

**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 Chineneye 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 Chinene 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:

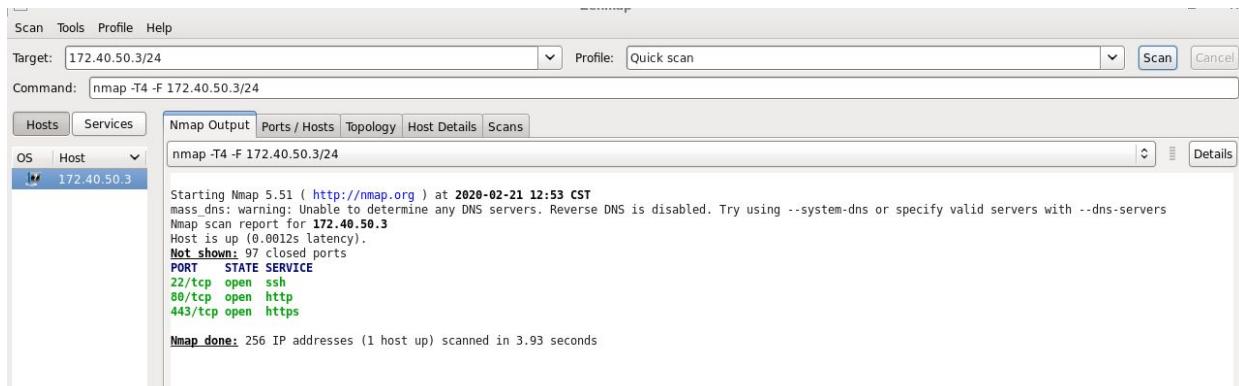
- Thursday (2/13) - Doohwan & Bryan - Initial network/computer and checking network for Task I.
- Friday (2/14) - Randall - Initial network/computer login & configuration
- Thursday (2/20) - Trevor - Fixed network pings from internal and external. A different group had firewall policies blocking, and 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.

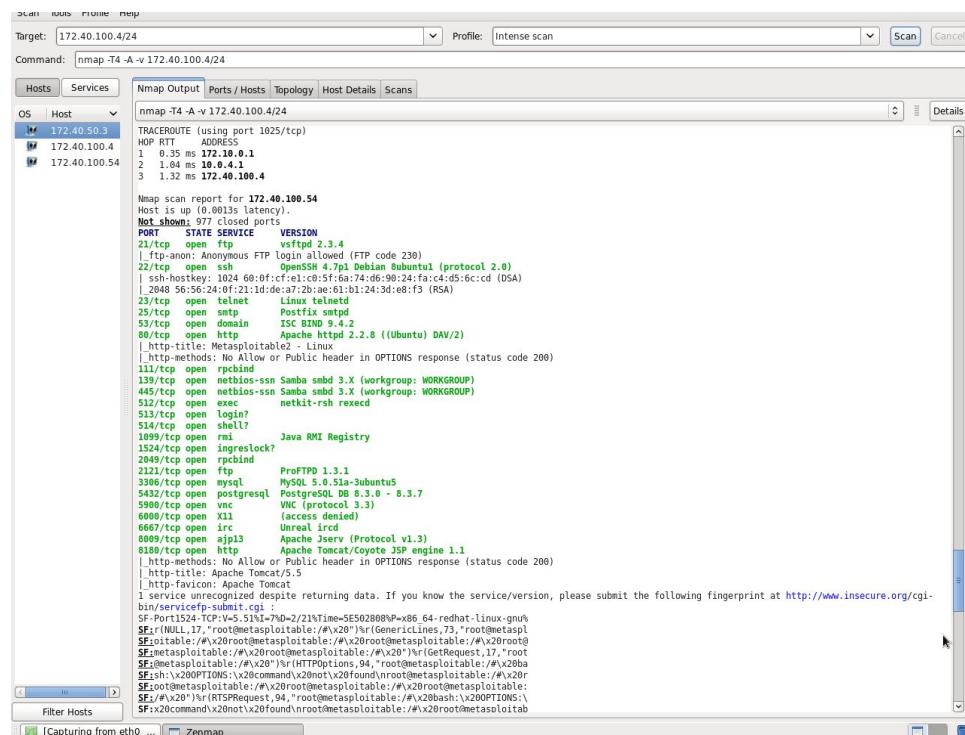
## **Section II (Task II): Default Cisco firewall policy & exploit testing**

