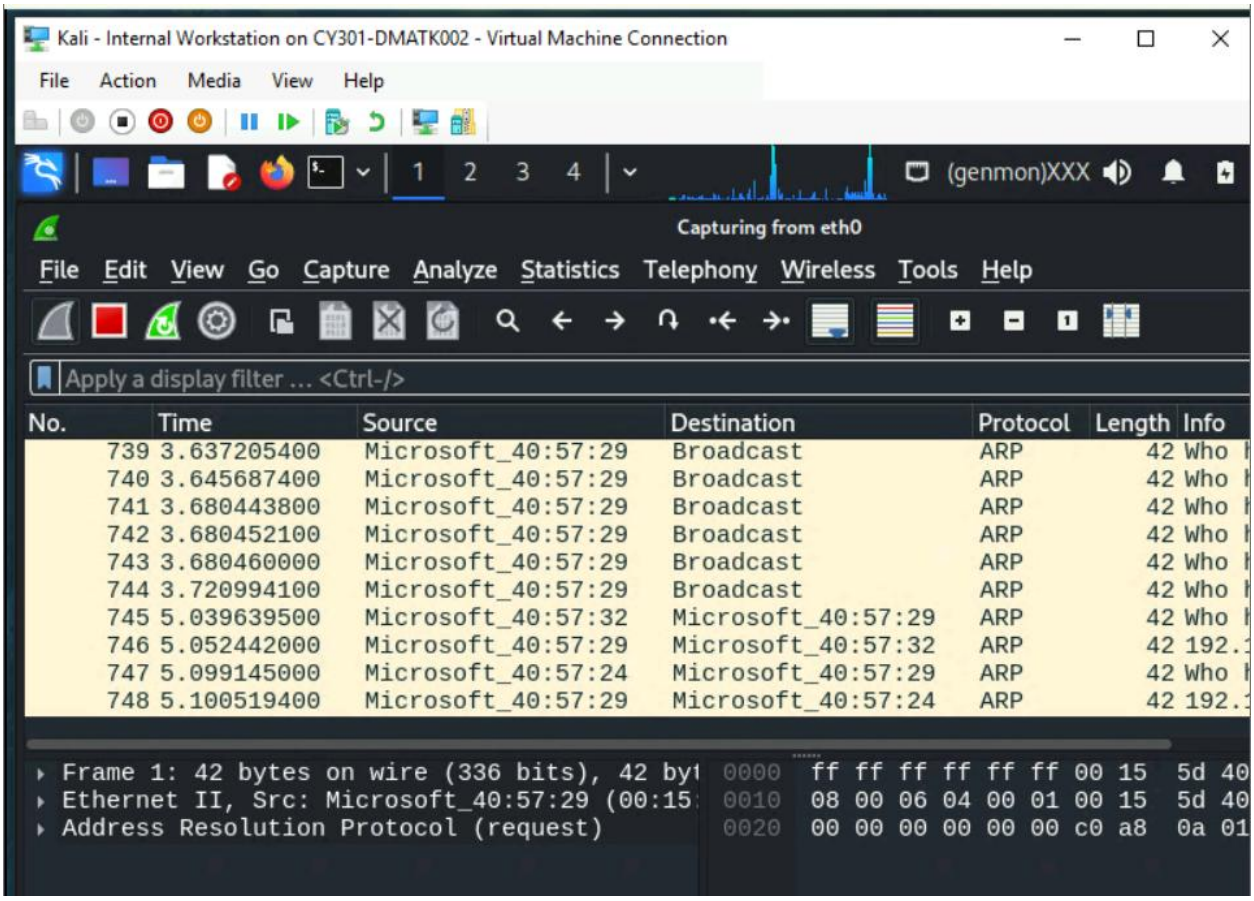
CYSE 301: Cybersecurity Technique and Operations

