

PROJECT 1 REPORT

CS4371

Instructor: Dr. Randy Klepetko

Feb 24, 2023

PROJECT 1

BY

Lauren Taylor

Dillon Hughes

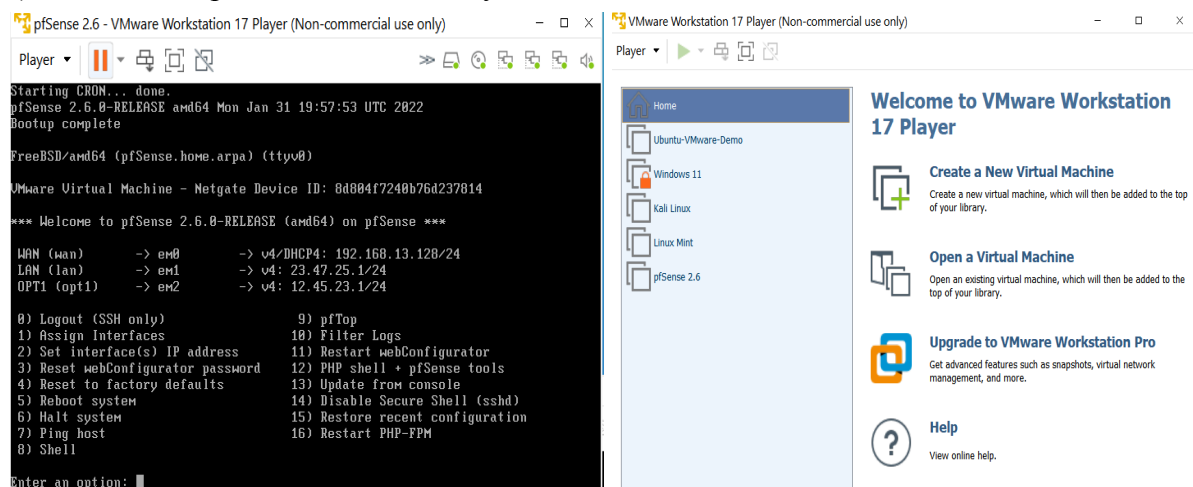
Stanley Nwajiaku

Section I (Introduction):

Our group worked together to finish all tasks. Since the sandbox was set up only on one computer we had to communicate and find times throughout the week that worked best for everyone. The sandbox was set up on Stanley's computer so when we had meetings in discord we were able to all help and contribute to all parts of the assignment. Furthermore, Lauren and Dillon worked on writing the reports such as the introduction and summary. Stanley was able to successfully set up his network for the project, so he worked on Task II and Task III with the help and commentary of everyone. Stanley also took the screenshots of his network. Moreover, Dillon worked on Task V after our group discussed the scenario. Lauren worked on implementing a security policy for the network also with the help from others. As a group, each team member was given a responsibility or task and was held accountable for their role. If a member needed assistance with a task, other team members were able to help. Thus, it was a group effort.

Section II (Task II):

a) Provide a snapshot of the network you built.



