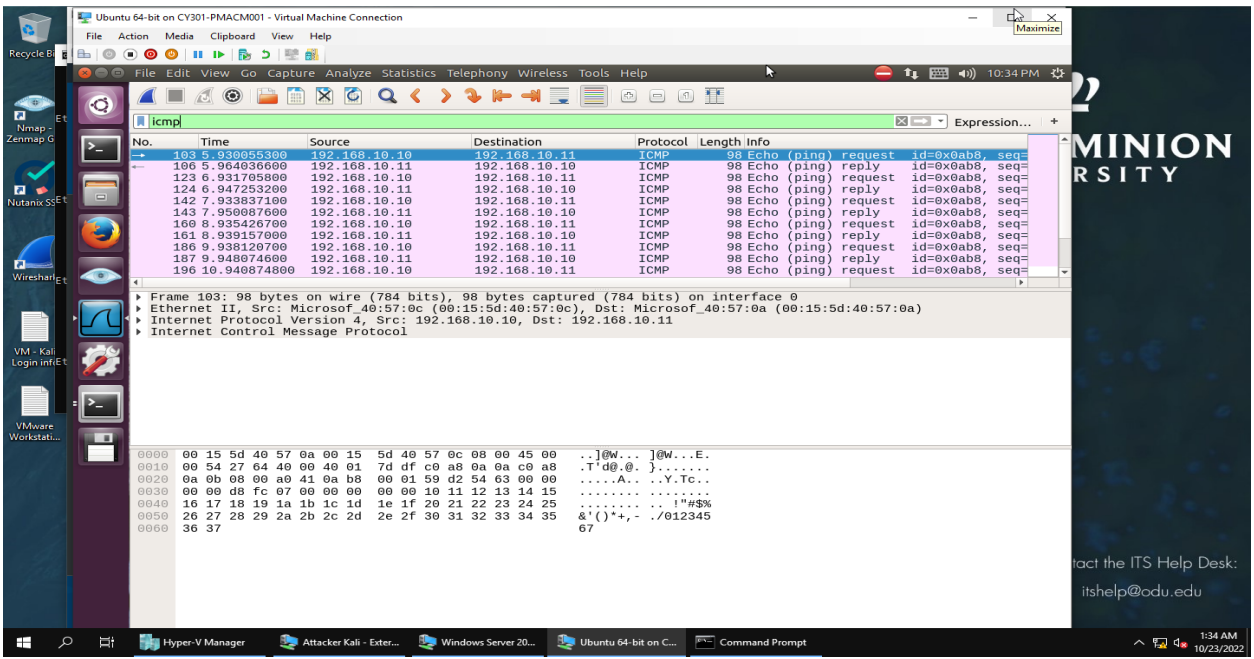
1. Sniff ICMP Traffic

a. In External Kali VM, ping Windows Server 2008 and Ubuntu VM from two separate terminals