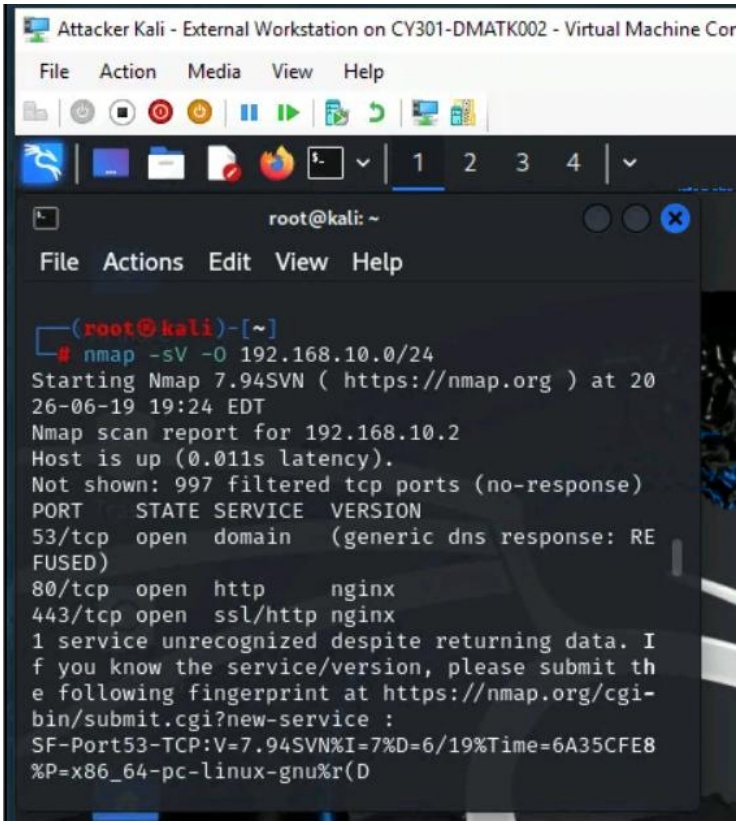
Assignment 2: Sword vs. Shield

Task A

1.



2.



Ip address of the VMS	Open ports	Service versions	Operating system detection	Backend software information
192.168.10.2	53, 80, and 443	Dns, nginx http, https	Linux	nginx
192.168.10.13	800, 8089	Splunkd httpd		Splunk
192.168.10.18	21,22	Vsftpd 3.0.5, open ssh 8.9p1	Ubuntu Linux	Vsftpd FTP
192.168.10.19	135,139,445	Msrpc, NetBios, Microsoft-ds	Windows	Windows file sharing

3. After doing the Nmap scan it had shown four active hosts on 192.168.10.0./24. We were able to see information about open ports, service versions, operating systems, and the backend software information. The ip address 192.168.10.2 was running DNS and had open ports 53, 80, and 443 using nginx. Using this information, we can assume the system was possibly a web server. The host 192.168.10.18 was running on Splunk services on the ports 8000 and 8089 and this is more likely to be used for log management/monitoring rather than webservices. The host 192.168.10.18 was shown as a Ubuntu Linux system and running FTP and SSH services on ports 221 and 22 through OpenSSH and vsFTPd. Lastly the host 192.168.10.19 was a Windows system with ports 135, 139, and 445. These have also been commonly used as windows networking/file sharing services.

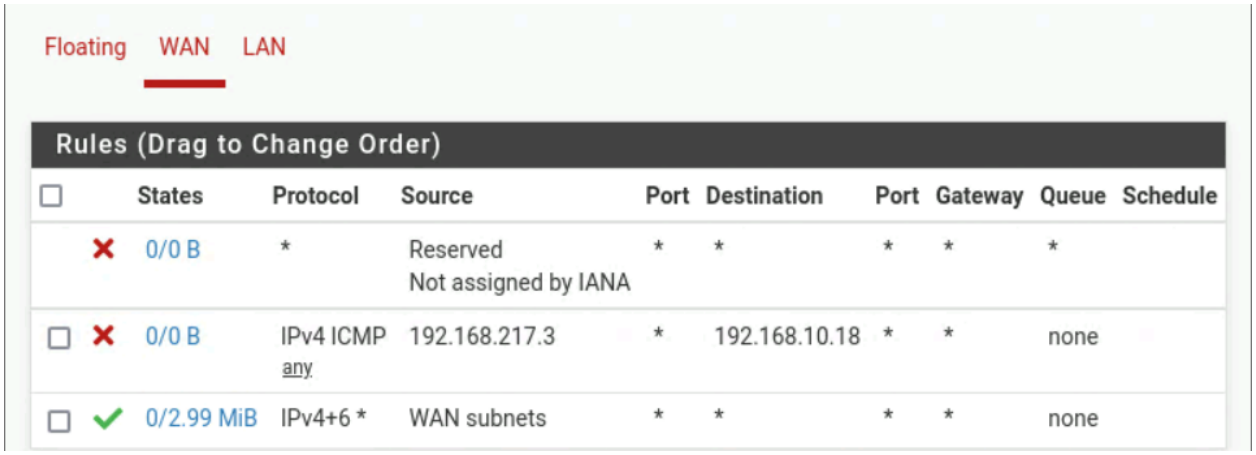
   The Nmap scan had identified a lot of useful information about the systems connected to the networks. It identifies the open ports and running services so an admin can understand the purpose of each host and can also verify any required services are operating correctly. However, the result also shows potential attackers the same information which can be useful to them when they are planning attacks.

