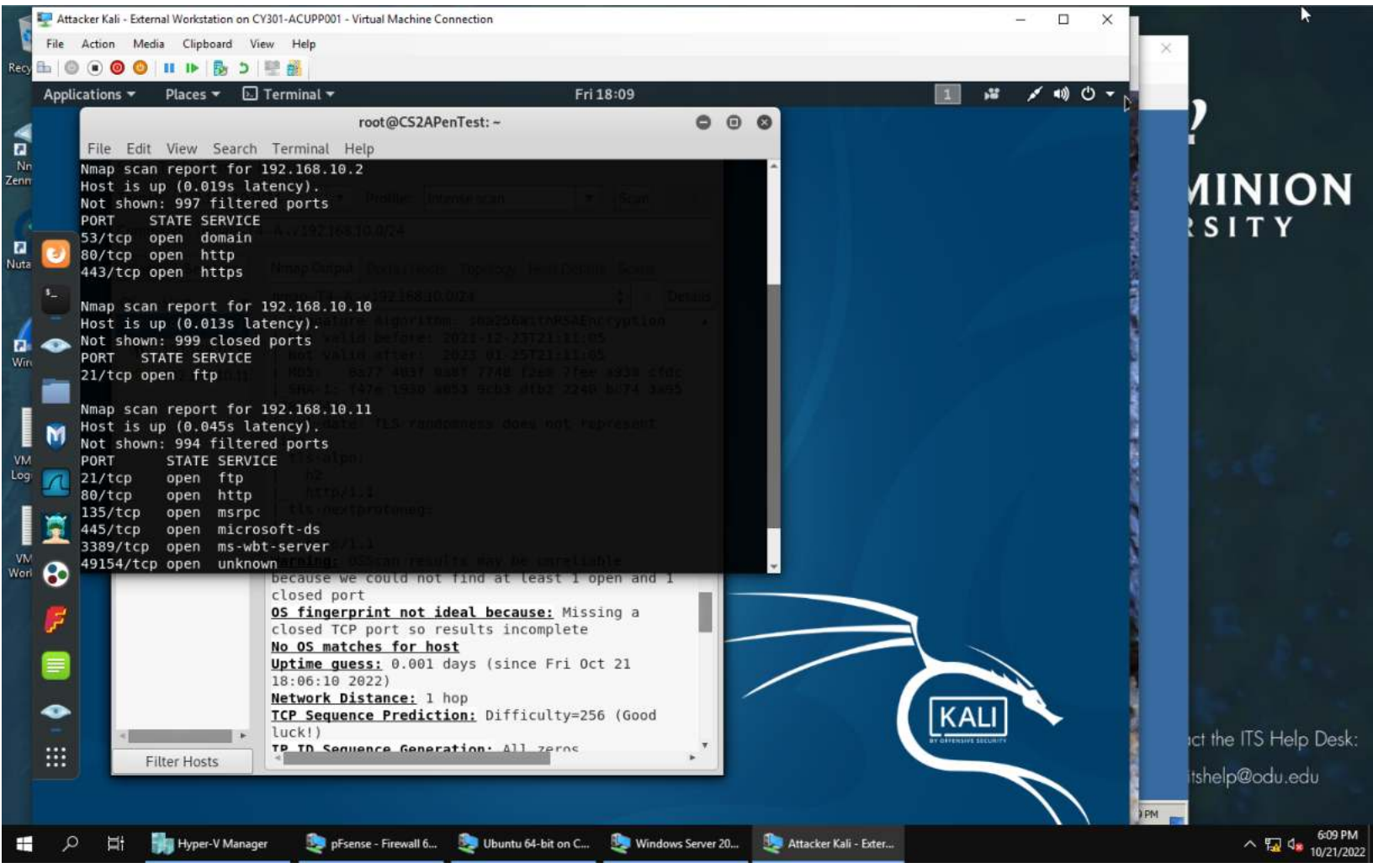
OLD DOMINION

CYSE301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #3 – Sword vs Shield

AUSTIN CUPP

01183567

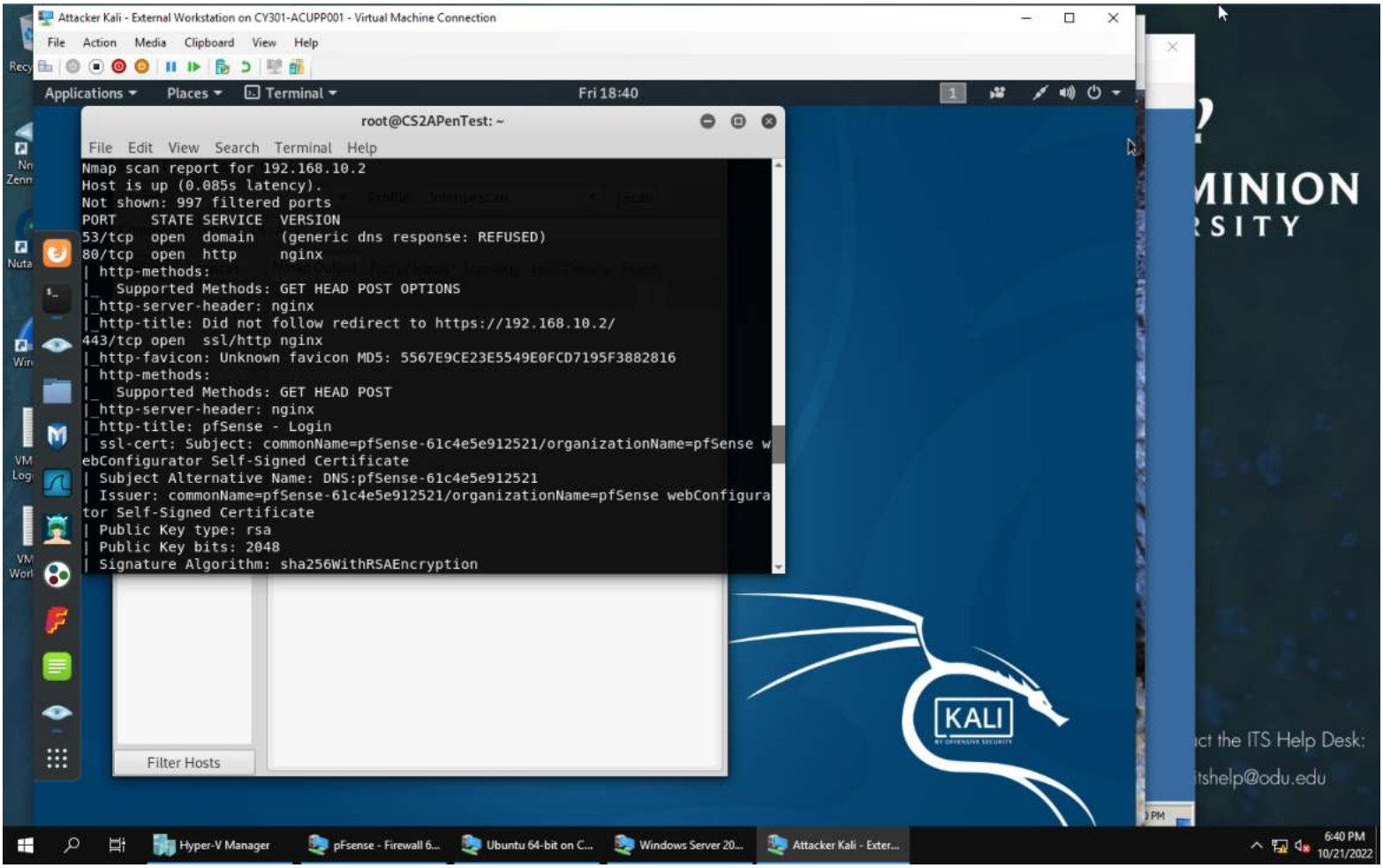


A1. A simple scan is ran to show the ports, with the OS being provided below instead of screenshot. I entered the command nmap -O 192.168.10.0/24 to get the operating systems and found as follows.