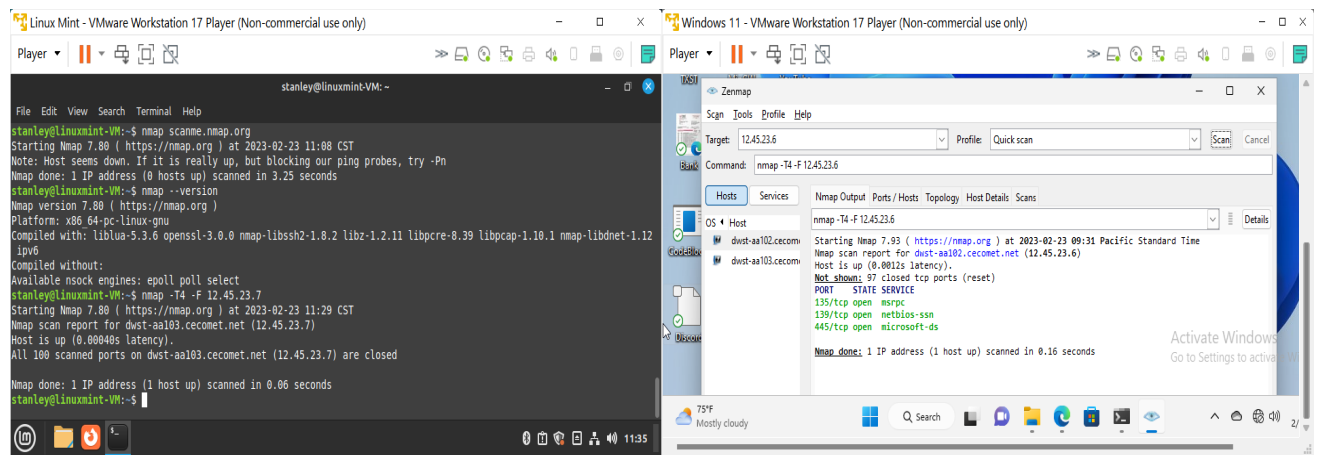
b) Those that use docker, a screenshot of the images.

c) Show the NMap commands to scan the computers and the service ports.

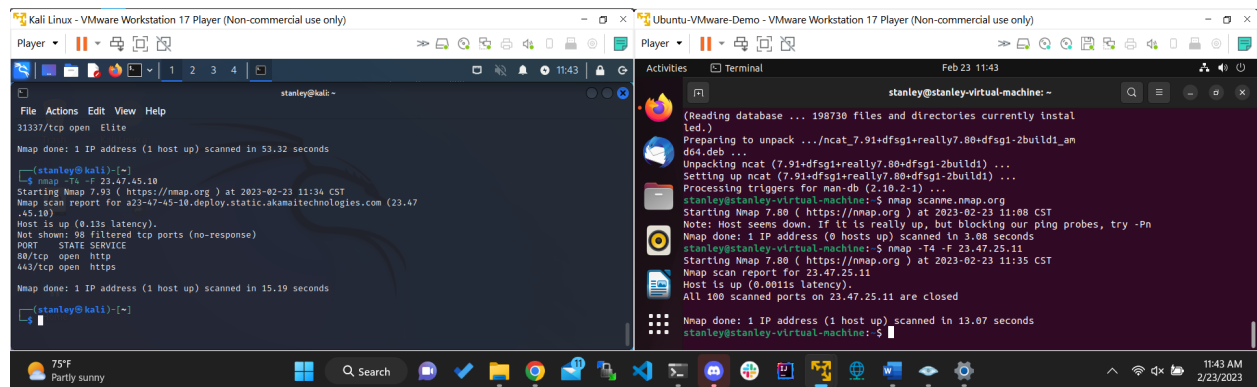
- ❖ In the command prompt: `nmap -T4 -F ip_address` will initiate a Quick scan.
- ❖ In the command prompt: `nmap scanme.nmap.org` will confirm if Nmap is installed and operating correctly and this scan will show Port | State | Service. The Port state includes open, closed, filtered, unfiltered.

d) Show the discovered IPs and services in Network A and B (screenshots).