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)



CS 4371 - COMPUTER SECURITY (Project 1)

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

The screenshot shows the Nmap interface with the following details:

- Target:** 172.40.100.4/24
- Profile:** Quick scan
- Command:** nmap -T4 -F 172.40.100.4/24
- Hosts:** OS | Host | 172.40.50.3 | 172.40.100.4 | 172.40.100.54
- Services:** Nmap Output | Ports / Hosts | Topology | Host Details | Scans | Scan
- Scan Results for 172.40.100.4:**
  - Starting Nmap 5.51 ( http://nmap.org ) at 2020-02-21 12:54 CST
  - mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
  - Nmap scan report for **172.40.100.4**
  - Host is up [0.0010s latency].
  - Not shown:** 97 closed ports
  - PORT STATE SERVICE**
  - 22/tcp open ssh
  - 80/tcp open http
  - 443/tcp open https
- Scan Results for 172.40.100.54:**
  - Starting Nmap 5.51 ( http://nmap.org ) at 2020-02-21 12:54 CST
  - Host is up [0.0011s latency].
  - Not shown:** 82 closed ports
  - PORT STATE SERVICE**
  - 21/tcp open ftp
  - 22/tcp open ssh
  - 23/tcp open telnet
  - 25/tcp open smtp
  - 53/tcp open domain
  - 80/tcp open http
  - 111/tcp open sunrpc
  - 139/tcp open netbios-ssn
  - 445/tcp open microsoft-ds
  - 513/tcp open login
  - 514/tcp open shell
  - 2049/tcp open nfs
  - 2121/tcp open cccproxy-ftp
  - 3306/tcp open mysql
  - 5432/tcp open postgresql
  - 5900/tcp open vnc
  - 6000/tcp open X11
  - 8089/tcp open ajp13
- Nmap done:** 256 IP addresses (2 hosts up) scanned in 3.93 seconds

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

The screenshot shows the Zmap application window with the following details:

- Target:** 172.40.100.4/24
- Profile:** Intense scan
- Command:** nmap -T4 -A -v 172.40.100.4/24

The results tab displays the Nmap output for the target host 172.40.100.54. The output includes:

- OS:** Linux 4.15.0-102-generic
- Host:** 172.40.100.54
- Ports:** 22/tcp (ssh), 25/tcp (smtp), 80/tcp (http), 443/tcp (https)
- Services:** OpenSSH 4.7p1 Debian Buntu1 (protocol 2.0), Postfix smtpd, Apache httpd 2.2.8 ((Ubuntu) DAV/2)
- Versions:** Apache/2.2.8 PHP/7.2.14 (Ubuntu)
- State:** Up (0.0013s latency).
- Reason:** Connection established.
- Scans:** Intense scan.