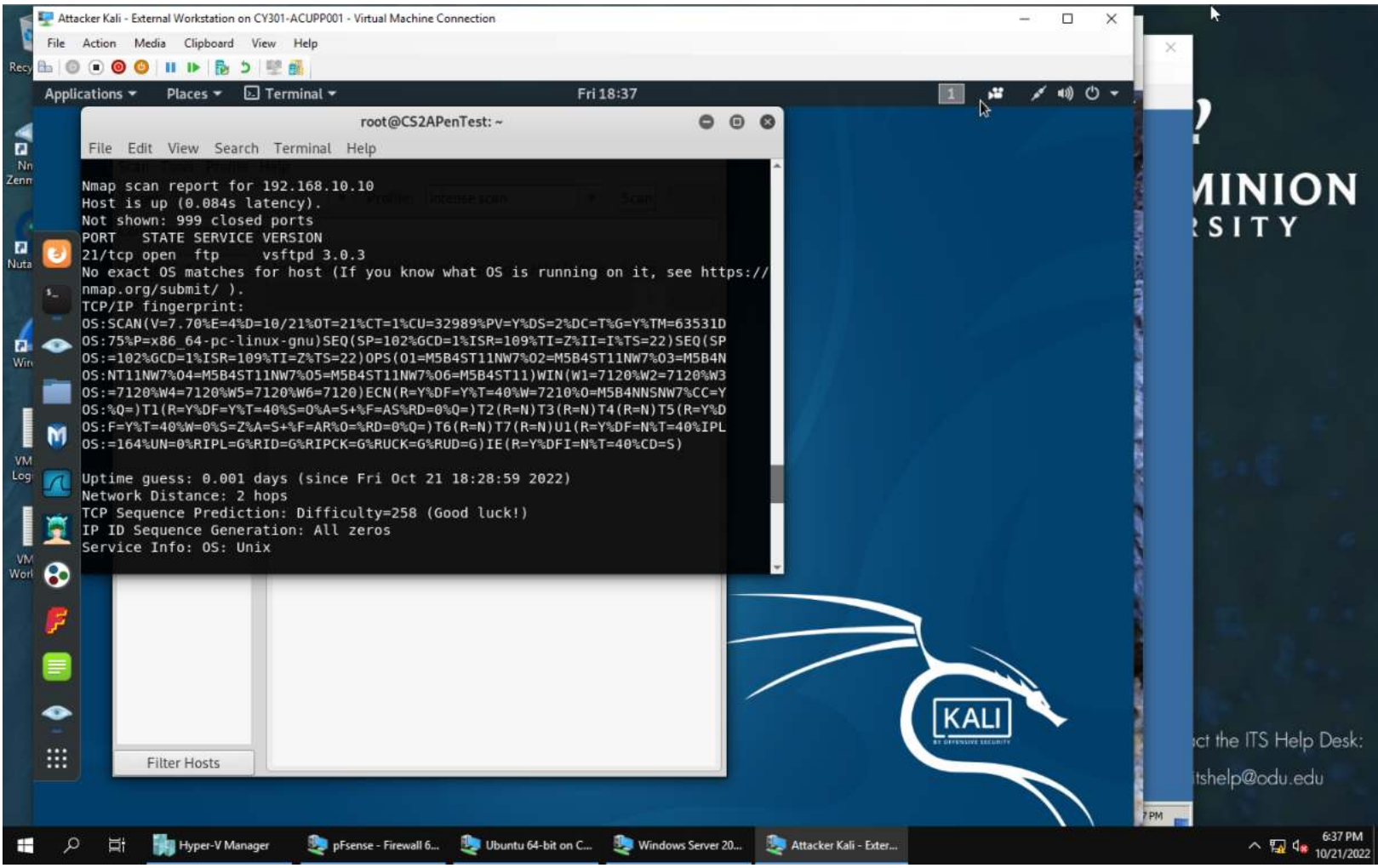
192.168.10.2: N/A

192.168.10.10: No exact OS matches

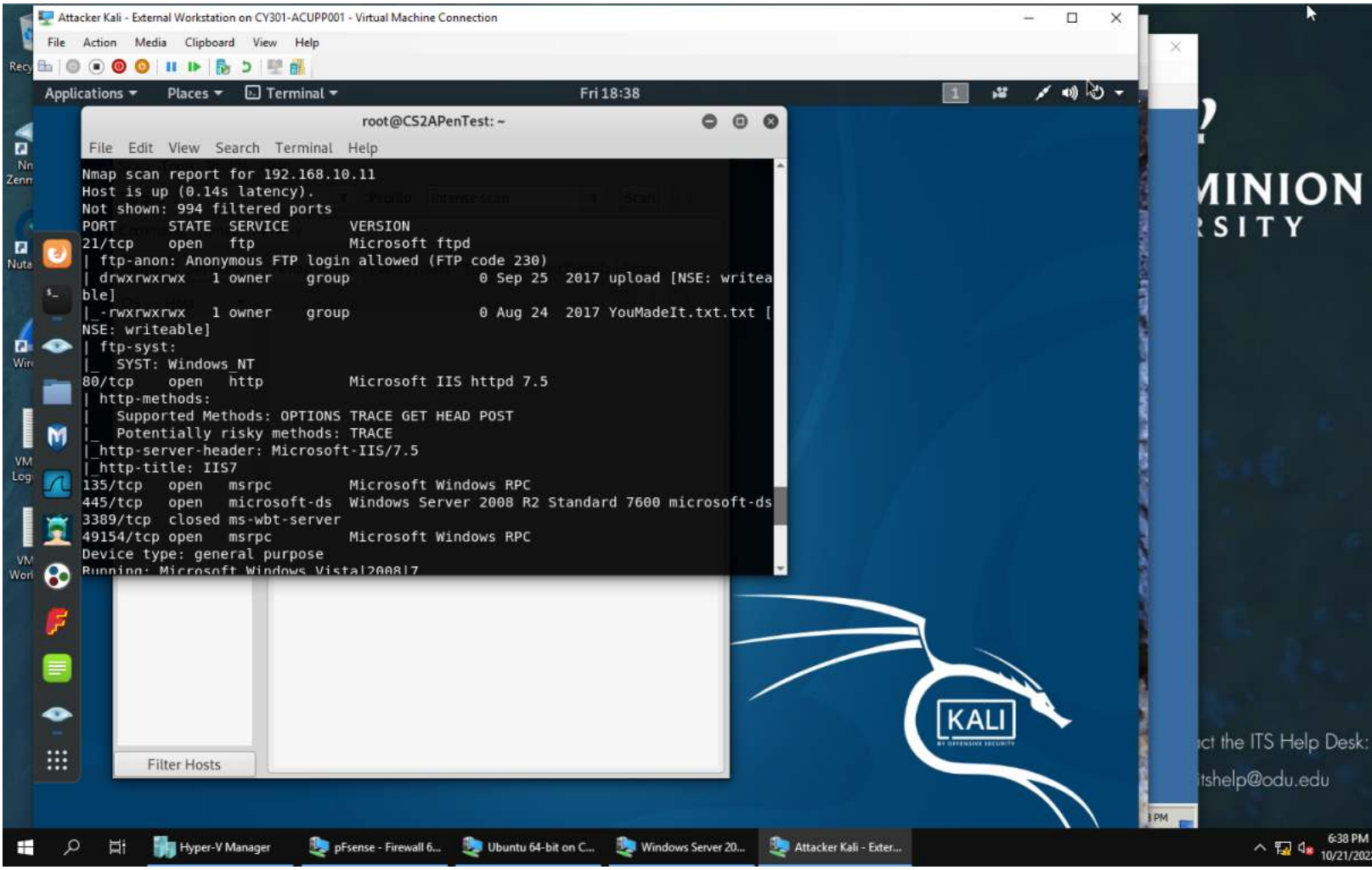
192.168.10.11: Microsoft Windows 7|8|Vista|2008