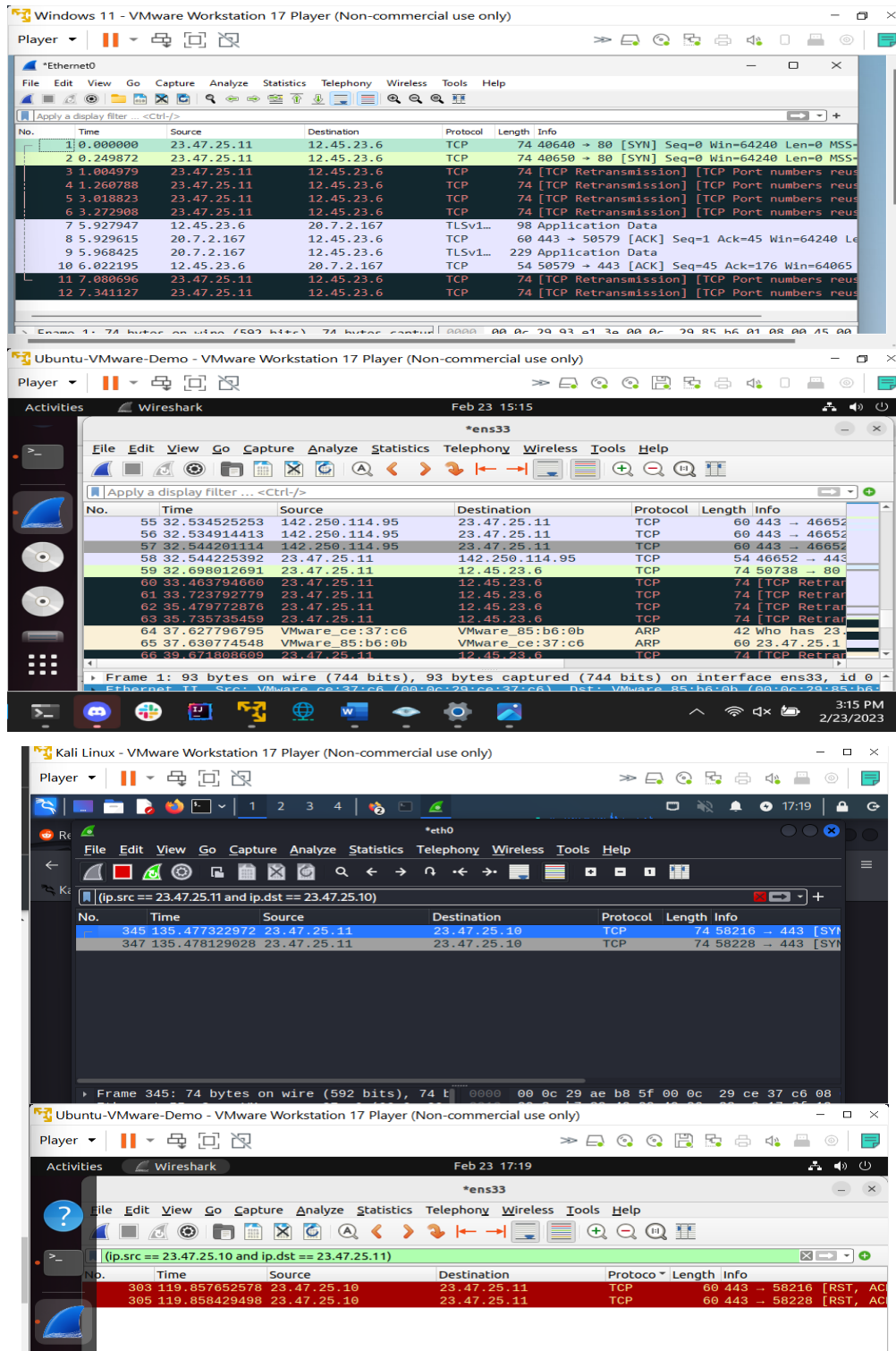
Network A: Ubuntu linux(A.1) ip: 23.24.25.11 and Kali linux(A.2) ip: 23.24.25.10



