Project #1: Firewall & Access Control

CS 4371 - Computer System Security, Spring ‘20

Instructor - Qijun Gu

Due Date: March 3rd, 2020

****

Group 12 Members:

Trevor Harmon

Randall Roy Harrison

Bryan Chinenye Muforo

Kelby Webster

Doohwan Yoon

****

Section I: Introduction

Individual credits

****

Task contributions:

- Trevor Harmon - wireshark tests, NMap tests, pinged computers, ran diagnostics, screenshots & internal/external network config + testing, helped fix network twice, succeeded troubleshooting on the external network, Cisco research, helped with firewall policies, wrote some of the report periodically, added screenshots for task 3 and 4 report (firewall policies, iptable commands, Nmap, and wireshark)
- Randall Roy Harrison - Cisco firewall research & implementation, ping + Wireshark testing, ran diagnostics, wrote some of the report periodically, succeeded troubleshooting on the external network, added screenshots for task 3 and 4 report (firewall policies, iptable commands, Nmap, and wireshark)
- Bryan Chinenye Muforo - Cisco firewall configuration/implementation, helped with ping and service testing, ran diagnostics on outside pc, general formatting for report, took screenshots from external computer.
- Kelby Webster - made ACM to represent security policy, ran zenmap quick/intense scans to determine devices & services on router, report introduction, task 2 screenshots, task 3 part a, b, d, & general layout/formatting
- Doohwan Yoon - configure firewall by the cisco configuration, testing ping and wireshark

****

Group Timeline:

- Thursday (2/13) - Doohwan & Bryan - Initial network/computer and checking network for Task I.
- Friday (2/14) - Randall - Initial network/computer login & configuration
- Thursday (2/20) - Trevor - Fixed network pings from internal and external. A different group had firewall policies blocking, and just had to delete their policies for the pings to work again.
- Friday (2/21) - Trevor & Kelby - Task II part 2 & 3: Checked internal/external web service requests with firewall on/off, and ran nMap quick/intense scans on all computers & services
- Friday (2/21) - Bryan & Randall - Initially open/configure Cisco firewall
- Monday (2/24) - Kelby - Created Access control matrix + graphic
- Thursday (2/27) - Whole group - met in lab but router was down & unable to use network for ~2 hours, reconfigured network gateway & able to continue
- Friday (2/28) - Randall, Trevor, and Bryan Finished tasks 3 and 4.

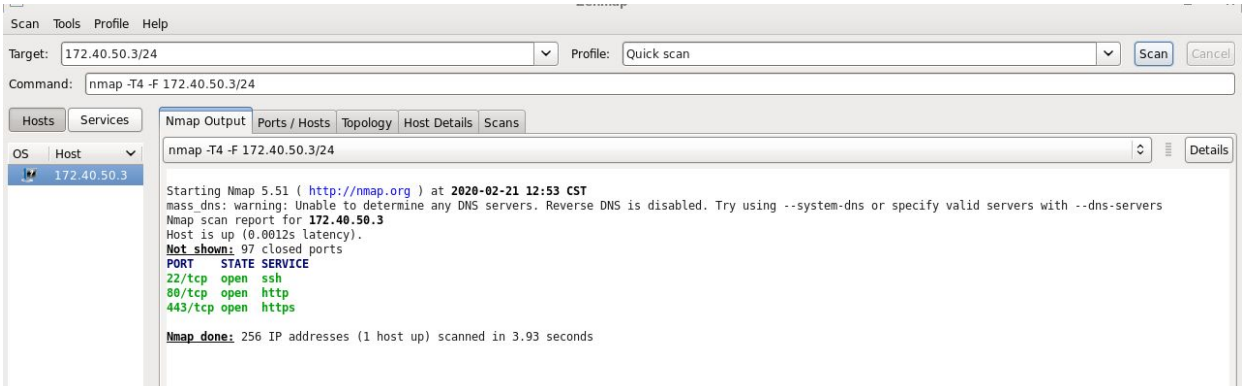
- March (3/2) - Kelby finished tasks 3 and 4 questions. She also formatted the report.

****

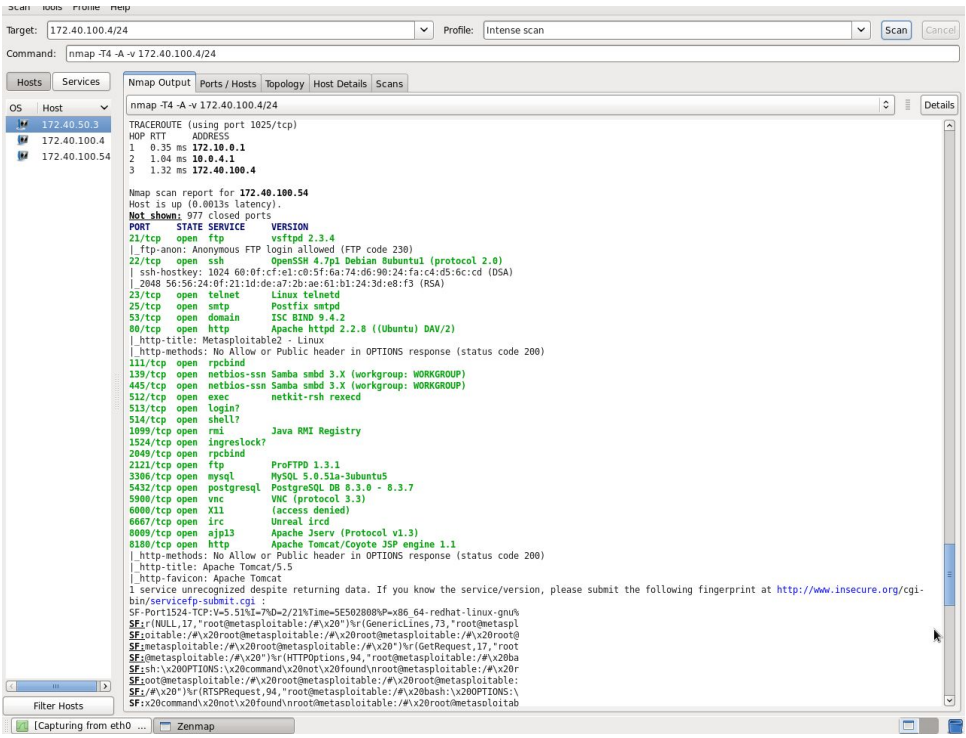
Section II (Task II): Default Cisco firewall policy & exploit testing