A2. Intense Scan for 192.168.10.2

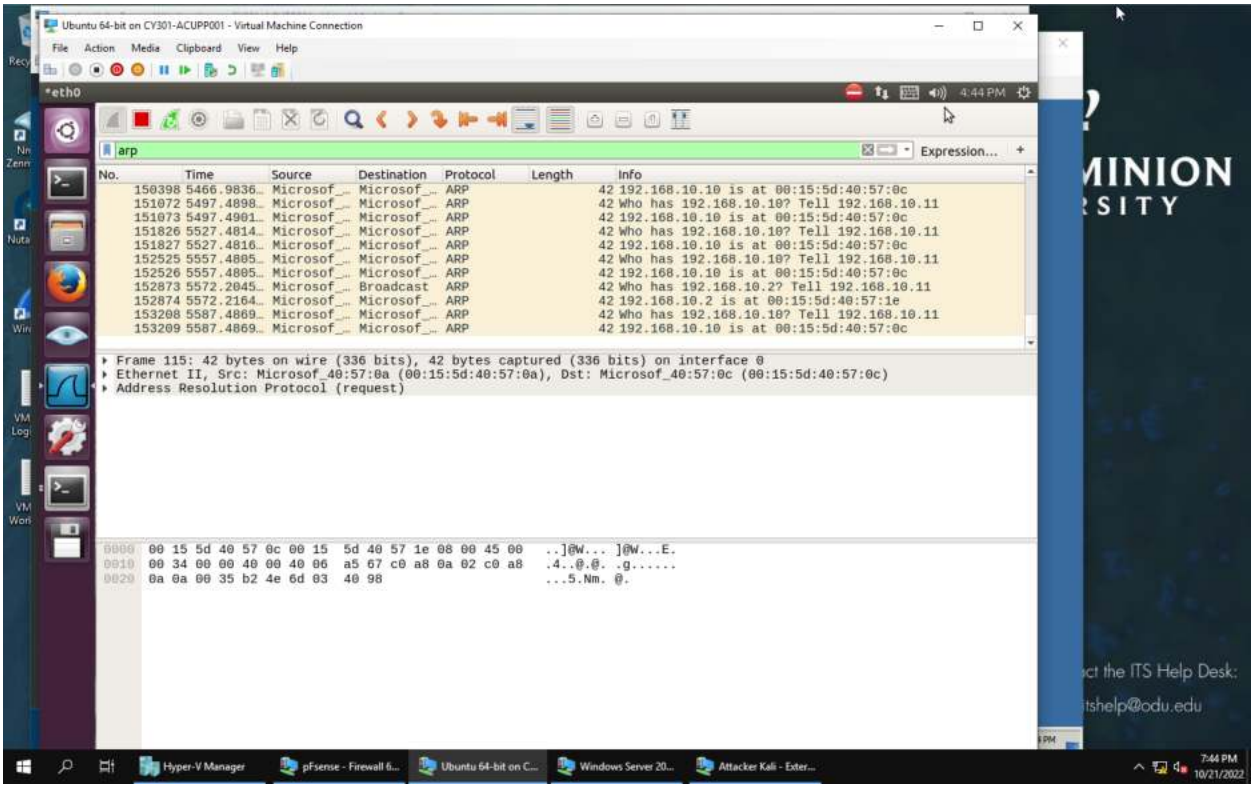


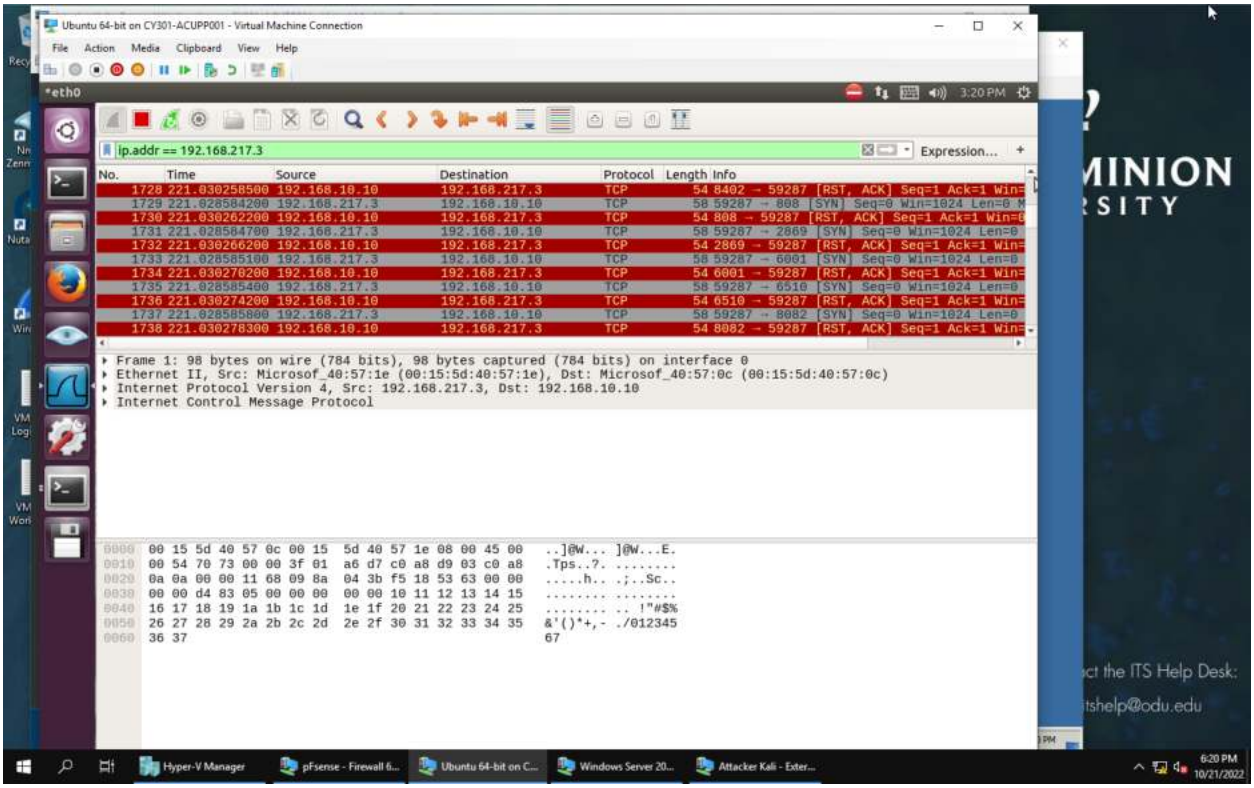
A2. Intense scan for 192.168.10.10



A2. Intense scan 192.168.10.11

A3. OBSERVED TRAFFIC PATTERN WITH ESSAY

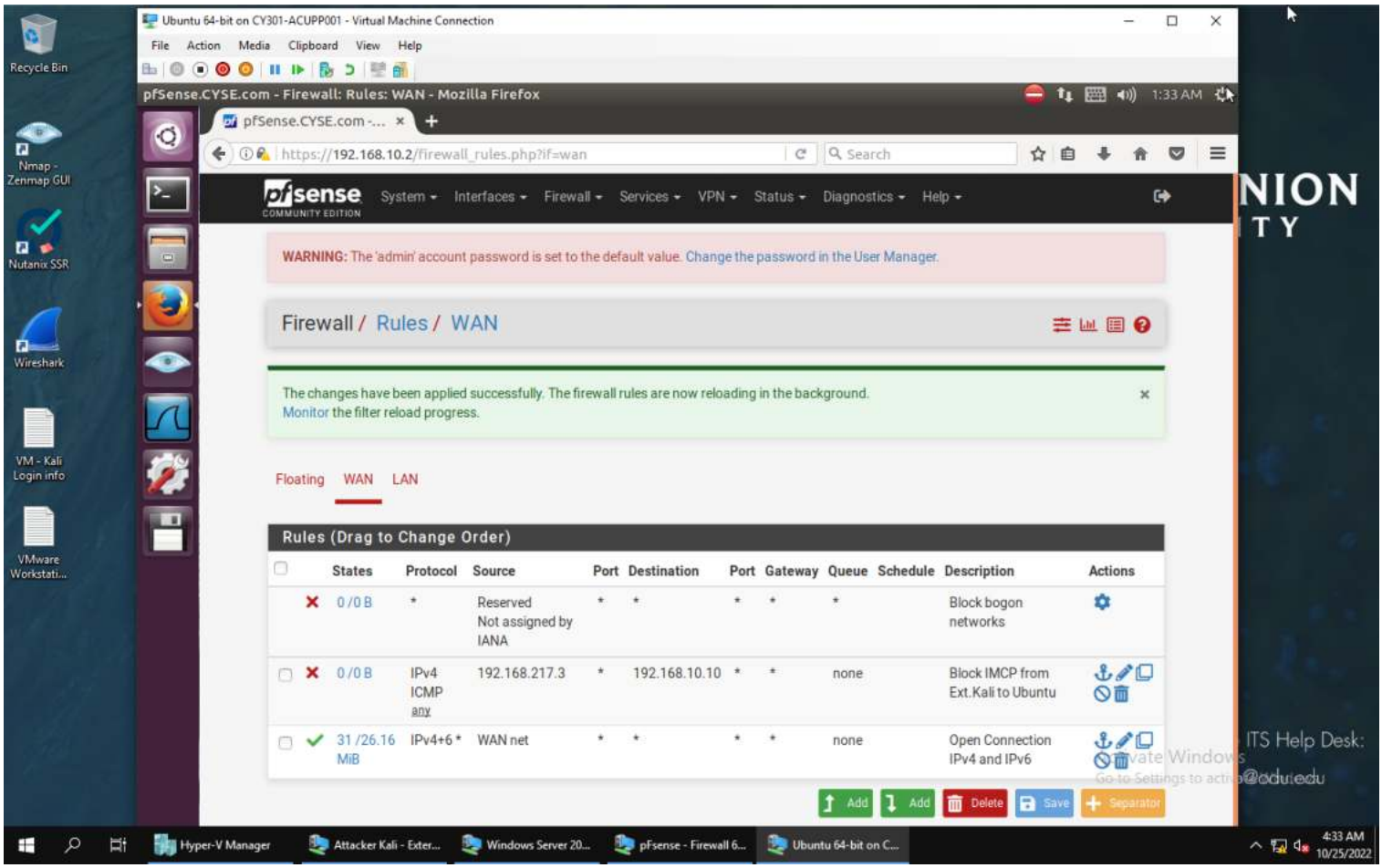




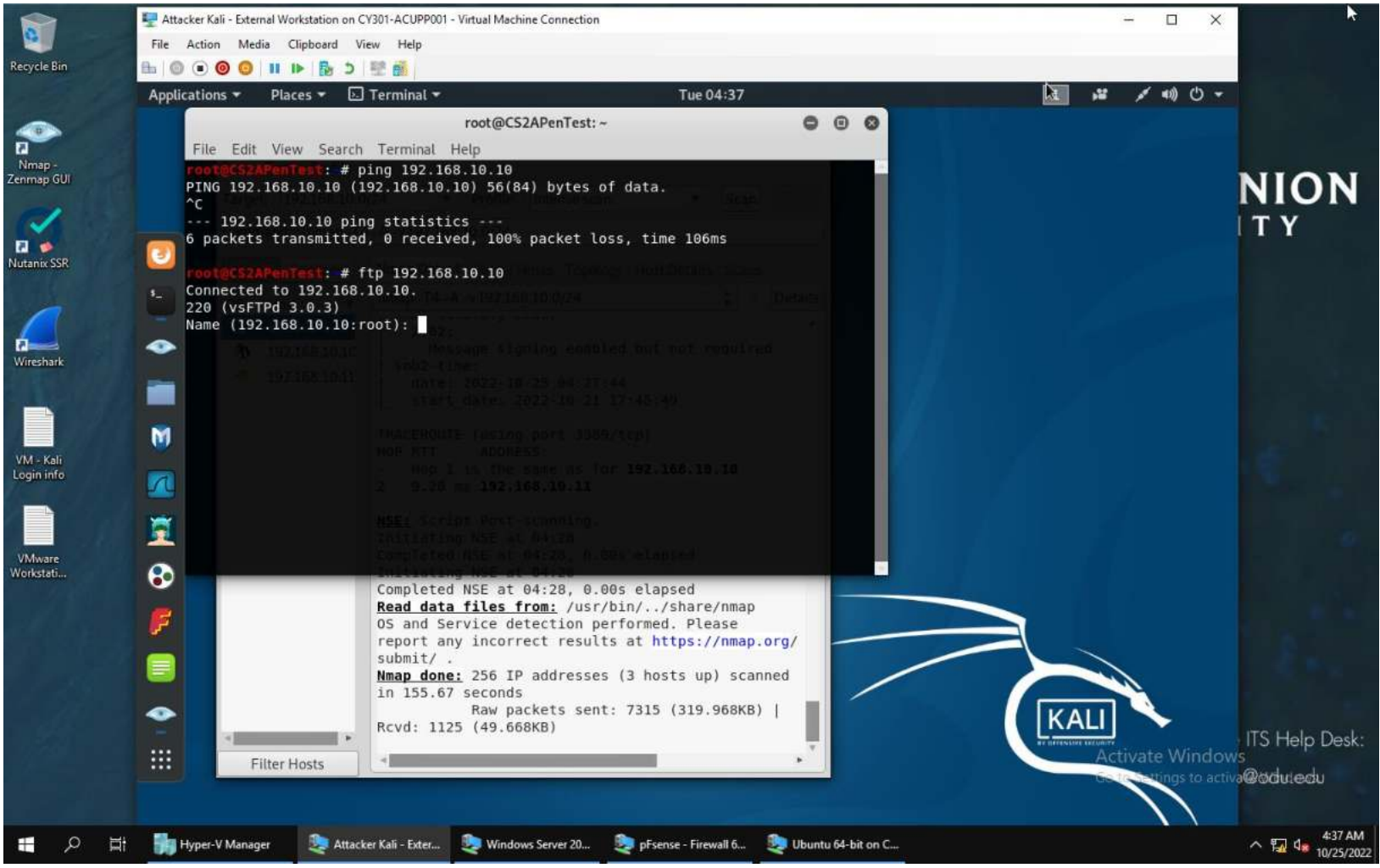
ESSAY: When running wireshark in the Ubuntu VMm while the External Kali VM scans the network, the traffic pattern presented first changes from the IMCP and DNS packets, in that IMCP contains the ping traffic and DNS the query, the traffic pattern changes to TCP protocol and a very consistent amount of TCP packets. This is because a lot of ports are open and this is identified by NMAP. The TCP packets are targeting all of the open ports. The ports are tugging on one another. The destination port in a way gets flooded. If a new intense scan is started and then we try to see the traffic pattern, what we see if a broadcast destination with the ARP packets now. This is asked what attacker is trying to scan the network, which is when the ARP protocol is broadcasted. All of the traffic comes back to the external network which is 192.168.10.2 and this is the bad guy. The round of ARP is done to see if anyone else will respond back. Then what comes after that in wireshark is the ping traffic will return with IMCP protocol.
So then here a combination of ARP and IMCP is present. Then after the broadcasts and ping, TCP packets become present again because there is a TCP query to every IP address. FTP is protocol is present as a form of communication where the request USER is anonymous with the request PASS IEUser and access is denied.