Network B: Windows 11(B.1) ip: 12.45.23.6 and linux mint(B.2) ip: 12.45.23.7

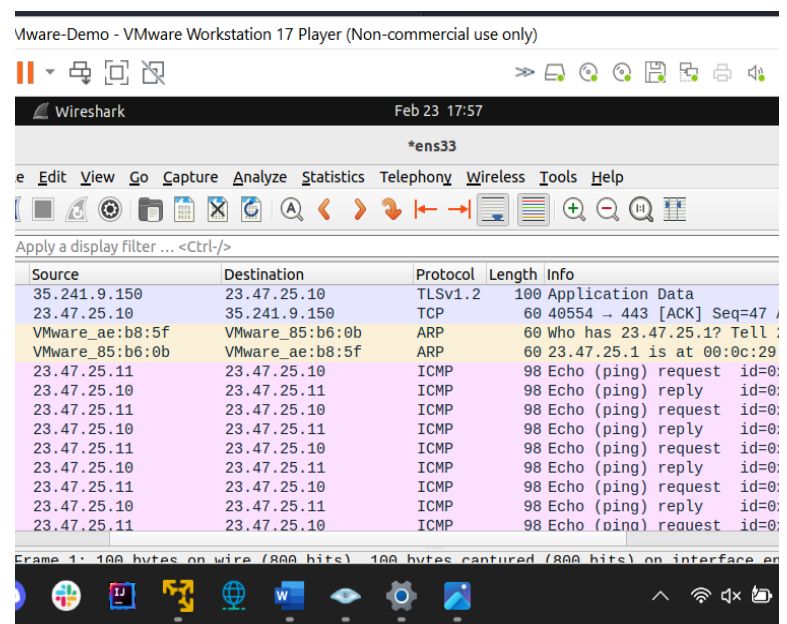
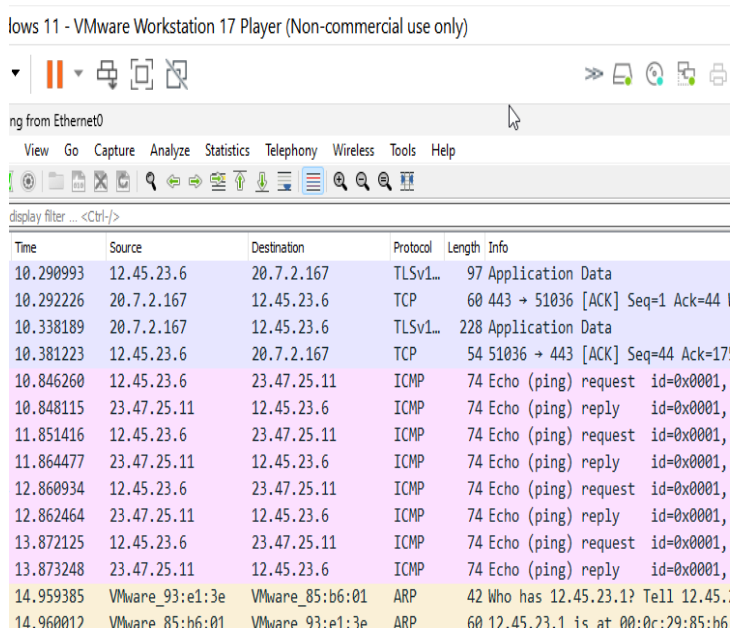


e) Show the Wireshark results (screen shots) of checking the web service between B.1 and A.1, and between A.2 and A.1. State if web service is allowed between computers.



- ❖ There is no complete web service communication between B.1 and A.1 and between A.1 and A.2 because there is no HTTP protocol to confirm that the communication is indeed a web service. There was only TCP retransmission, ACK (acknowledges) between the two ip addresses.

f) Show the Wireshark results (screen shots) of checking the ping between B.1 and A.1, and between A.2 and A.1. State if ping is allowed between computers.



- ❖ Yes we could ping between Ubuntu(A.1) and Windows11 (B.1), and between Kali linux (A.2) and Ubuntu(A.1).

Section III (Task III):

a) Show the access control matrix.

- ❖ An Access control from the given security policy in Task III

<i>ACM</i>	Server(A.1)	Workstations (A.2)	External Computers
Server	Deny	Allow(http, ssh)	Allow(http)
Workstations	Allow(http, ssh)	Deny	Allow(http)
External computers	Deny	Deny	N/A

<i>Source</i>	Destination	Service	Action
External Computer	Server(A.1)	HTTP	Allow

External Computer	Server(A.1)	SSH	Deny
Workstations (A.2)	Server(A.1)	HTTP	Allow
Workstations (A.2)	Server(A.1)	SSH	Allow
Server(A.1)	External Computer	Any	Deny
Workstations (A.2)	External Computer	HTTP	Allow
Workstations (A.2)	External Computer	SSH	Deny
A.1,A.2, Any	Any	ICMP	Allow
External Computer	A.1,A.2, Any	ICMP	Deny
Workstations (A.2)	External Computer	Any	Deny

b) Find and explain which policy CANNOT be completely enforced by the iptables of R.