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

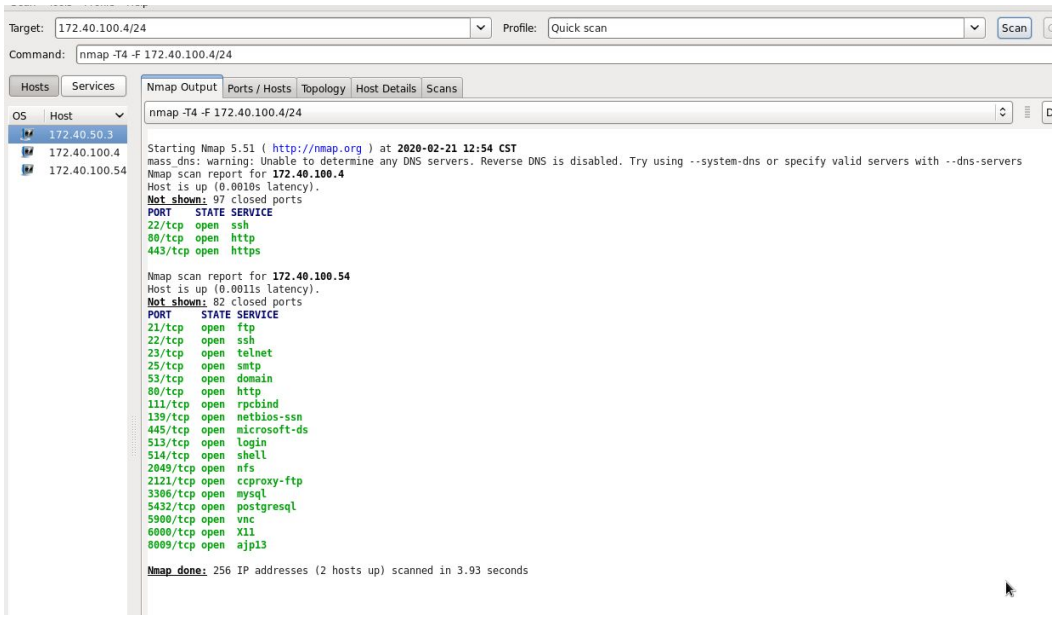
Scan 1: Type = Quick scan, Target = Computer D1 (172.40.50.3)



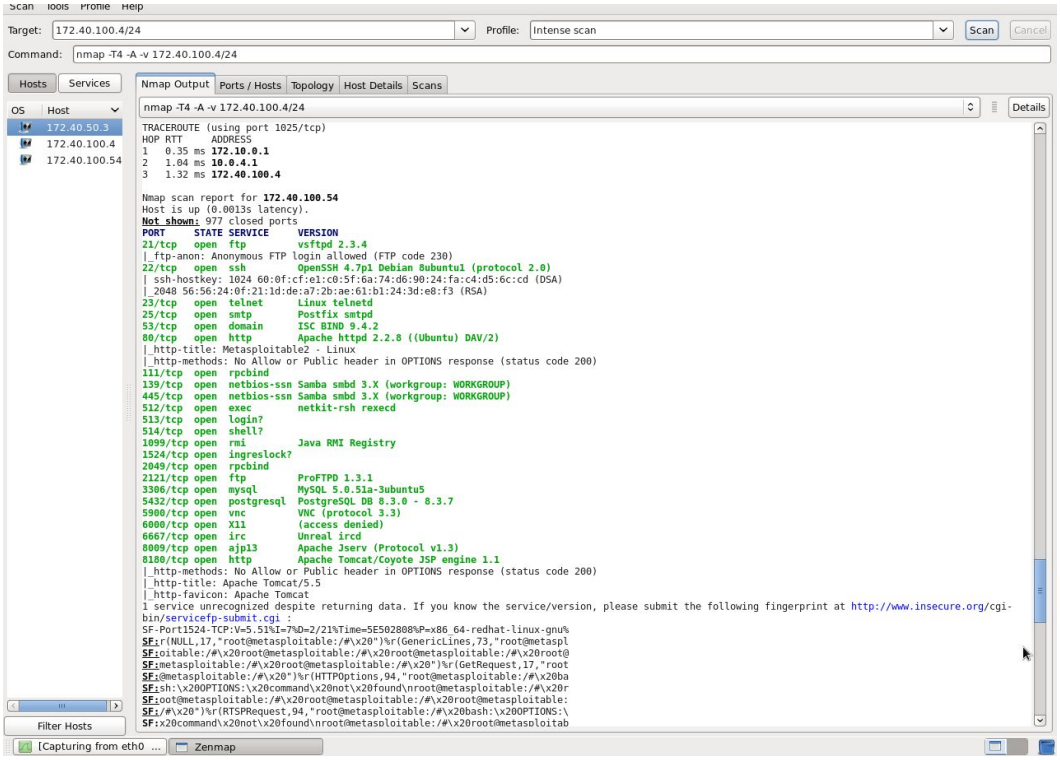
Scan 2: Type = Intense scan, Target = Computer D1 (172.40.50.3)



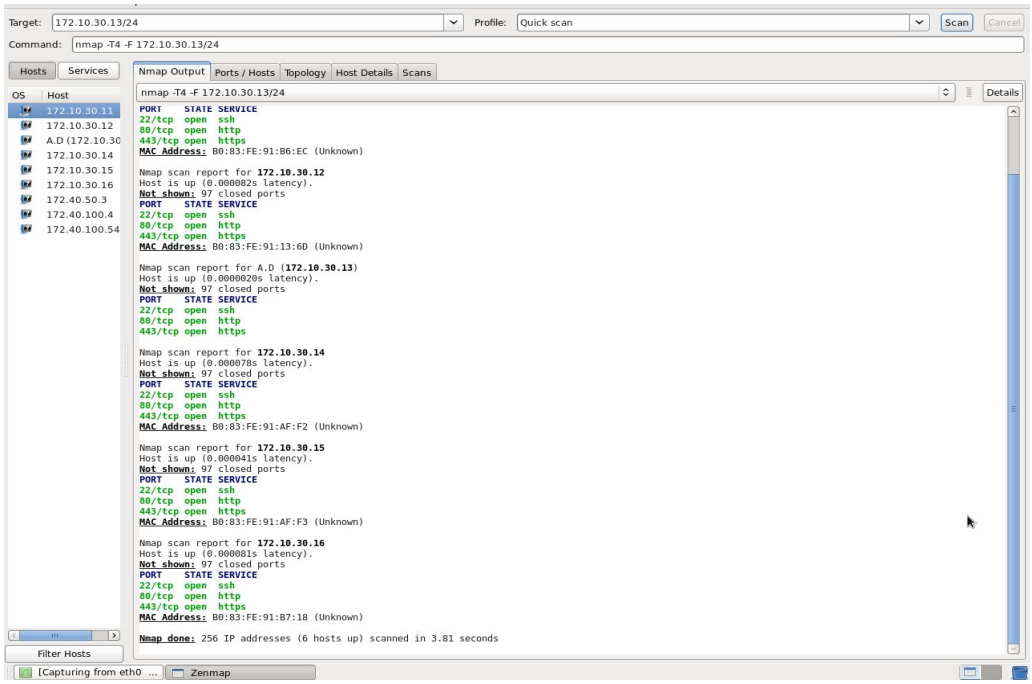
Scan 3: Type = Quick scan, Target = Computer D2 (172.40.100.4)