Task B

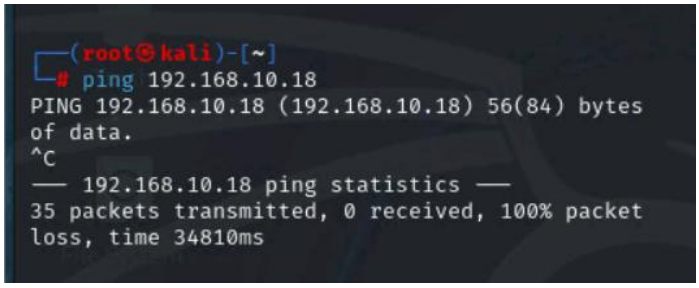
1.

Rule #	Interface	Acton	Source ip	Destination ip	Protocol
1	WAN	IPv4 ICMP	192.168.217.3	192.168.10.18	Block

a.



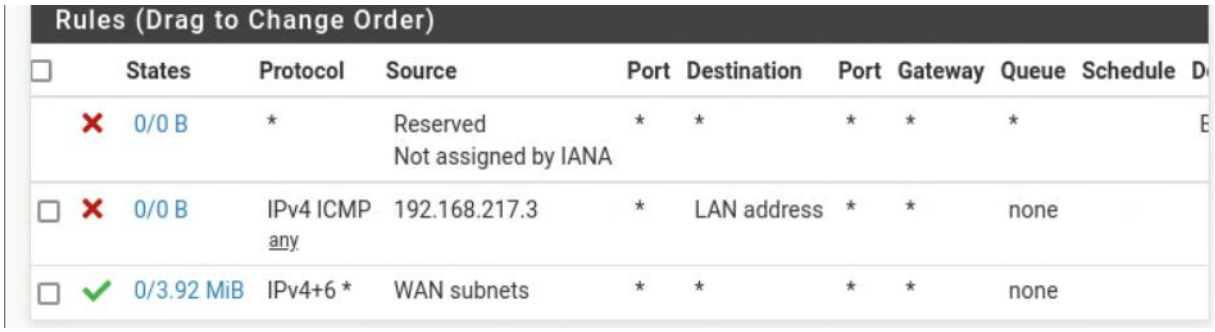
b.



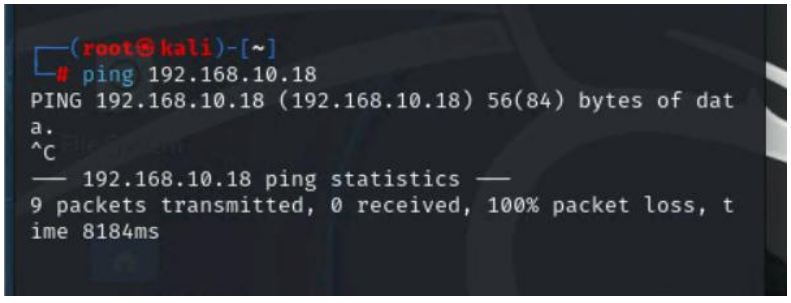
2.

Rule #	Interface	Action	Source IP	Destination Ip	Protocol
1	WAN	Block	192.168.217.3	Lan subnet	ICMP

c. Changed this to lan subnet*



d.



What security advantages does blocking ICMP provide?

Blocking ICMP can help lead to a couple different security advantages. Since ICMP is used for network discovery by blocking ICMP traffic, administrators can attempt to hide systems from attacks. This is important since attackers might use ICMP requests so they can find any active hosts before executing attacks. By preventing ICMP responses, we can reduce the amount of information that any threat actors can use to try and get into the network.

