OLD DOMINION UNIVERSITY

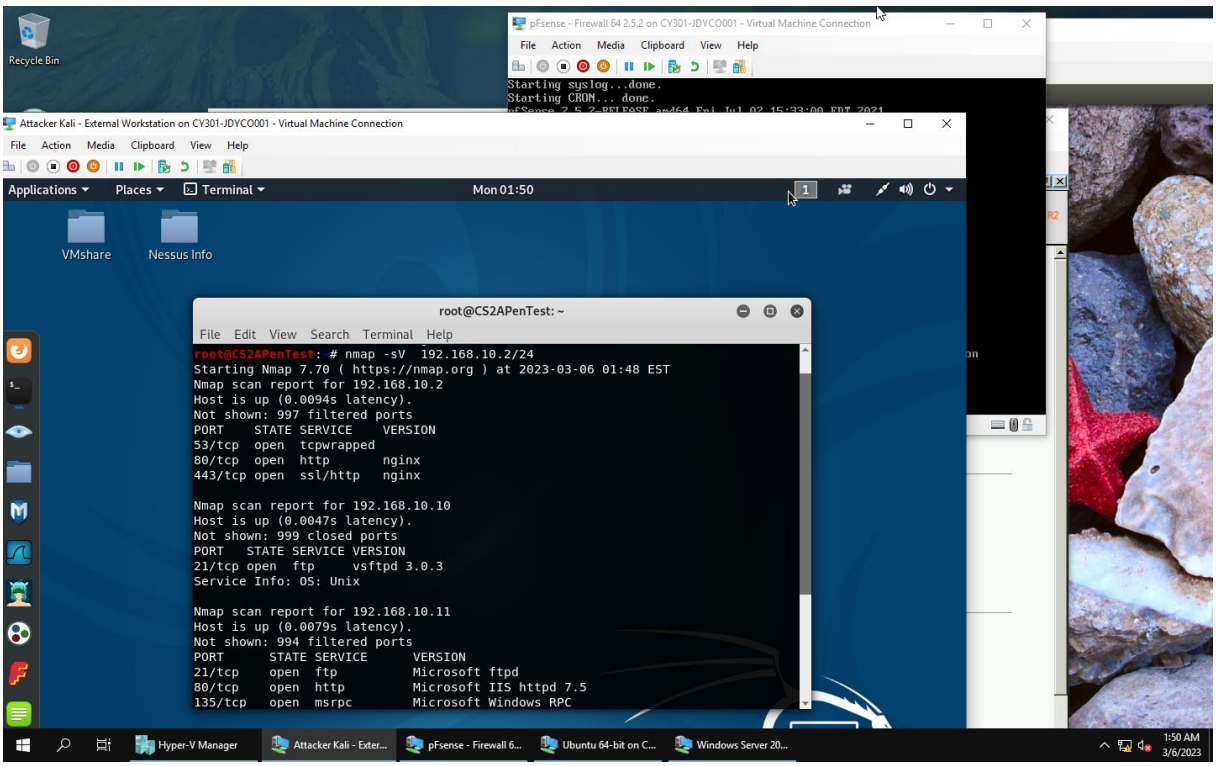
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