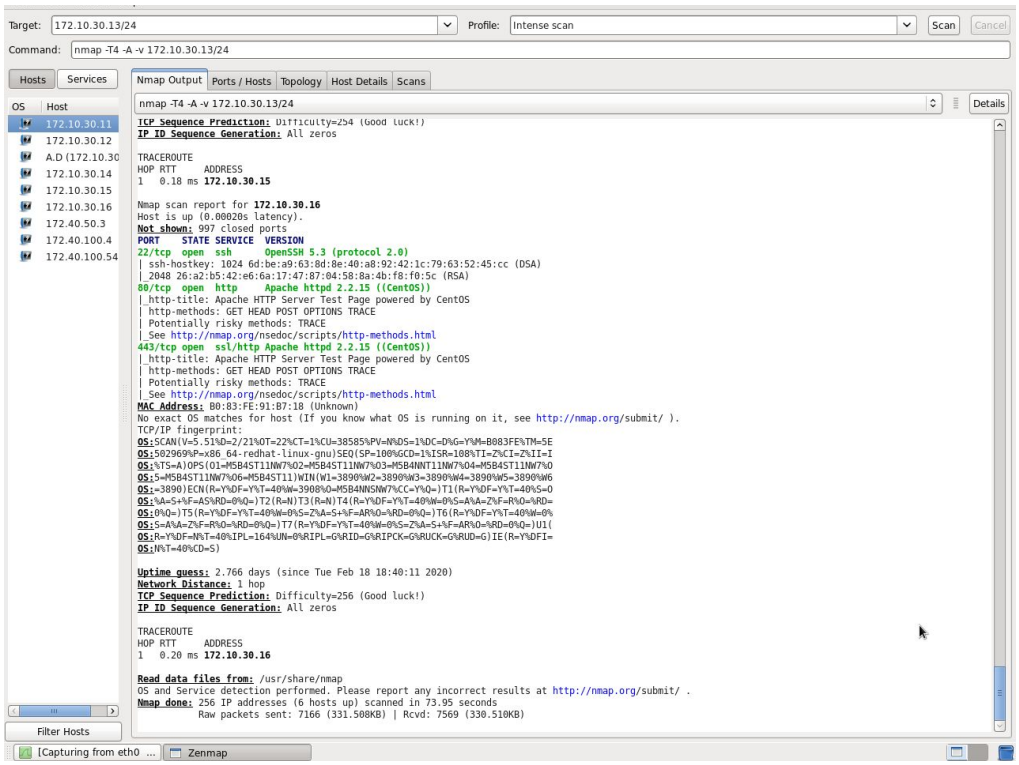
Scan 4: Type = Intense scan, Target = Computer D2 (172.40.100.4)



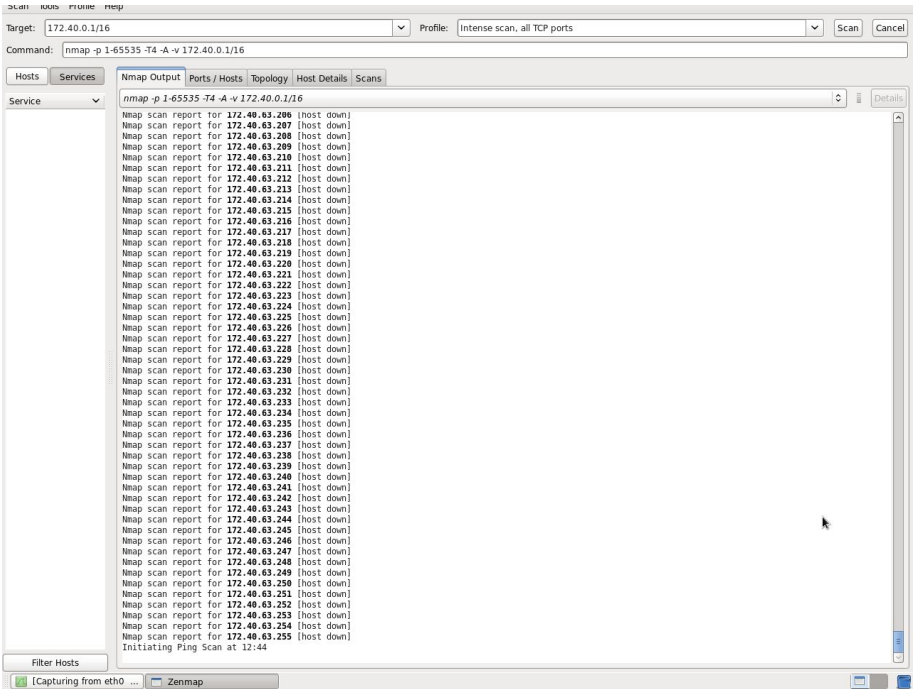
Scan 5: Type = Quick scan, Target = Computer A.D (172.10.30.13)



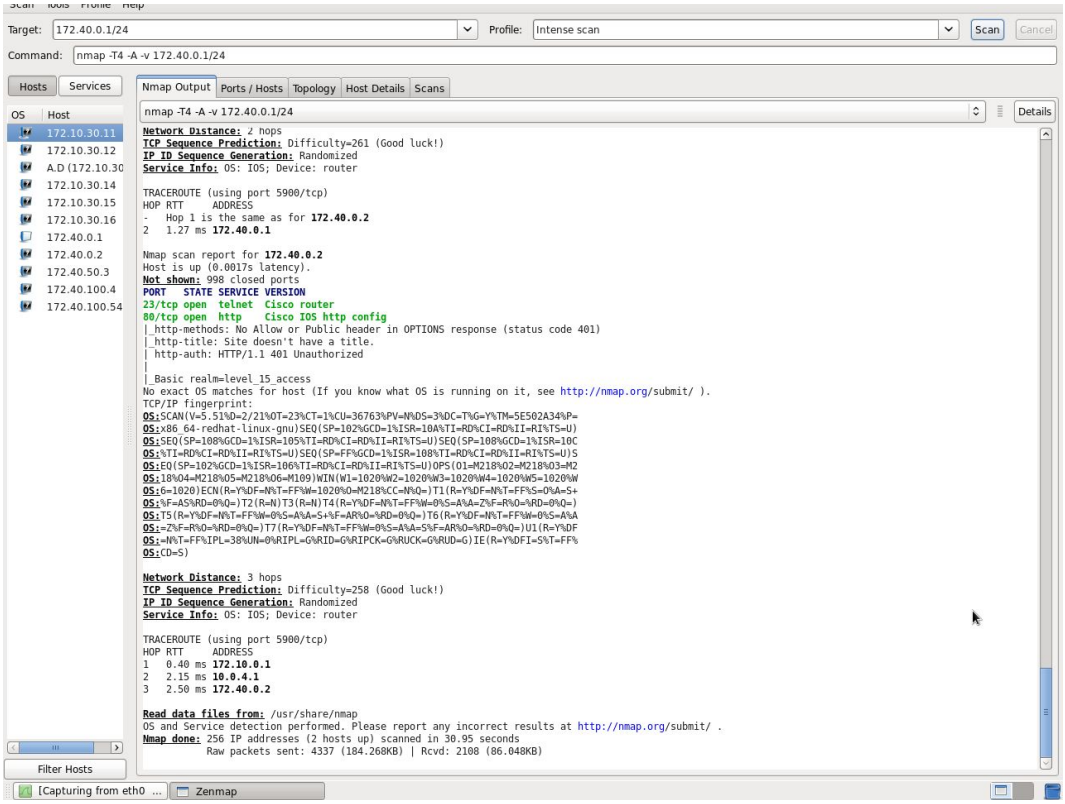
Scan 6: Type = Intense scan, Target = Computer A.D (172.10.30.13)