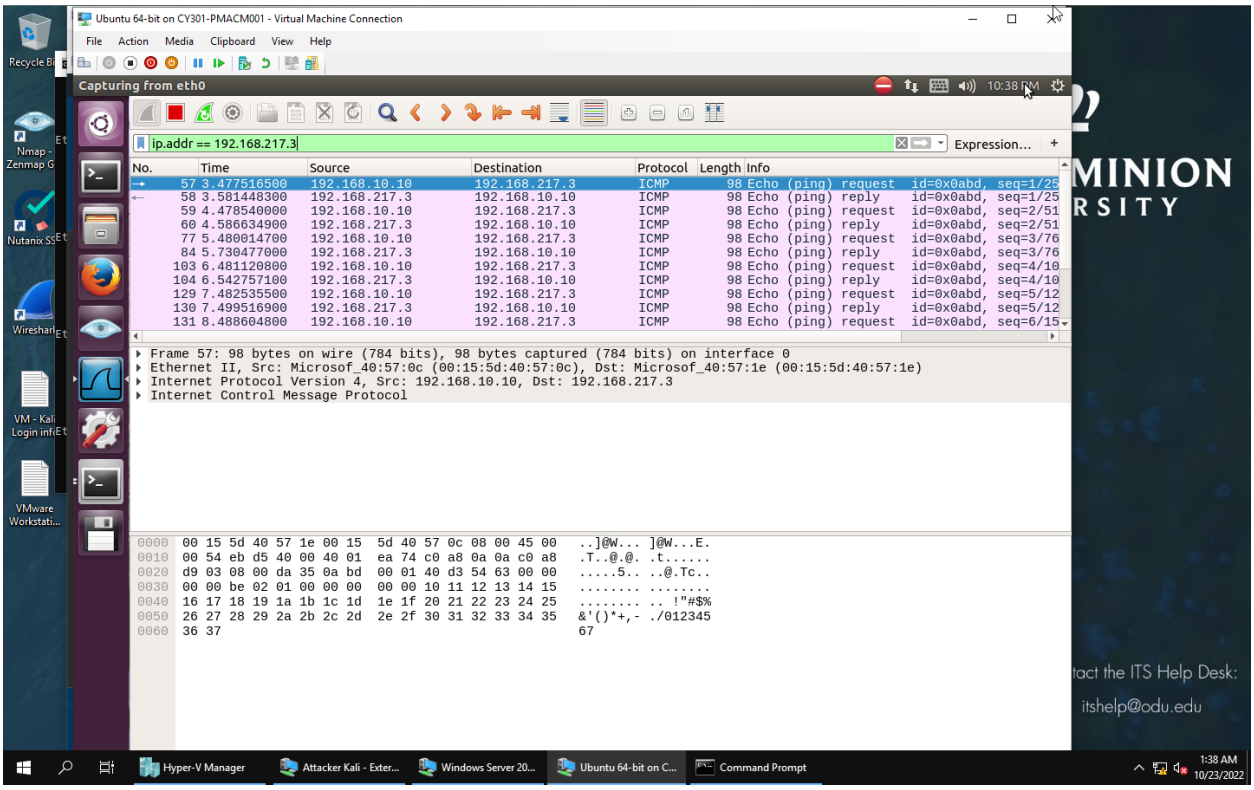


Used ping command, followed by Ubuntu and Windows Server's IP to verify connection with them

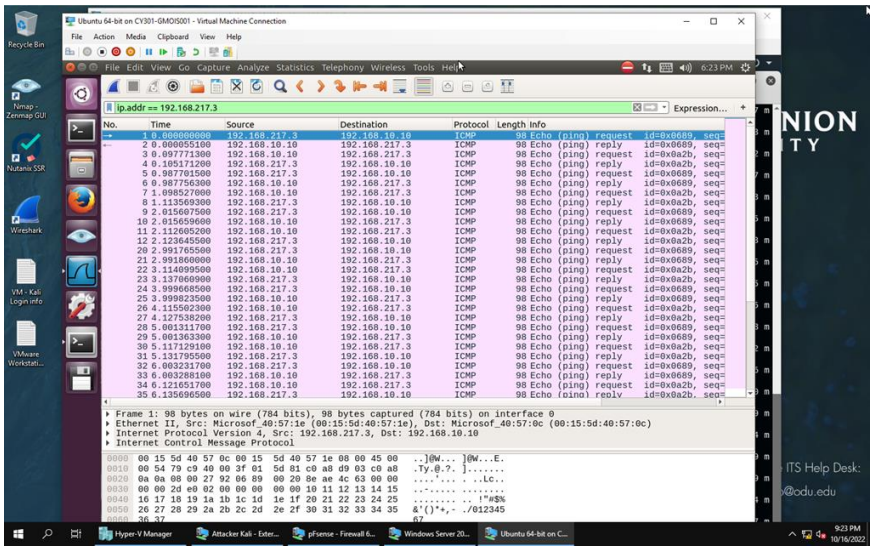
b. Apply proper display or capture filter on Ubuntu VM to show all ping traffic.