- ❖ Policy f: The workstations can access only the web service provided by external computers.

According to the iptable rules, workstations may also have access to other services besides web services on any other external computer in Network B. Thus, policy f cannot be completely enforced by the iptables of R.

- ❖ Policy h: External computers cannot ping to the workstations or the server.

Blocking ping or ICMP requests does not offer many benefits. Iptables should allow ping requests in order to troubleshoot.

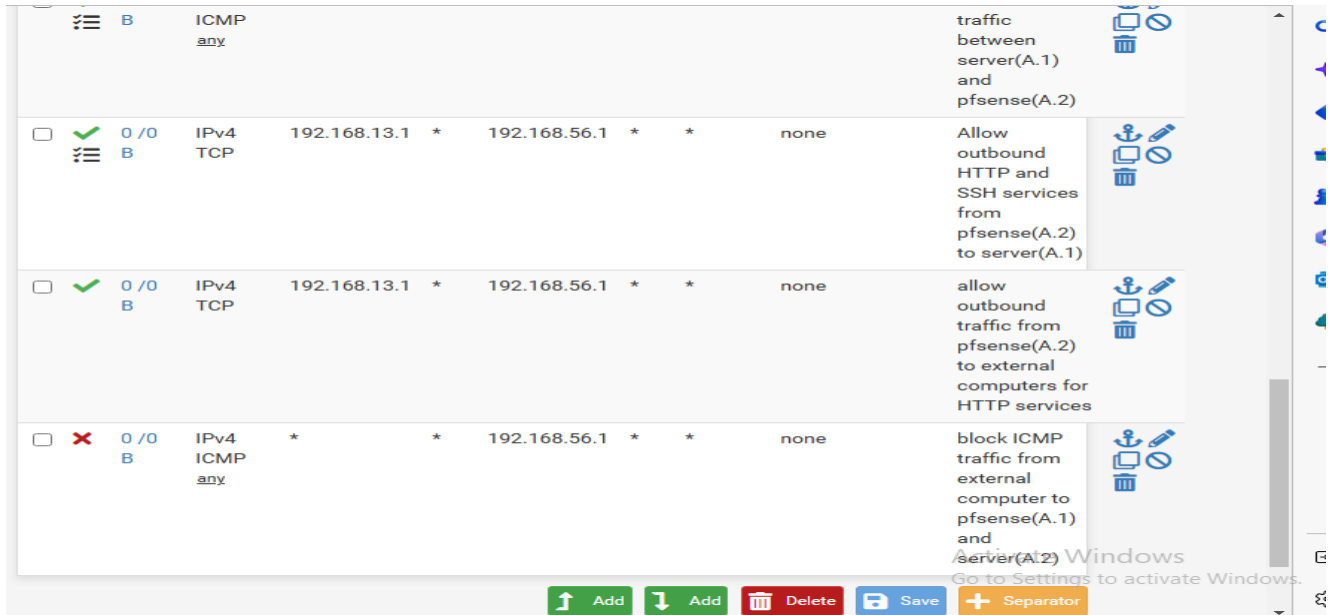
c) Show the iptables rules (iptables -S) in R. Explain the purpose of each iptables rule.