Scan 7: Type = TCP port scan, Target = Router D (172.40.0.1/16)

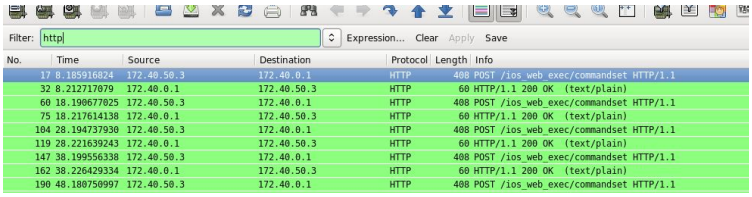


Scan 8: Type = Intense scan, Target = Router D (172.40.0.1/16)

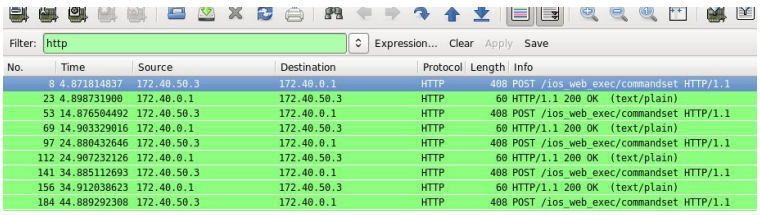


b) Show the Wireshark results (screen shots) of checking the web service between computers. State if web service is allowed between computers.

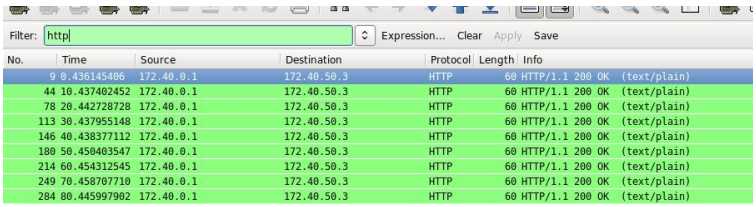
- D.1 accessing web service of A.D: web service is allowed



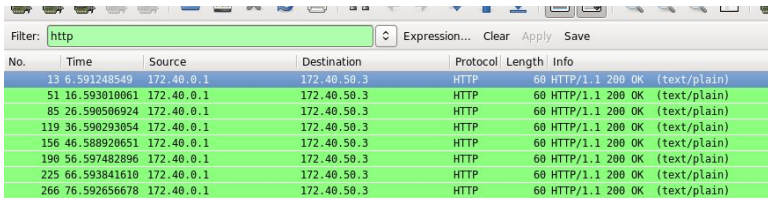
- D.1 accessing web service of D.2: web service is allowed



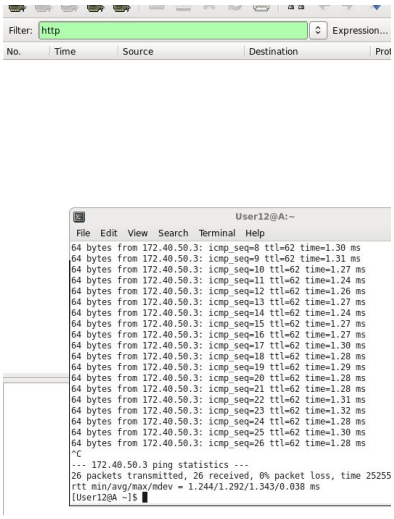
- D.2 accessing web service of A.D: web service is allowed



- D.2 accessing web service of D.1: web service is allowed



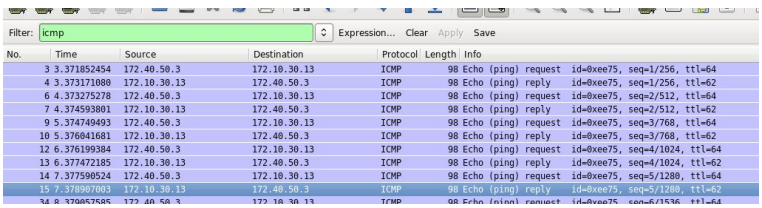
- A.D accessing web service of D.1: web service is NOT allowed



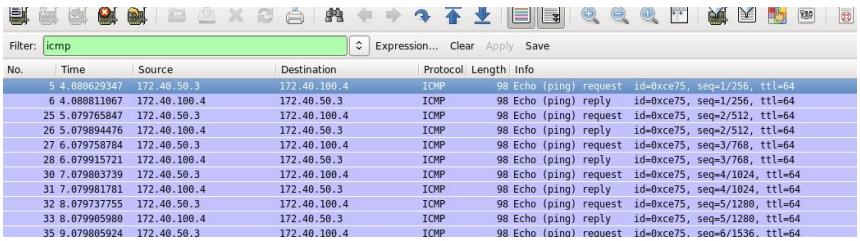
- A.D accessing web service of D.2: web service is NOT allowed

c) Show the Wireshark results (screen shots) of checking the ping between computers. State if ping is allowed between computers.