Firewall table filled out for Task B:

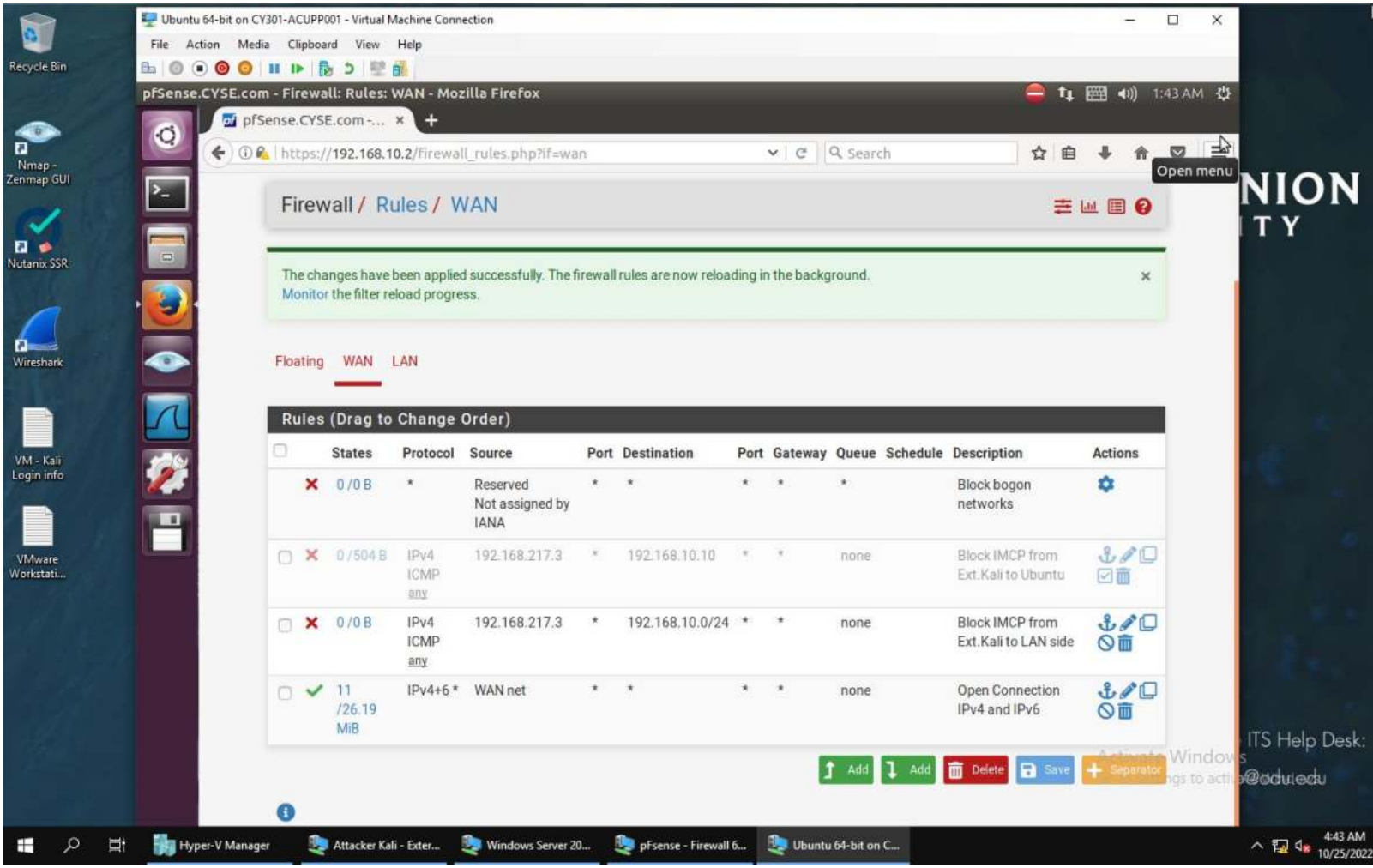
Rule #	Interface	Action	Source IP	Destination IP	protocol
1	WAN	Block	192.168.217.3	192.168.10.10	ICMP/no port
1	WAN	Block	192.168.217.3	192.168.10.0/24	ICMP
2	WAN	PASS	192.168.217.3	192.168.10.11	All
2	WAN	Block	192.168.217.3	192.168.10.0/24	All