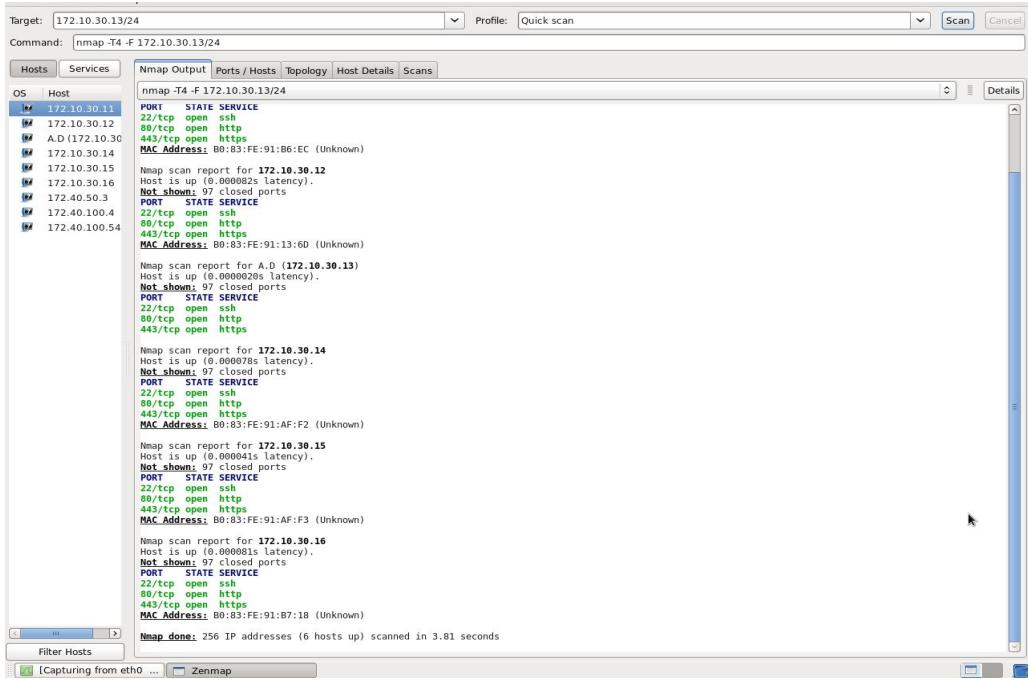
The detailed output shows various ports and services, including:

- 22/tcp open ssh OpenSSH 4.7p1 Debian Buntu1 (protocol 2.0)
- 25/tcp open smtp Postfix smtpd
- 80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
- 443/tcp open https Apache/2.2.8 PHP/7.2.14 (Ubuntu)
- 139/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
- 445/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
- 512/tcp open exec netkit-rsh rexecd
- 513/tcp open login?
- 514/tcp open shell?
- 1099/tcp open java-rmi Java RMI Registry
- 1524/tcp open ingreslock?
- 2049/tcp open rpcbind
- 2121/tcp open ftp ProFTPD 1.3.1
- 3386/tcp open mysql MySQL 5.0.51a-3ubuntu5
- 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
- 5900/tcp open vnc VNC (protocol 3.3)
- 6000/tcp open x11 (access denied)
- 6667/tcp open irc Unreal ircd
- 8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
- 8180/tcp open httpd Apache Tomcat/Coyote JSP engine 1.1

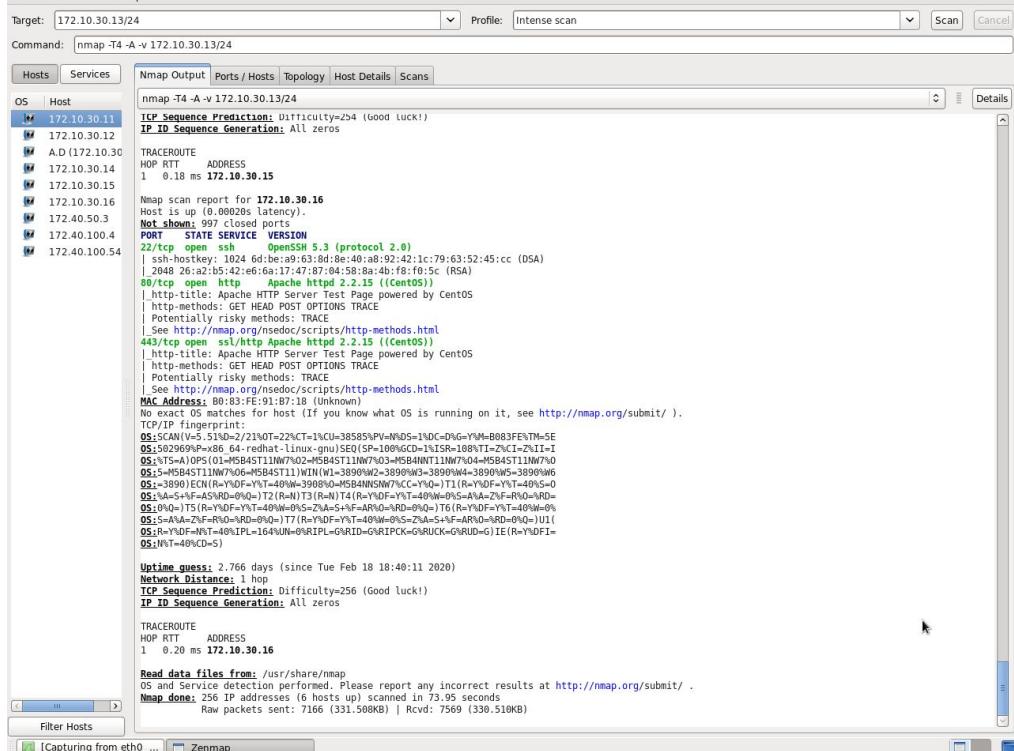
The output also includes a service recognition section and a note about reporting findings to <http://www.insecure.org/cgi-bin/servicefp-submit.cgi>.