ASSIGNMENT #3– SWORD AND SHIELD

JEGGO PAOLO V. DYCOK

01242866

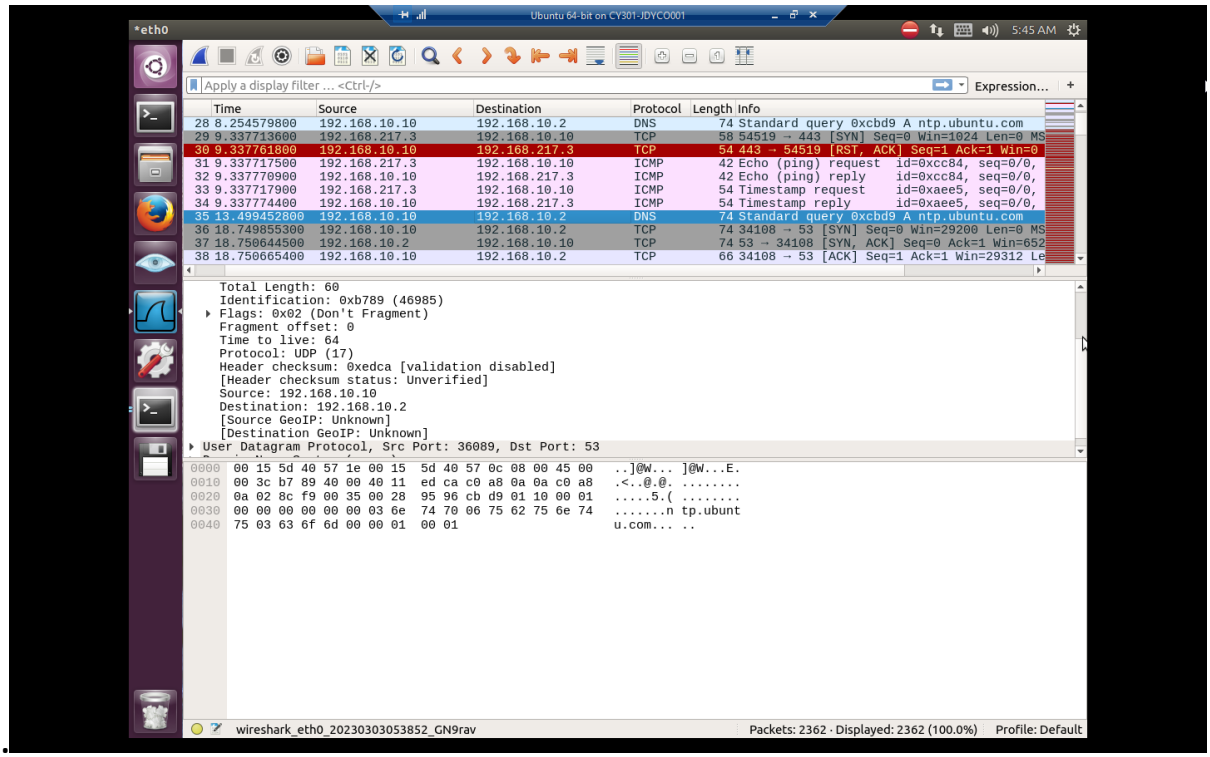
1. **Use Nmap to profile the basic information about the subnet topology (including open ports information, operation systems, etc.) You need to get the service and backend software information associated with each opening port in each VM.**