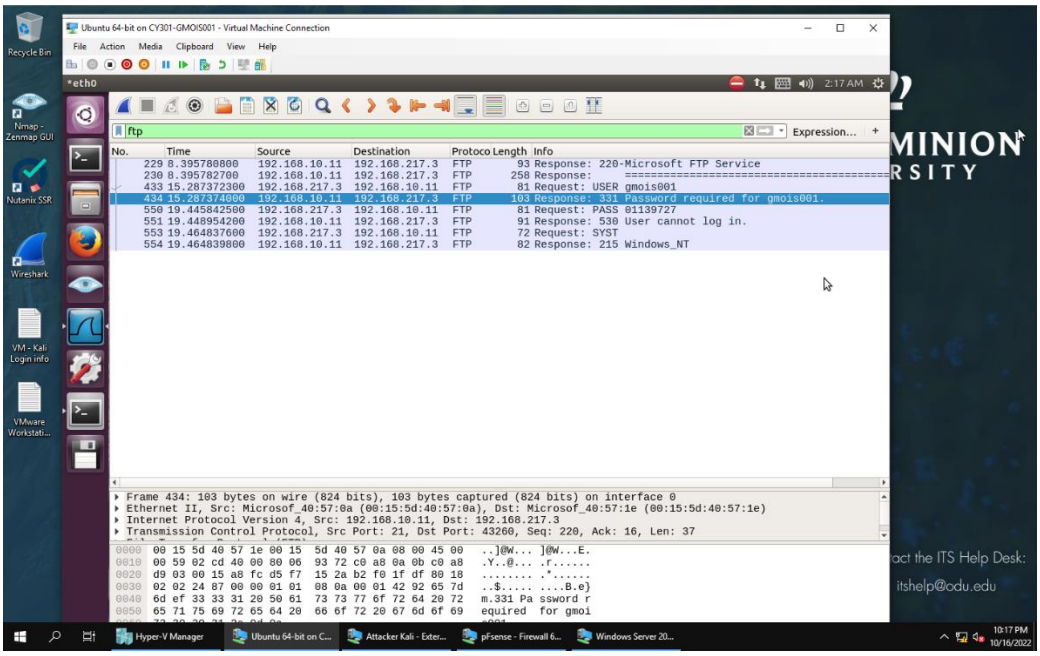
c. Apply proper display or capture filter on Ubuntu VM that ONLY displays ICMP request originated from external Kali VM and goes to Windows Server 2008.



2. Sniff FTP Traffic



To capture the username and password to log into Windows' FTP via Kali Linux, I pinged Windows and Ubuntu while logging into FTP via Kali Linux. Then, while capturing via Wireshark, I applied the FTP display filter to only show FTP results.


Ubuntu 64-bit on CY301-GMOIS001 - Virtual Machine Connection
File Action Media Clipboard View Help
*eth0
2:17 AM
ftp
Expression...
No. Time Source Destination Protoco Length Info
229 8.395780800 192.168.10.11 192.168.217.3 FTP 93 Response: 220-Microsoft FTP Service
230 8.395782700 192.168.10.11 192.168.217.3 FTP 258 Response: ==========
433 15.287372300 192.168.217.3 192.168.10.11 FTP 81 Request: USER gmois001
434 15.287374000 192.168.10.11 192.168.217.3 FTP 103 Response: 331 Password required for gmois001.
550 19.445842500 192.168.217.3 192.168.10.11 FTP 81 Request: PASS 01139727
551 19.448954200 192.168.10.11 192.168.217.3 FTP 91 Response: 530 User cannot log in.
553 19.464837600 192.168.217.3 192.168.10.11 FTP 72 Request: SYST
554 19.464839800 192.168.10.11 192.168.217.3 FTP 82 Response: 215 Windows_NT
Frame 434: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
Ethernet II, Src: Microsof_40:57:0a (00:15:5d:40:57:0a), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e)
Internet Protocol Version 4, Src: 192.168.10.11, Dst: 192.168.217.3
Transmission Control Protocol, Src Port: 21, Dst Port: 43260, Seq: 220, Ack: 16, Len: 37
0000 00 15 5d 40 57 1e 00 15 5d 40 57 0a 08 00 45 00 ..]@W...]@W...E.
0010 00 59 02 cd 40 00 80 06 93 72 c0 a8 0a 0b c0 a8 .Y..@... .r......
0020 d9 03 00 15 a8 fc d5 f7 15 2a b2 f0 1f df 80 18 ....*......
0030 02 02 24 87 00 00 01 01 08 0a 00 01 42 92 65 7d ..$..... ....B.e}
0040 6d ef 33 33 31 20 50 61 73 73 77 6f 72 64 20 72 m.331 Pa ssword r
0050 65 71 75 69 72 65 64 20 66 6f 72 20 67 6d 6f 69 equired for gmoi
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
Hyper-V Manager
Ubuntu 64-bit on C...
Attacker Kali - Exter...
pFsense - Firewall 6...
Windows Server 20...
10:17 PM
10/16/2022
MINION
RSITY
act the ITS Help Desk:
itshelp@odu.edu