Floating WAN LAN OPT1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 4 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0 / 2 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	*	*	192.168.56.1	*	*	none		allow inbound traffic from external computer to the server (A.1) for HTTP and SSH services.	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 *	192.168.56.1	*	*	*	*	none		blocks outbound traffic from server (A.1) to external computers	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0	IPv4 *	*	*	192.168.13.1	*	*	none		block inbound	

<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 *	192.168.56.1	*	*	*	*	none		blocks outbound traffic from server (A.1) to external computers..	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 *	*	*	192.168.13.1	*	*	none		block inbound traffic to pfsense(A.2) from any external computers	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 ICMP any	192.168.56.1	*	This Firewall	*	*	none		block ICMP traffic from external computer to WAN(pfsense)	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 ICMP any	*	*	*	*	*	none		allow ICMP traffic between server(A.1) and pfsense(A.2)	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP	192.168.13.1	*	192.168.56.1	*	*	none		Allow outbound HTTP and SSH services from	



Section IV (Task IV):

a) Show the NMap results (screen shots) of the exposed computers and ports of Network A.

```

^C
stanley@stanley-virtual-machine:~$ nmap -p1-65535 23.47.25.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 20:43 CST
Stats: 0:02:41 elapsed; 253 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 77.78% done; ETC: 20:47 (0:00:45 remaining)
Stats: 0:05:40 elapsed; 253 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 86.80% done; ETC: 20:50 (0:00:51 remaining)
Stats: 0:10:11 elapsed; 253 hosts completed (3 up), 3 undergoing Connect Scan
Connect Scan Timing: About 98.85% done; ETC: 20:54 (0:00:07 remaining)
Nmap scan report for pfSense.home.arpa (23.47.25.1)
Host is up (0.00081s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http

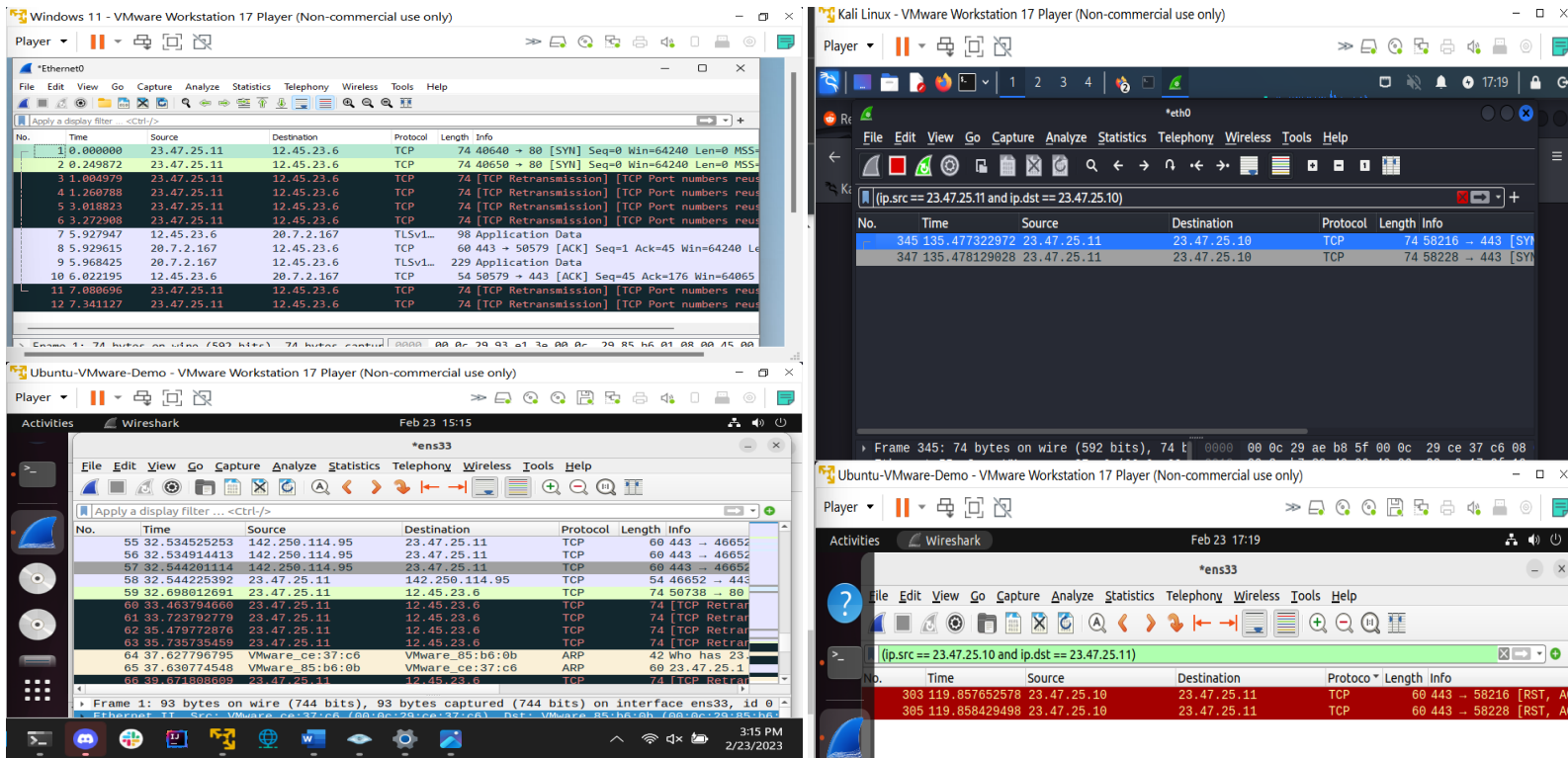
Nmap scan report for a23-47-25-10.deploy.static.akamaitechnologies.com (23.47.25.10)
Host is up (0.0014s latency).
All 65535 scanned ports on a23-47-25-10.deploy.static.akamaitechnologies.com (23.47.25.10) are closed

Nmap scan report for a23-47-25-11.deploy.static.akamaitechnologies.com (23.47.25.11)
Host is up (0.00081s latency).
All 65535 scanned ports on a23-47-25-11.deploy.static.akamaitechnologies.com (23.47.25.11) are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 636.61 seconds
stanley@stanley-virtual-machine:~$