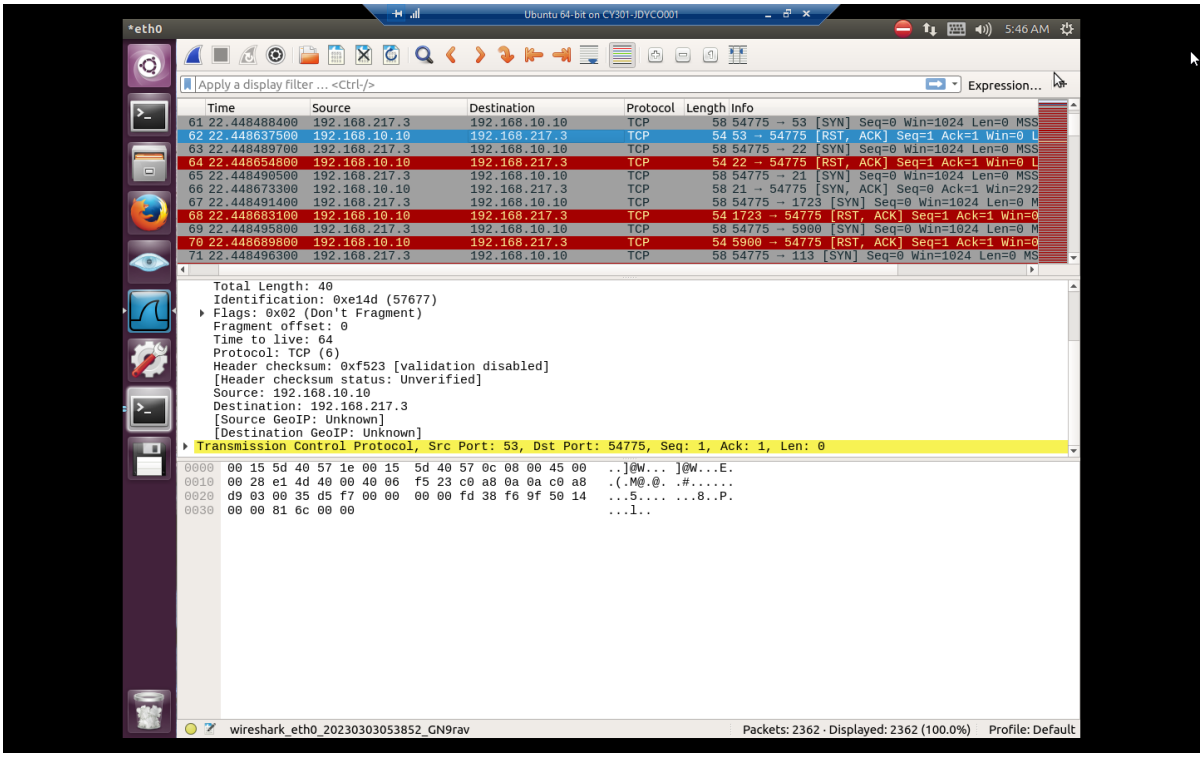


PROCEDURE:

- **I entered the command “nmap -sV 192.168.10.2/24” to get a scan of the topology within the subnet.**

2. **Run Wireshark in Ubuntu VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? Please write a 200-word essay to discuss your findings.**