CS 4371 - COMPUTER SECURITY (Project 1)

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

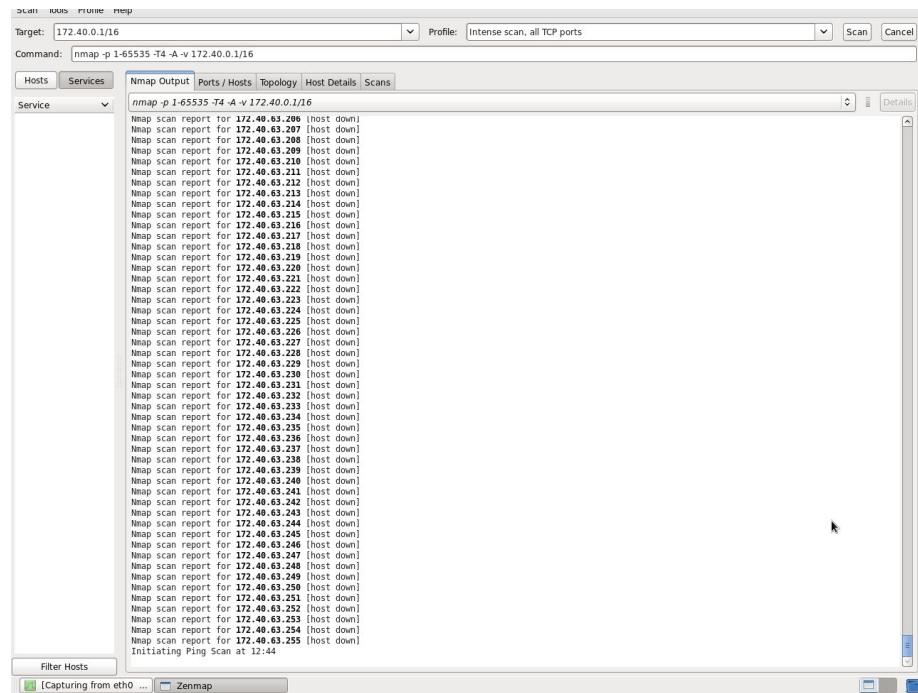


Scan 6: Type = Intense scan, Target = Computer A.D (172.10.30.13)