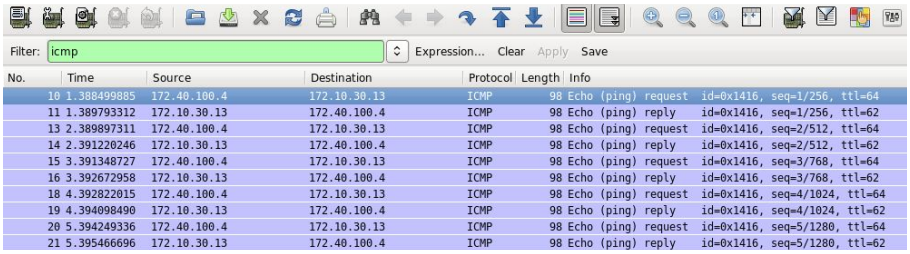
- D.1 ping A.D, ping allowed



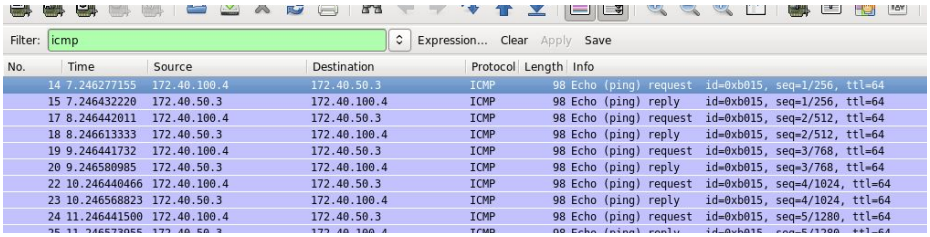
- D.1 ping D.2, ping allowed



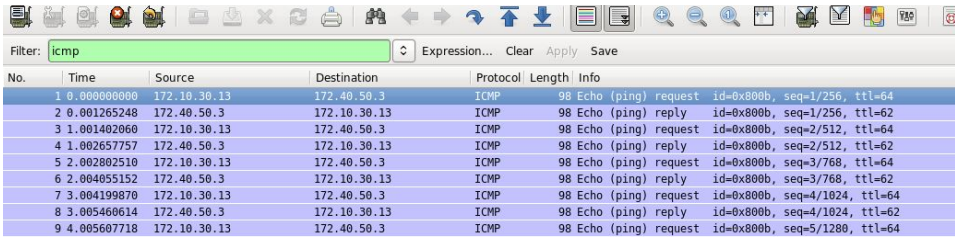
- D.2 ping A.D, ping allowed



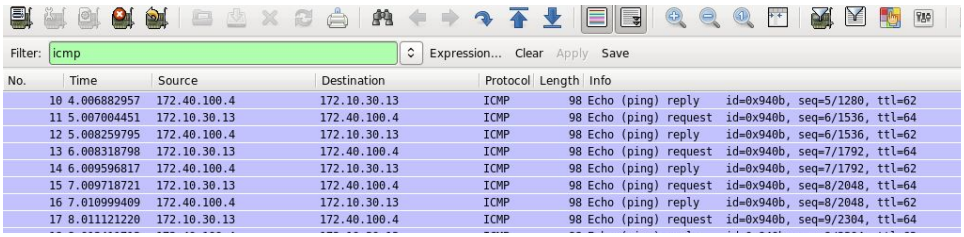
- D.2 ping D.1, ping allowed



- A.D ping D.1, ping allowed



- A.D ping D.2, ping allowed



d) Summarize the default Cisco firewall policy.

The default policy makes the computers which are on the internal network (D1 & D2) able to access each other's web services, in addition to the external network (A.D). Both computers on the internal network could ping each other as well as the computer which was on the external network. However, on the external network computer, we were unable to access web services or ping the computers on the internal network.

Section III (Task III): Implement security policy

a) Copy and paste the access control matrix.

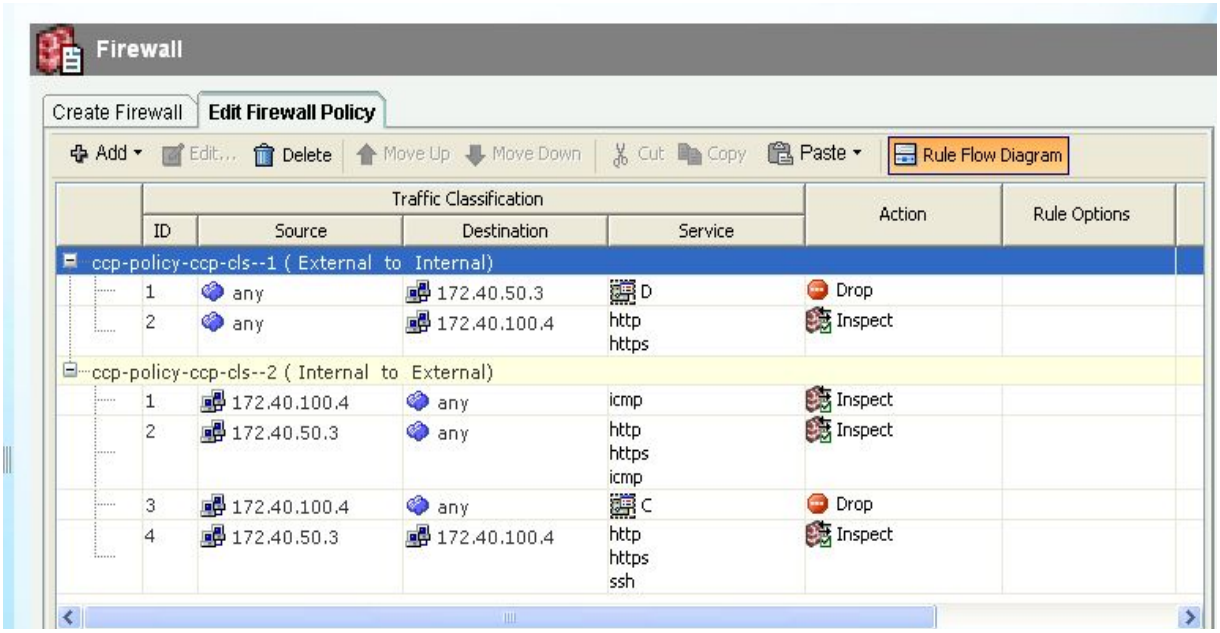
	Internal Server	Internal Workstation	External Computer
Internal Server	ping	ping	ping
Internal Workstation	Web, SSH, ping	ping	Web, ping
External Computer	web	N/A	N/A

b) Find and explain which policy cannot be enforced by the Cisco firewall and which policy can only partially be enforced by the Cisco firewall.

The Cisco firewall is unable to enforce policies that have to be implemented between the internal server & internal workstations. This is due to the fact that Cisco requires each new "zone" that is created to have a link to an existing interface. Both the

internal server and the internal workstations are in the same zone because they both are on the VLan. Any policy for a firewall does not allow us to put any rules inside the internal network because the configuration would be required between the internal and external zones, and our workstation & server are both internal, sharing a single interface.