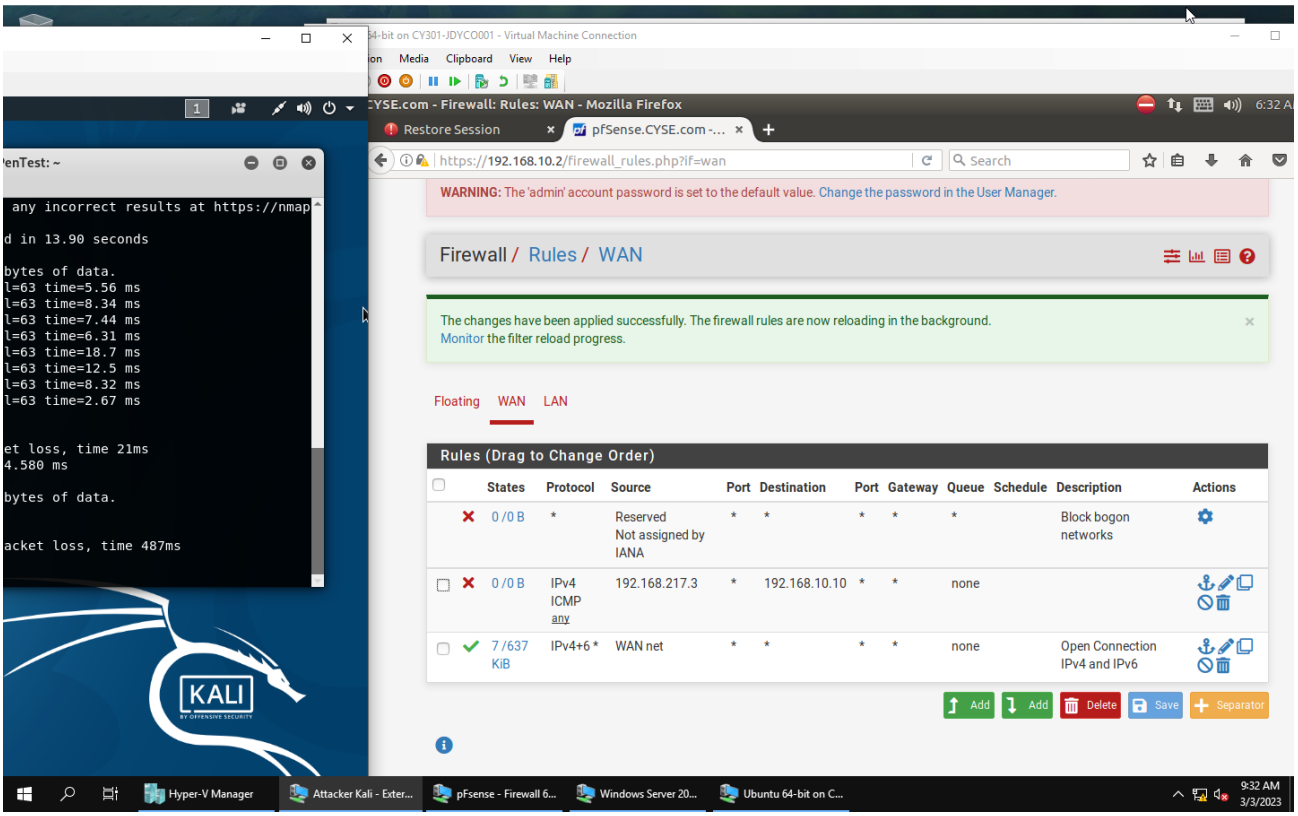


While running Wireshark, I observed that kali first sends ICMP requests to both the Ubuntu and the Windows server 2008. Wireshark then begins sending TCP requests and receives highlighted the TCP responses in red and sends out an “RST, ACK” in Flags. Plenty of packets were sent and plenty of them were dropped as well as indicated by black highlights. I also noticed that some of the TCP packets from

the subnet has been marked with red highlight as well as indicated by the source having the IP 192.168.10.2, forming a TCP connection with 192.168.10.10(Ubuntu) and 192.168.10.11(Windows Server 2008. By the end of the TCP transmissions, Kali sends TCP request to an open port which is port 21 and received an ACK reply. A couple of packets later, I see that there is an RST from the regular external Kali port used to send TCP packets 50088 to port 21 in Ubuntu. After the scan has been performed, external kali nmap scan returns a full port scan indicating that ports 21, 80, 135, 445 are open ports for windows server 2008 and port 21 for Ubuntu. It also displays the version under “Service Info”. The scan went through a total of 256 IP addresses in total.

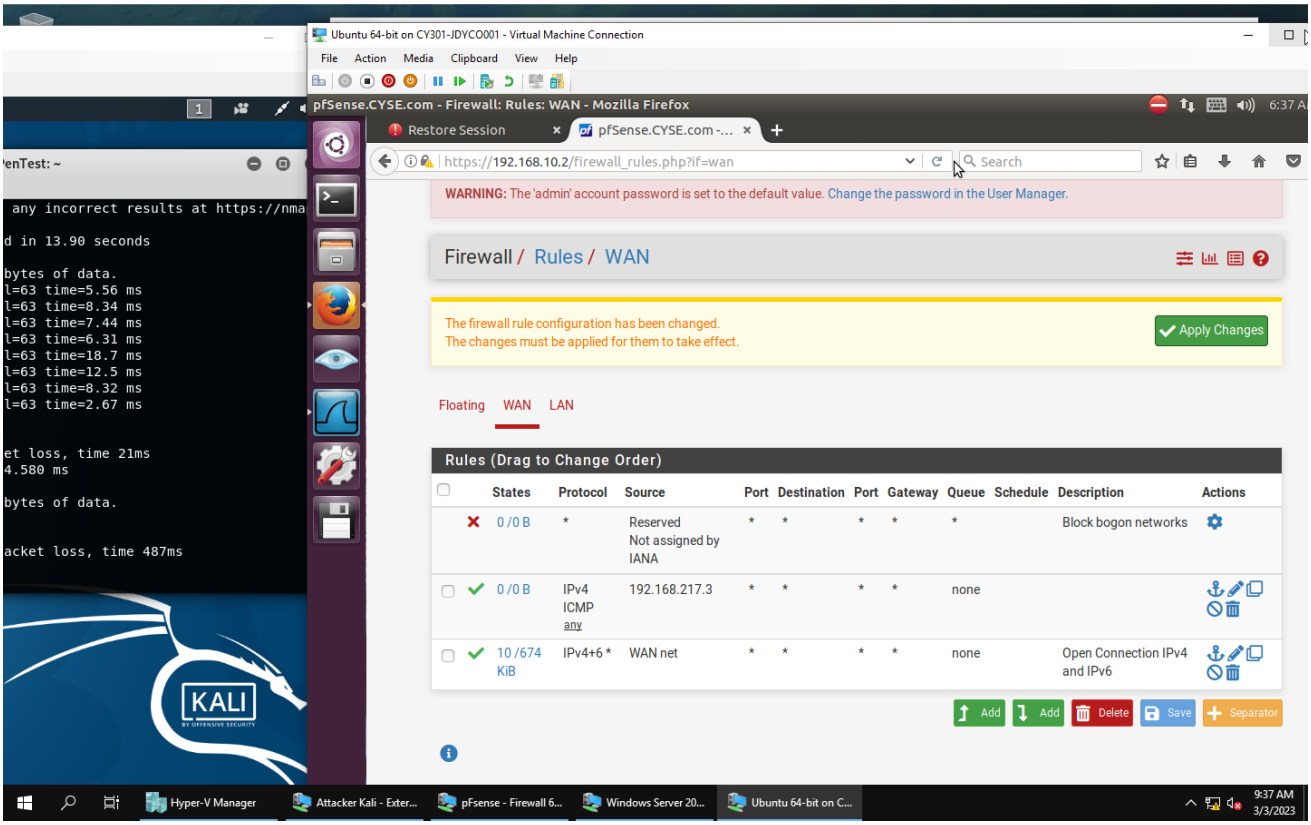
TASK B:

1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.



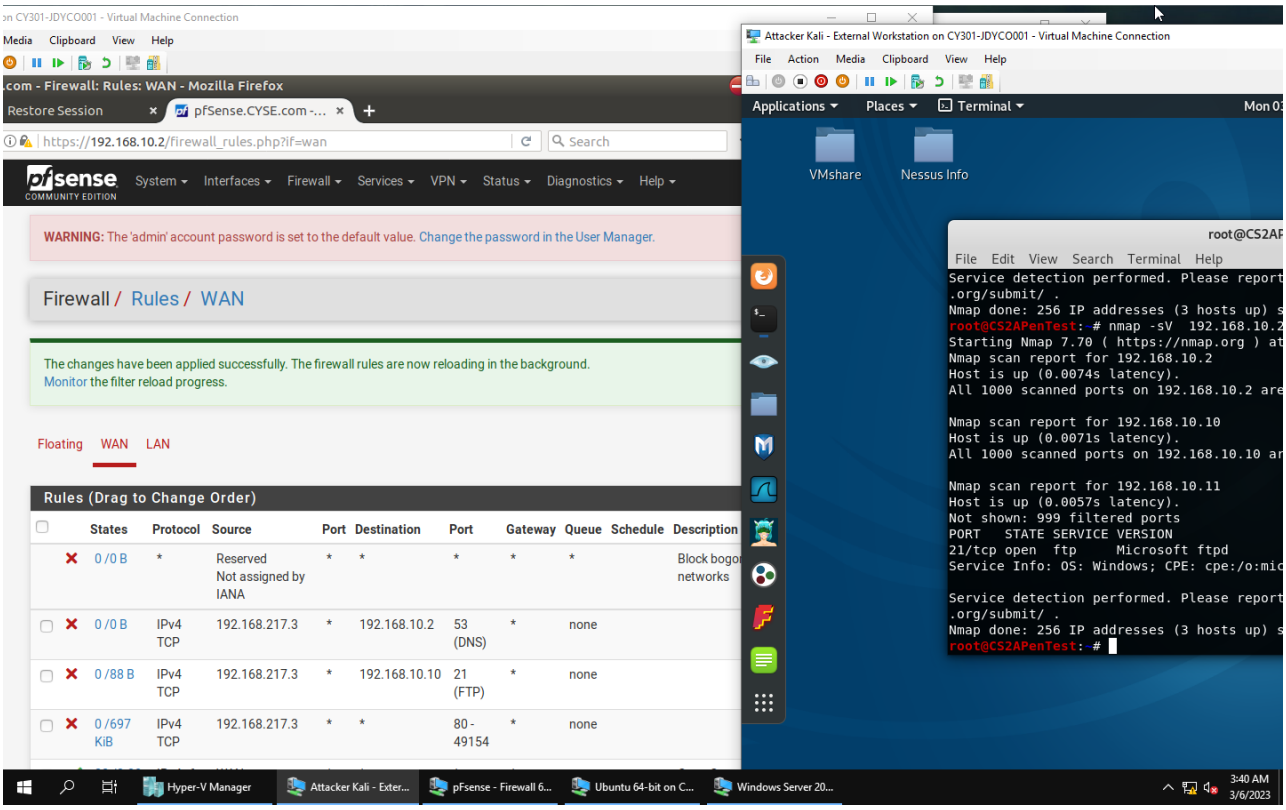
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port# if applicable)
2	WAN	Block	192.168.217.3	192.168.10.10	ICMP(any)

2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.