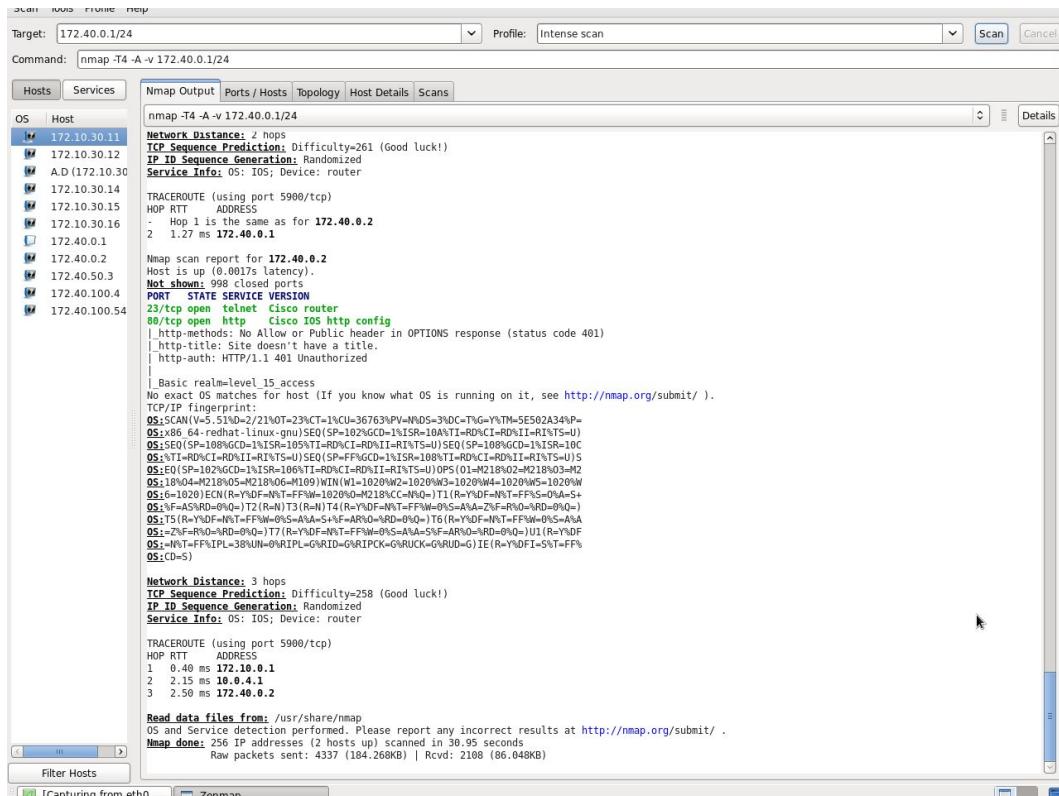


CS 4371 - COMPUTER SECURITY (Project 1)

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

No.	Time	Source	Destination	Protocol	Length	Info
17	8.185916824	172.40.50.3	172.40.0.1	HTTP	408	POST /ios_web_exec/commandset HTTP/1.1
32	8.212717079	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
60	18.198677825	172.40.50.3	172.40.0.1	HTTP	408	POST /ios_web_exec/commandset HTTP/1.1
75	18.217614138	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
104	28.194737939	172.40.50.3	172.40.0.1	HTTP	408	POST /ios_web_exec/commandset HTTP/1.1
119	28.221639243	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
147	38.19956338	172.40.50.3	172.40.0.1	HTTP	408	POST /ios_web_exec/commandset HTTP/1.1
162	38.226429334	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
190	48.188758997	172.40.50.3	172.40.0.1	HTTP	408	POST /ios_web_exec/commandset HTTP/1.1

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

No.	Time	Source	Destination	Protocol	Length	Info
8	4.871814837	172.40.50.3	172.40.0.1	HTTP	408	POST /ios_web_exec/commandset HTTP/1.1
23	4.898731908	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
53	14.876504492	172.40.50.3	172.40.0.1	HTTP	408	POST /ios_web_exec/commandset HTTP/1.1
69	14.903329016	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
97	24.880432646	172.40.50.3	172.40.0.1	HTTP	408	POST /ios_web_exec/commandset HTTP/1.1
112	24.987232126	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
141	34.885112693	172.40.50.3	172.40.0.1	HTTP	408	POST /ios_web_exec/commandset HTTP/1.1
156	34.912038623	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
184	44.889292308	172.40.50.3	172.40.0.1	HTTP	408	POST /ios_web_exec/commandset HTTP/1.1

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

No.	Time	Source	Destination	Protocol	Length	Info
9	0.436145406	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
44	10.437462452	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
78	20.442728728	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
113	30.437955148	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
146	40.438377112	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
188	50.450463547	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
214	60.454312545	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
249	70.458707718	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
284	80.445997992	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)