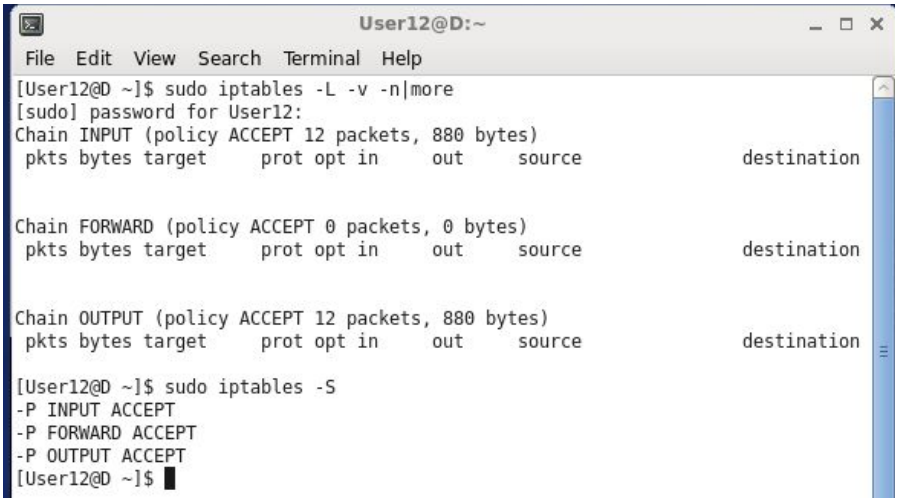
c) Copy and paste a screenshot of your Cisco firewall configuration.



d) Discuss how to use iptables to enforce the security policy that is not implemented in the Cisco firewall.

We have to use iptables between the internal workstation & the internal servers. This is because any Cisco firewall policy that is on the router cannot be enforced locally. For the internal workstation, other computers need to be blocked from using its web/SSH services. As for the internal server, other “outside” internal servers need to be blocked from using its web/SSH services as well.

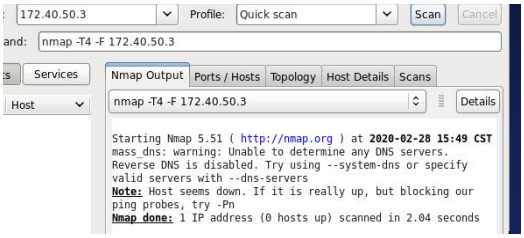
e) Show the iptables commands in the internal server that enforce the security policy that is not implemented in the Cisco firewall.



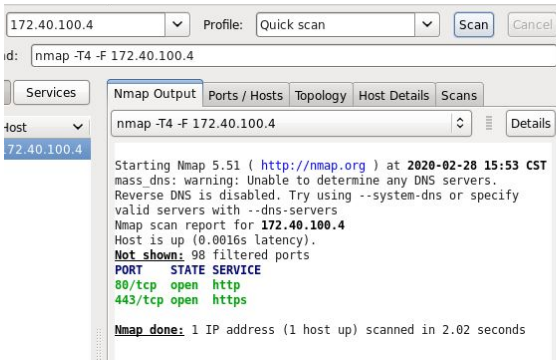
Section IV (Task IV): Test the implementation of the security policy

a) Show the NMap results (screenshots) of the exposed computers and ports.

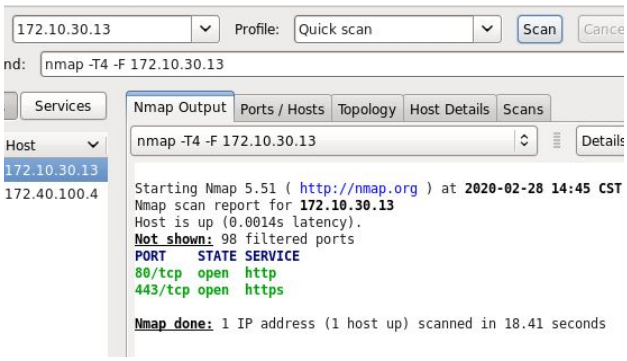
- A.D to D.1:



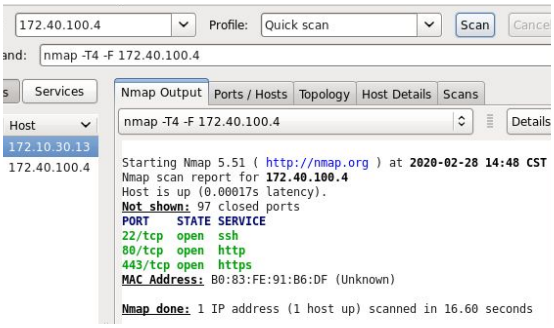
- A.D to D.2:



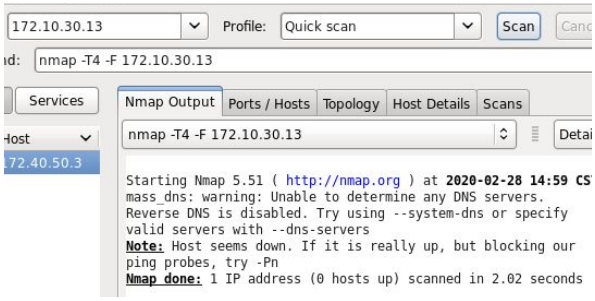
- D.1 to A.D:



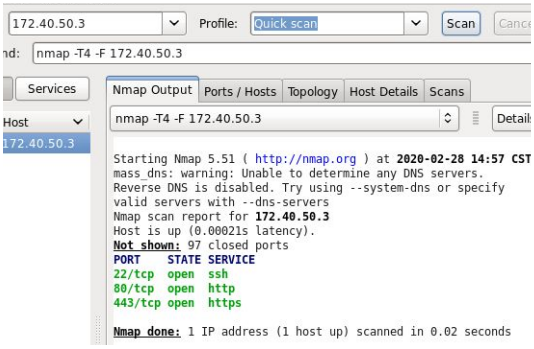
- D.1 to D.2:



- D.2 to A.D:

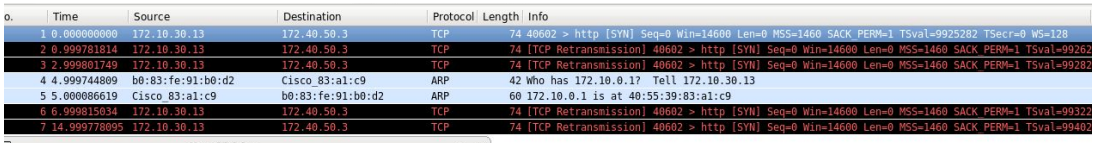


- D.2 to D.1:

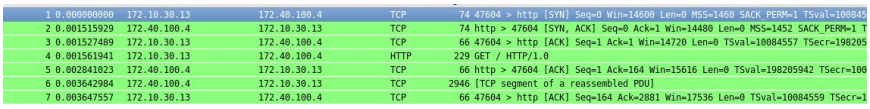


b) Show the Wireshark results (screen shots) of checking the web service between computers. State if web service is allowed between computers.