```

b) Show the Wireshark results (screen shots) of checking the web service between B.1 and A.1, and between A.2 and A.1. State if web service is allowed between computers.

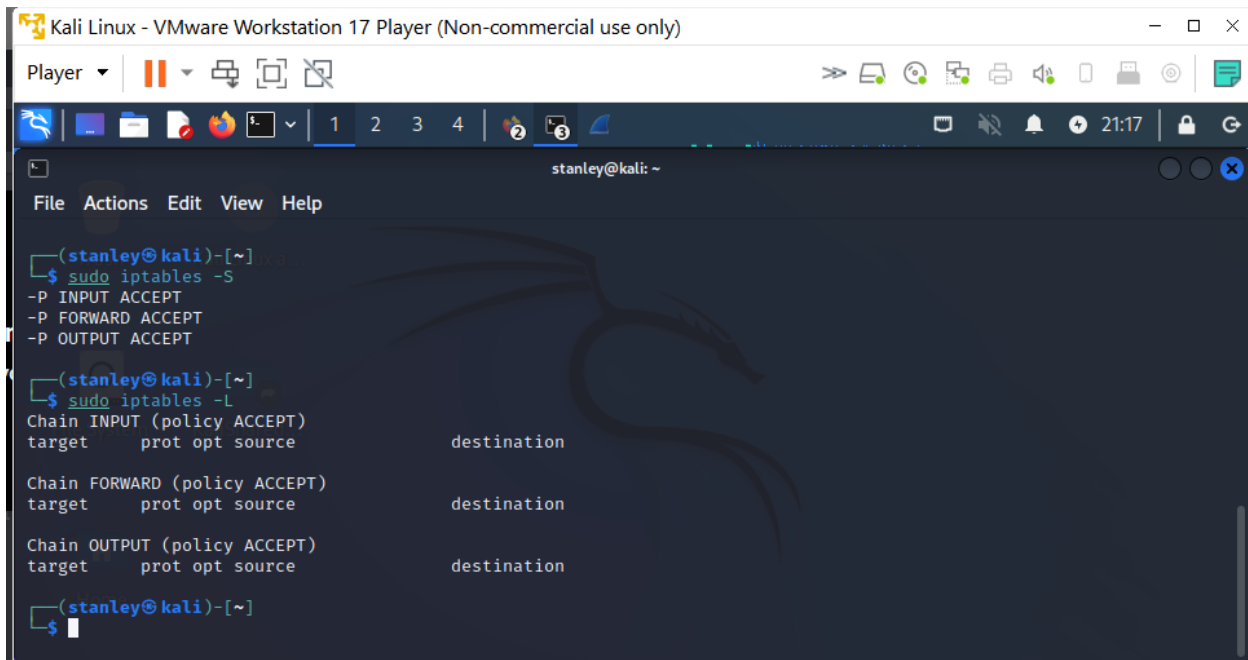


- ❖ There is no complete web service communication between B.1 and A.1 and between A.1 and A.2 because there is no HTTP protocol to confirm that the communication is indeed a web service. There was only TCP retransmission, ACK (acknowledges) between the two ip addresses.

c) Show the Wireshark results (screen shots) of checking the ping between B.1 and A.1, and between A.2 and A.1. State if ping is allowed between computers.

The output shows that the default policy for the three chains (INPUT, FORWARD, and OUTPUT) is set to ACCEPT. This means that if no specific rules are defined for a particular type of traffic, the firewall will allow it to pass through without further filtering.

b) Show the iptables rules (iptables -S) to enforce the security policy in A.2 that is not implemented in R. Explain each iptables rule.

A screenshot of a Kali Linux terminal window running inside a VMware Workstation 17 Player. The terminal shows the output of the 'sudo iptables -S' and 'sudo iptables -L' commands. The default policies for INPUT, FORWARD, and OUTPUT chains are all set to ACCEPT. The terminal output is as follows:

```
(stanley@kali)-[~]
$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT

(stanley@kali)-[~]
$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

(stanley@kali)-[~]
$
```

c) Assume the company only stores classified business data in Computer A.1, and does not allow anyone to carry a device to transfer data. Users have accounts on A.1 to access the data. Discuss whether the security policy can ensure that the classified data will not be disclosed to external computers through the network. Be as specific as possible in your discussion. For example, if you do not think the security policy is secure, you shall show which item of the policy has a problem or which policy is missing.

Response:

This company has a reasonable security policy. There are a few flaws in the given policy. The first flaw in this policy is that it does not explicitly address the possibility of an inside threat. The policy states that the users have accounts on A.1 to access data. What is not stated is access controls or monitoring mechanisms. The access controls and monitoring mechanisms should be implemented in this case to prevent and detect unauthorized access and/or misuse by an authorized user. Role-based access control, logging and auditing of user activity, and regular security training for employees to promote security awareness.

Secondly, the given policy assumes there are no vulnerabilities or exploits in the software running on the computer with the business data. The assumption of not having vulnerabilities can be something the security or I.T department just sweeps under the rug and eventually someone is going to find a hole in the security and be able to gain unauthorized access to the data. For the company to be able to protect their network, a regular updated system, and vulnerability scanning and penetration testing should be applied periodically to identify and remediate any weakness in the business system.

Lastly, the policy does not address the possibility of network based attacks or data exfiltration. Even though the users are not allowed to carry devices to transfer data, an attacker can still potentially compromise the network and steal or intercept the data in transit. For the company to be able to protect themselves, the network should be separated or segmented and firewalled to limit access to computer A.1. and the other non mentioned sensitive and confidential data. Encryption and other security protocols should also be in place for an extra layer to the firewall and to protect data in transit.

In conclusion, the given security policy provides a good foundation but you can never be too sure. Additional measures should be taken to address the insider threats, software vulnerabilities and network-based attacks. A security team should be implemented to in force specific access controls, network monitoring and regular security assessments and updates. As well as network segmentation and encryption. These are all important policies and components of a comprehensive security strategy.