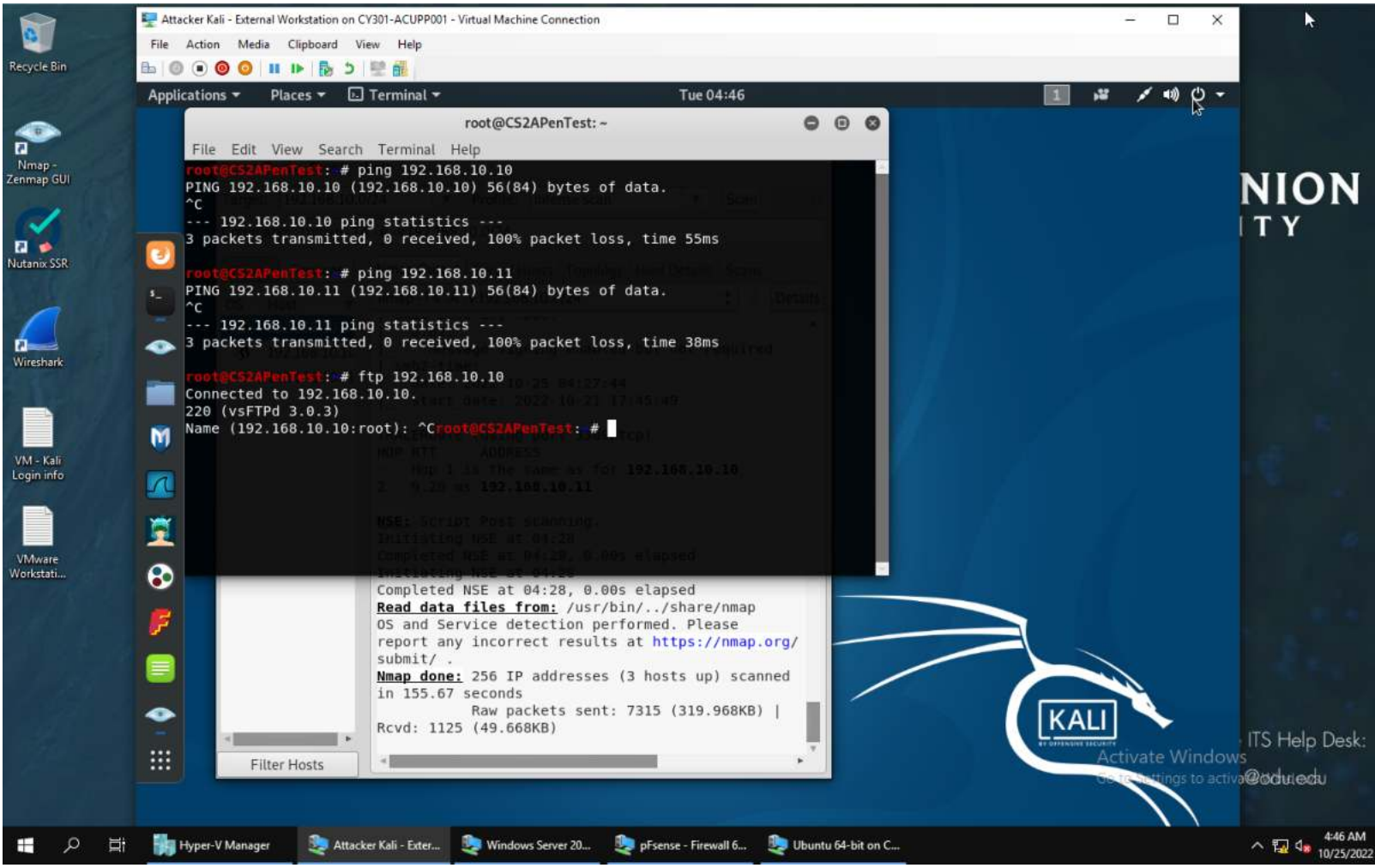
Picture of firewall for task B.1



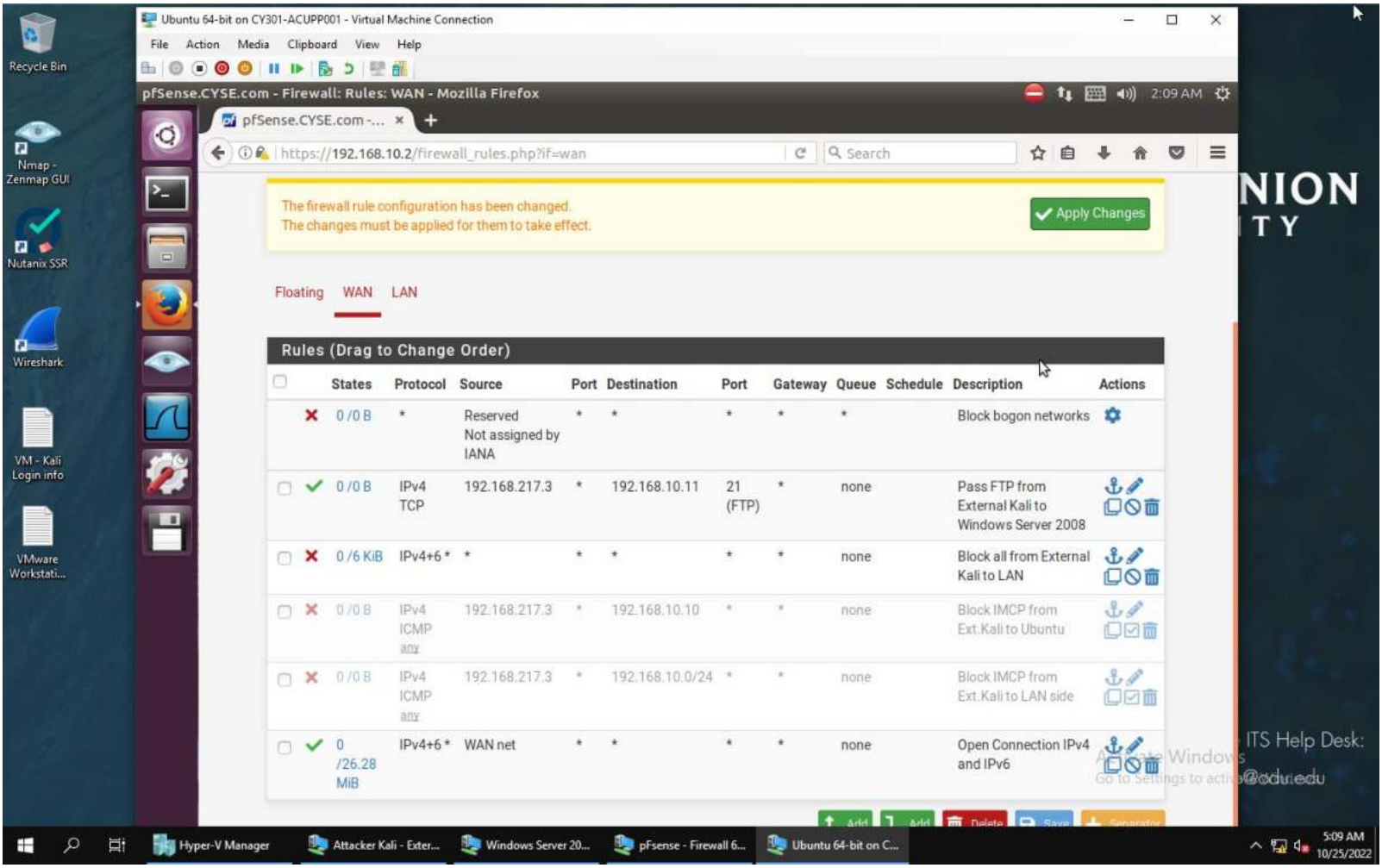
Verified result of firewall for task B.1