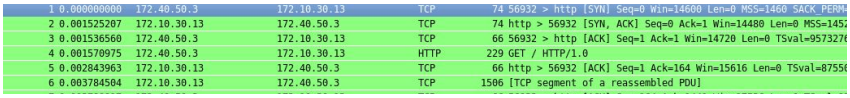
- A.D to D.1: Web service allowed? NO



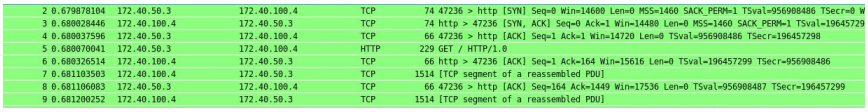
- A.D to D.2: Web service allowed? YES



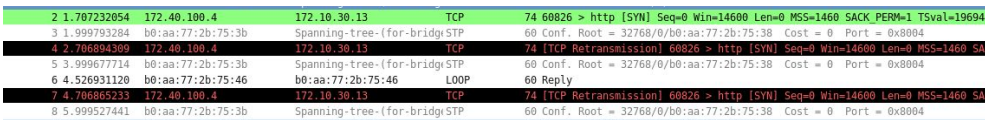
- D.1 to A.D: Web service allowed? YES



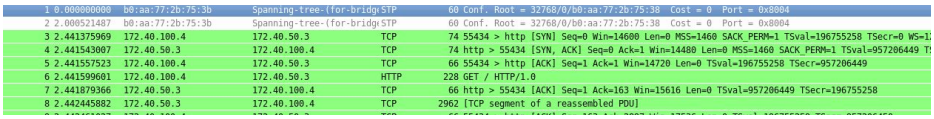
- D.1 to D.2: Web service allowed? YES



- D.2 to A.D: Web service allowed? NO



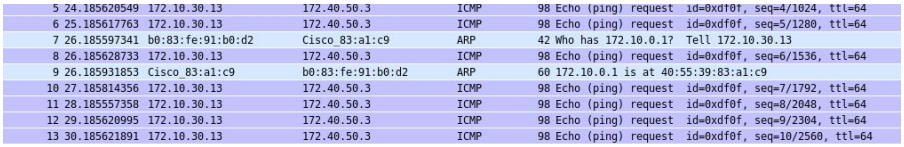
- D.2 to D.1: Web service allowed? YES



1	0.000000000	b0:aa:77:2b:75:3b	Spanning-tree-(for-bridge	STP	60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8004
2	2.000521487	b0:aa:77:2b:75:3b	Spanning-tree-(for-bridge	STP	60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8004
3	2.441375969	172.40.100.4	172.40.50.3	TCP	74 55434 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=196755258 TSecr=0 WS=1
4	2.441543007	172.40.50.3	172.40.100.4	TCP	74 http > 55434 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=957206449 T
5	2.441557523	172.40.100.4	172.40.50.3	TCP	66 55434 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=196755258 TSecr=957206449
6	2.441599601	172.40.100.4	172.40.50.3	HTTP	228 GET / HTTP/1.0
7	2.441879366	172.40.50.3	172.40.100.4	TCP	66 http > 55434 [ACK] Seq=1 Ack=163 Win=15616 Len=0 TSval=957206449 TSecr=196755258
8	2.442445882	172.40.50.3	172.40.100.4	TCP	2962 [TCP segment of a reassembled PDU]

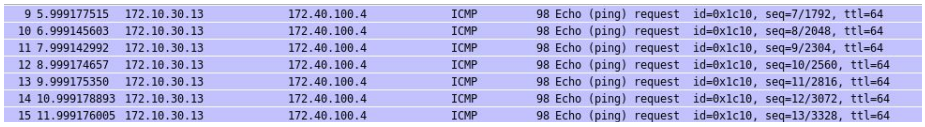
c) Show the Wireshark results (screen shots) of checking the ping between computers. State if ping is allowed between computers.

- A.D to D.1: Ping allowed? NO



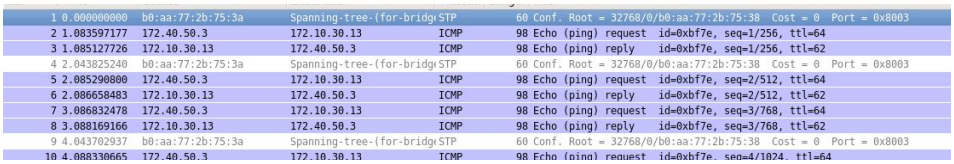
5	24.185620549	172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xdf0f, seq=4/1024, ttl=64
6	25.185617763	172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xdf0f, seq=5/1280, ttl=64
7	26.185597341	b0:83:fe:91:b0:d2	Cisco_83:a1:c9	ARP	42 Who has 172.10.0.1? Tell 172.10.30.13
8	26.185628733	172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xdf0f, seq=6/1536, ttl=64
9	26.185931853	Cisco_83:a1:c9	b0:83:fe:91:b0:d2	ARP	60 172.10.0.1 is at 40:55:39:83:a1:c9
10	27.185814356	172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xdf0f, seq=7/1792, ttl=64
11	28.185557358	172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xdf0f, seq=8/2048, ttl=64
12	29.185620995	172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xdf0f, seq=9/2304, ttl=64
13	30.185621891	172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xdf0f, seq=10/2560, ttl=64

- A.D to D.2: Ping allowed? NO



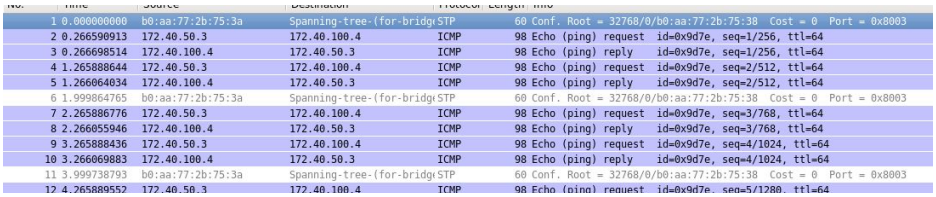
9	5.999177515	172.10.30.13	172.40.100.4	ICMP	98 Echo (ping) request id=0x1c10, seq=7/1792, ttl=64
10	6.999145603	172.10.30.13	172.40.100.4	ICMP	98 Echo (ping) request id=0x1c10, seq=8/2048, ttl=64
11	7.999142992	172.10.30.13	172.40.100.4	ICMP	98 Echo (ping) request id=0x1c10, seq=9/2304, ttl=64
12	8.999174657	172.10.30.13	172.40.100.4	ICMP	98 Echo (ping) request id=0x1c10, seq=10/2560, ttl=64
13	9.999175350	172.10.30.13	172.40.100.4	ICMP	98 Echo (ping) request id=0x1c10, seq=11/2816, ttl=64
14	10.999178893	172.10.30.13	172.40.100.4	ICMP	98 Echo (ping) request id=0x1c10, seq=12/3072, ttl=64
15	11.999176005	172.10.30.13	172.40.100.4	ICMP	98 Echo (ping) request id=0x1c10, seq=13/3328, ttl=64