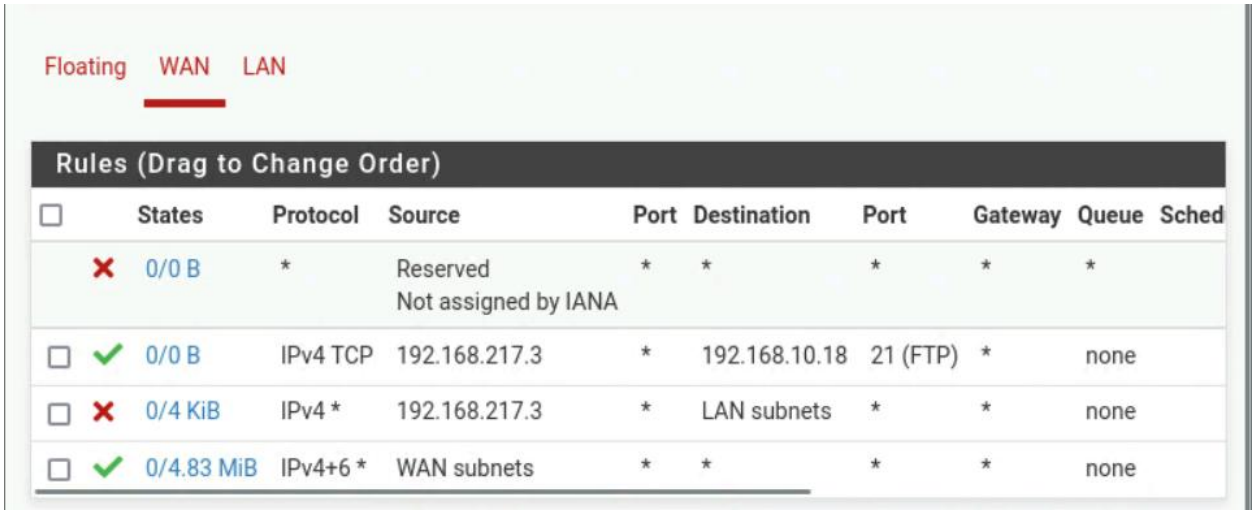
What operational disadvantages might occur?

However, while blocking does help hide some valuable information from threat actors, it does also create a few disadvantages as well. Administrators sometimes rely on ICMP for troubleshooting any connectivity issues. So if ICMP is blocked, then any diagnosing network issues will fail because tests like pinging will fail even if a system is functioning how it is supposed to. So while blocking ICMP can help improve security by reducing visibility, at the same time it also makes network monitoring and troubleshooting more challenging.

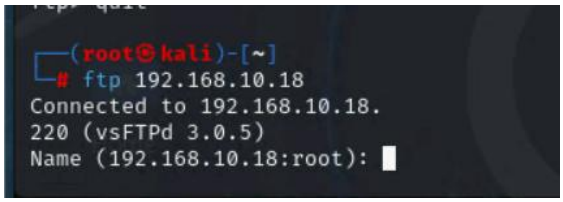
3.

Rule #	Interface	Action	Source IP	Destination Ip	Protocol
1	WAN	Pass	192.168.217.3	192.168.10.18	FTP
2	WAN	Block	192.168.217.3	Lan subnets	any

e.



f.



4.



Before firewall rules	**After firewall rule**
Open ports	No hosts were discovered and no open ports identified
OS detection accuracy	No OS detection
Service Enumeration	No services detected

a. **Why does Nmap show "filtered" instead of "closed", if there is any**
   Nmap would show filtered instead of closed because when a firewall blocks the scan packets before they reach the system. A closed port would normally respond to Nmap and then indicate that the host can be reached but not listening on the port. However, a filtered port doesn't respond because the firewall prevents any communication from reaching the destination and then returning to the scanner.

b. **How firewall behavior affects scan results**
   Firewall behavior can affect scan results because it controls which network traffic is allowed through or blocked. Before firewall rules are implemented, Nmap is able to identify any active hosts, detect open ports, and services. After the firewall was activated, Nmap was not able to discover any hosts on the network. This helped show how firewalls can limit scanning activities by restricting the traffic between networks.

c. **What information is hidden from attackers**

   The firewall can hide information from attackers like active hosts, open ports, service versions, and a couple other operating system information. Implementing a firewall can help prevent this information from falling into attacker's hands. So, by reducing the amount of information the attackers can see makes it more difficult for them to find any vulnerabilities.