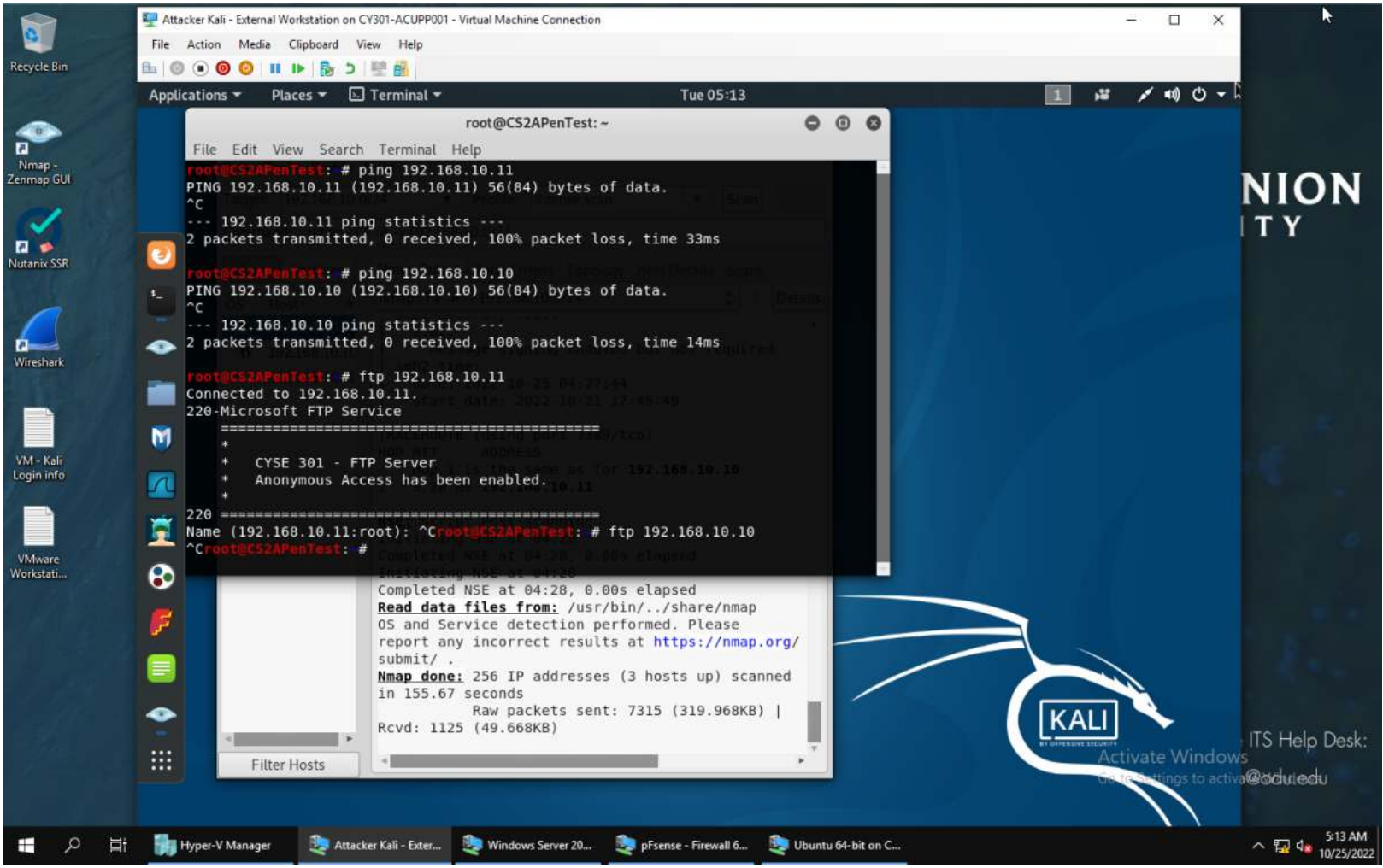
Picture of firewall for task B.2



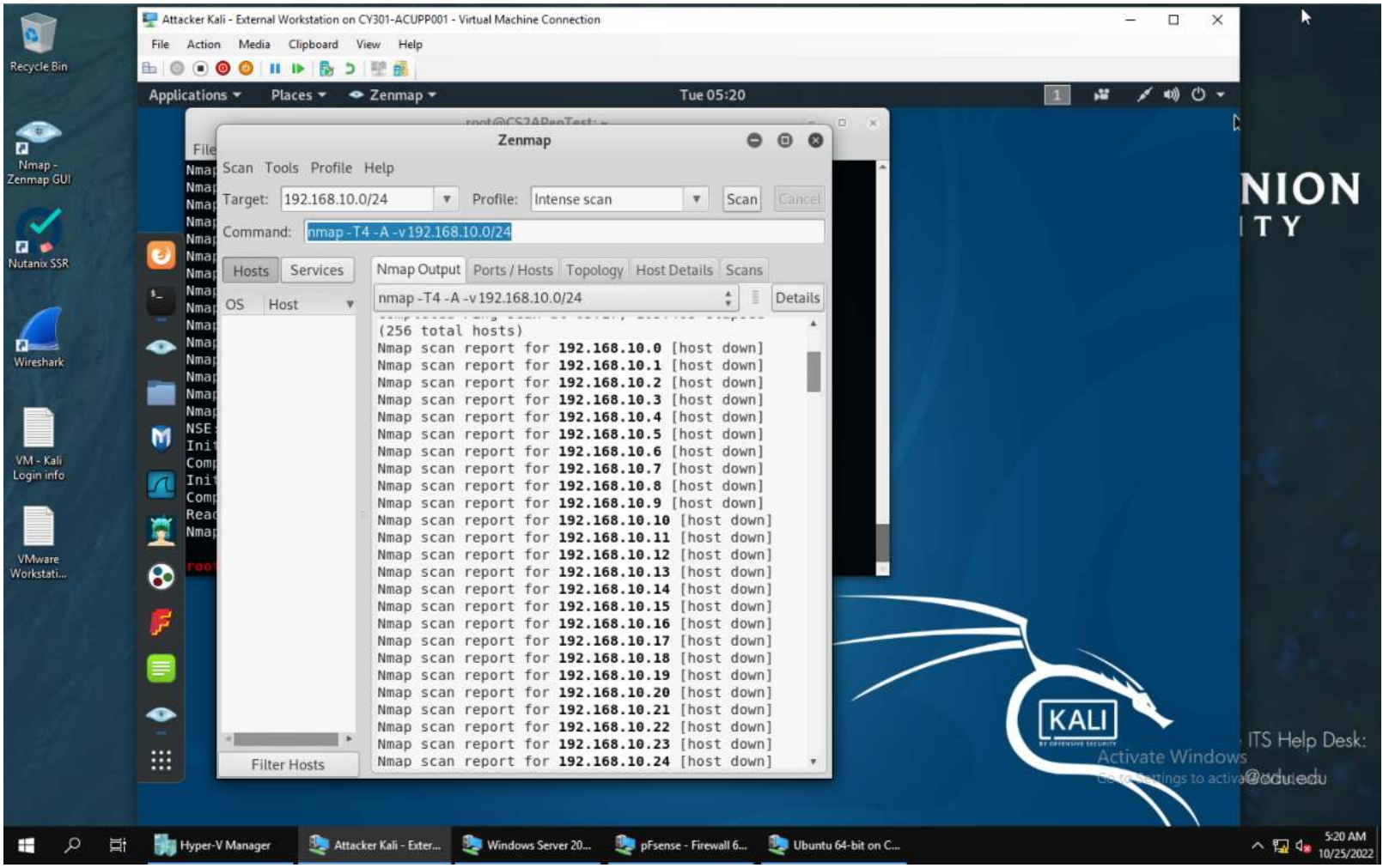
Verified result of firewall for task B.2



Picture of firewall for task B.3



Verified result of firewall for task B.3



B.4. The firewall policies created in B.3 is kept and task A.2 is repeated. As shown in the provided screenshot, the difference is the host for 192.168.10.2, 192.168.10.10, 192.168.10.11 are now down instead of up.