- D.1 to A.D: Ping allowed? YES



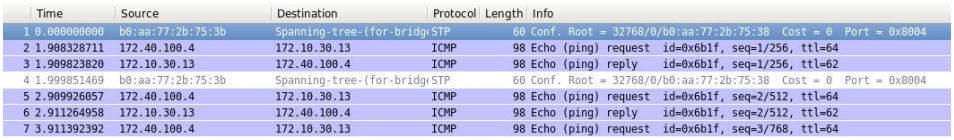
1	0.000000000	b0:aa:77:2b:75:3a	Spanning-tree-(for-bridge	STP	60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8003
2	1.083597177	172.40.50.3	172.10.30.13	ICMP	98 Echo (ping) request id=0xbf7e, seq=1/256, ttl=64
3	1.085127726	172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) reply id=0xbf7e, seq=1/256, ttl=62
4	2.043825240	b0:aa:77:2b:75:3a	Spanning-tree-(for-bridge	STP	60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8003
5	2.085290800	172.40.50.3	172.10.30.13	ICMP	98 Echo (ping) request id=0xbf7e, seq=2/512, ttl=64
6	2.086658483	172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) reply id=0xbf7e, seq=2/512, ttl=62
7	3.086832478	172.40.50.3	172.10.30.13	ICMP	98 Echo (ping) request id=0xbf7e, seq=3/768, ttl=64
8	3.088169166	172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) reply id=0xbf7e, seq=3/768, ttl=62
9	4.043702937	b0:aa:77:2b:75:3a	Spanning-tree-(for-bridge	STP	60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8003
10	4.088330665	172.40.50.3	172.10.30.13	ICMP	98 Echo (ping) request id=0xbf7e, seq=4/1024, ttl=64

- D.1 to D.2: Ping allowed? YES



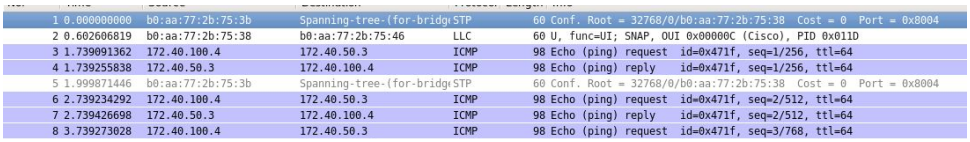
1	0.000000000	b0:aa:77:2b:75:3a	Spanning-tree-(for-bridge	STP	60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8003
2	0.266590913	172.40.50.3	172.40.100.4	ICMP	98 Echo (ping) request id=0x9d7e, seq=1/256, ttl=64
3	0.266698514	172.40.100.4	172.40.50.3	ICMP	98 Echo (ping) reply id=0x9d7e, seq=1/256, ttl=64
4	1.265888644	172.40.50.3	172.40.100.4	ICMP	98 Echo (ping) request id=0x9d7e, seq=2/512, ttl=64
5	1.266064034	172.40.100.4	172.40.50.3	ICMP	98 Echo (ping) reply id=0x9d7e, seq=2/512, ttl=64
6	1.999864765	b0:aa:77:2b:75:3a	Spanning-tree-(for-bridge	STP	60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8003
7	2.265886776	172.40.50.3	172.40.100.4	ICMP	98 Echo (ping) request id=0x9d7e, seq=3/768, ttl=64
8	2.266055946	172.40.100.4	172.40.50.3	ICMP	98 Echo (ping) reply id=0x9d7e, seq=3/768, ttl=64
9	3.265888436	172.40.50.3	172.40.100.4	ICMP	98 Echo (ping) request id=0x9d7e, seq=4/1024, ttl=64
10	3.266069883	172.40.100.4	172.40.50.3	ICMP	98 Echo (ping) reply id=0x9d7e, seq=4/1024, ttl=64
11	3.999738793	b0:aa:77:2b:75:3a	Spanning-tree-(for-bridge	STP	60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8003
12	4.265889552	172.40.50.3	172.40.100.4	ICMP	98 Echo (ping) request id=0x9d7e, seq=5/1280, ttl=64

- D.2 to A.D: Ping allowed? YES



	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	b0:aa:77:2b:75:3b	Spanning-tree-(for-bridge	STP		60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8004
2	1.908328711	172.40.100.4	172.10.30.13	ICMP		98 Echo (ping) request id=0x6b1f, seq=1/256, ttl=64
3	1.909823820	172.10.30.13	172.40.100.4	ICMP		98 Echo (ping) reply id=0x6b1f, seq=1/256, ttl=62
4	1.999851469	b0:aa:77:2b:75:3b	Spanning-tree-(for-bridge	STP		60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8004
5	2.909926057	172.40.100.4	172.10.30.13	ICMP		98 Echo (ping) request id=0x6b1f, seq=2/512, ttl=64
6	2.911264958	172.10.30.13	172.40.100.4	ICMP		98 Echo (ping) reply id=0x6b1f, seq=2/512, ttl=62
7	3.911392392	172.40.100.4	172.10.30.13	ICMP		98 Echo (ping) request id=0x6b1f, seq=3/768, ttl=64

- D.2 to D.1: Ping allowed? YES



1	0.000000000	b0:aa:77:2b:75:3b	Spanning-tree-(for-bridg	STP	60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8004
2	0.602606819	b0:aa:77:2b:75:38	b0:aa:77:2b:75:46	LLC	60 U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x011D
3	1.739091362	172.40.100.4	172.40.50.3	ICMP	98 Echo (ping) request id=0x471f, seq=1/256, ttl=64
4	1.739255838	172.40.50.3	172.40.100.4	ICMP	98 Echo (ping) reply id=0x471f, seq=1/256, ttl=64
5	1.999871446	b0:aa:77:2b:75:3b	Spanning-tree-(for-bridg	STP	60 Conf. Root = 32768/0/b0:aa:77:2b:75:38 Cost = 0 Port = 0x8004
6	2.739234292	172.40.100.4	172.40.50.3	ICMP	98 Echo (ping) request id=0x471f, seq=2/512, ttl=64
7	2.739426698	172.40.50.3	172.40.100.4	ICMP	98 Echo (ping) reply id=0x471f, seq=2/512, ttl=64
8	3.739273028	172.40.100.4	172.40.50.3	ICMP	98 Echo (ping) request id=0x471f, seq=3/768, ttl=64

d) Assume the company only stores classified business data in Computer B.1, & does not allow anyone to carry a device to transfer data. Discuss whether or not 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 what policy is missing.

There is a vulnerability created by the internal servers providing web services to the external computers. This type of security policy would not be able to ensure that the classified business data will not be available to external computers found on the network. Only the transport layer is accessible, instead of looking deeper to the application layer. The policy is flawed in the sense that data is secured only by the computer & people able to access it. Therefore if it is the only policy the business uses, it would be easy for someone to find something within the system & exploit/extract classified information.