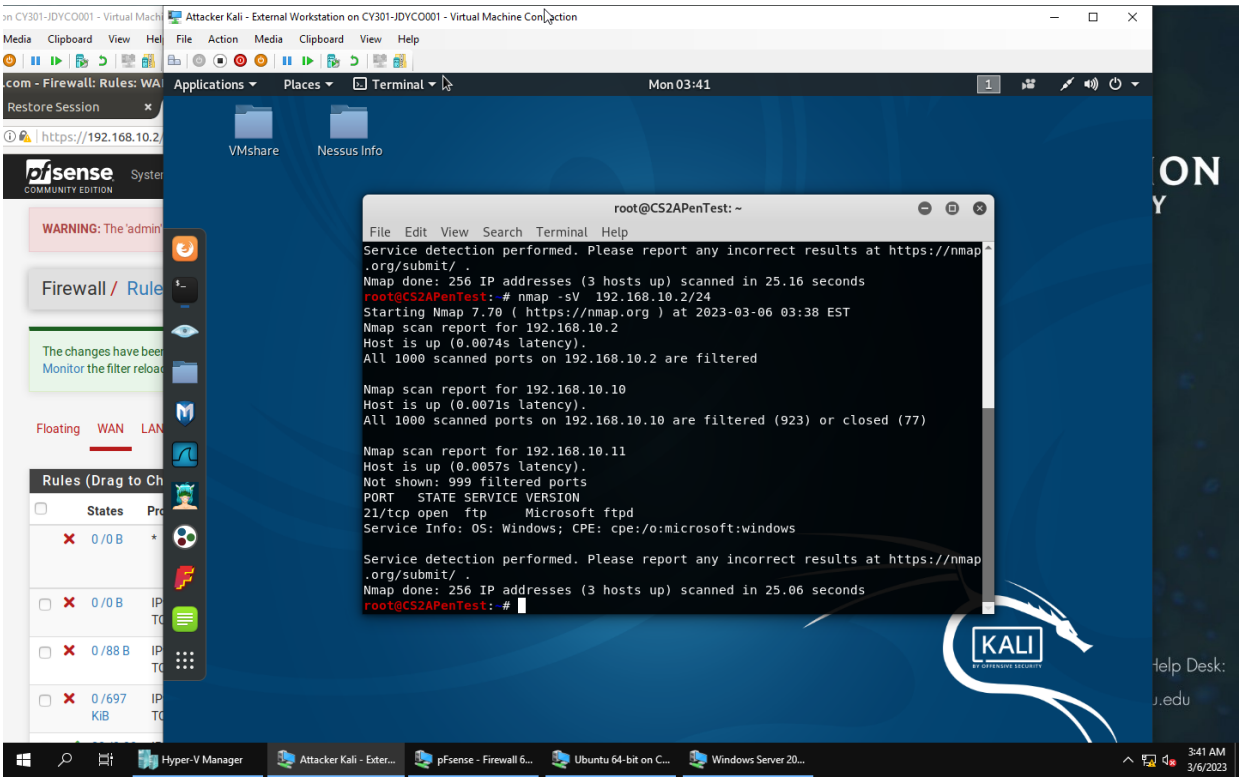
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port# if applicable
2	WAN	BLOCK	192.168.217.3	ANY	ICMP(ANY)

3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.



Rule #	Interface	Action	Source IP	Destination IP	Protocol (port# if applicable
2	WAN	BLOCK	192.168.217.3	ANY	TCP
3	WAN	BLOCK	192.168.217.3	192.168.10.10	TCP PORT:21
4	WAN	BLOCK	192.168.217.3	ANY	TCP POR:53

4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?



Procedure

- By blocking all TCP packets except FTP port 21 on windows 2008 server, nmap yields no reports on open ports.