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

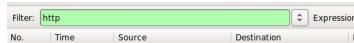
No.	Time	Source	Destination	Protocol	Length	Info
13	6.591248549	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
51	16.593010861	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
85	26.5909506924	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
119	36.590239054	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
156	46.588926051	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
190	56.597482896	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
225	66.593841610	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)
266	76.592656678	172.40.0.1	172.40.50.3	HTTP	68	HTTP/1.1 200 OK (text/plain)

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



```
User12@A:~  
File Edit View Search Terminal Help  
64 bytes from 172.40.50.3: icmp seq=8 ttl=62 time=1.30 ms  
64 bytes from 172.40.50.3: icmp seq=9 ttl=62 time=1.31 ms  
64 bytes from 172.40.50.3: icmp seq=10 ttl=62 time=1.27 ms  
64 bytes from 172.40.50.3: icmp seq=11 ttl=62 time=1.24 ms  
64 bytes from 172.40.50.3: icmp seq=12 ttl=62 time=1.26 ms  
64 bytes from 172.40.50.3: icmp seq=13 ttl=62 time=1.27 ms  
64 bytes from 172.40.50.3: icmp seq=14 ttl=62 time=1.24 ms  
64 bytes from 172.40.50.3: icmp seq=15 ttl=62 time=1.27 ms  
64 bytes from 172.40.50.3: icmp seq=16 ttl=62 time=1.27 ms  
64 bytes from 172.40.50.3: icmp seq=17 ttl=62 time=1.29 ms  
64 bytes from 172.40.50.3: icmp seq=18 ttl=62 time=1.28 ms  
64 bytes from 172.40.50.3: icmp seq=19 ttl=62 time=1.29 ms  
64 bytes from 172.40.50.3: icmp seq=20 ttl=62 time=1.28 ms  
64 bytes from 172.40.50.3: icmp seq=21 ttl=62 time=1.29 ms  
64 bytes from 172.40.50.3: icmp seq=22 ttl=62 time=1.31 ms  
64 bytes from 172.40.50.3: icmp seq=23 ttl=62 time=1.32 ms  
64 bytes from 172.40.50.3: icmp seq=24 ttl=62 time=1.28 ms  
64 bytes from 172.40.50.3: icmp seq=25 ttl=62 time=1.30 ms  
64 bytes from 172.40.50.3: icmp seq=26 ttl=62 time=1.28 ms  
"  
... 172.40.50.3 ping statistics ...  
26 packets transmitted, 26 received, 0% packet loss, time 25255 ms  
rtt min/avg/max/mdev = 1.244/1.292/1.343/0.038 ms  
[User12@A ~]
```

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



```
User12@A:~  
File Edit View Search Terminal Help  
64 bytes from 172.40.100.4: icmp seq=4 ttl=62 time=1.32 ms  
64 bytes from 172.40.100.4: icmp seq=5 ttl=62 time=1.32 ms  
64 bytes from 172.40.100.4: icmp seq=6 ttl=62 time=1.32 ms  
64 bytes from 172.40.100.4: icmp seq=7 ttl=62 time=1.29 ms  
64 bytes from 172.40.100.4: icmp seq=8 ttl=62 time=1.29 ms  
64 bytes from 172.40.100.4: icmp seq=9 ttl=62 time=1.32 ms  
64 bytes from 172.40.100.4: icmp seq=10 ttl=62 time=1.32 ms  
64 bytes from 172.40.100.4: icmp seq=11 ttl=62 time=1.29 ms  
64 bytes from 172.40.100.4: icmp seq=12 ttl=62 time=1.30 ms  
64 bytes from 172.40.100.4: icmp seq=13 ttl=62 time=1.27 ms  
64 bytes from 172.40.100.4: icmp seq=14 ttl=62 time=1.26 ms  
64 bytes from 172.40.100.4: icmp seq=15 ttl=62 time=1.33 ms  
64 bytes from 172.40.100.4: icmp seq=16 ttl=62 time=1.33 ms  
64 bytes from 172.40.100.4: icmp seq=17 ttl=62 time=1.34 ms  
64 bytes from 172.40.100.4: icmp seq=18 ttl=62 time=1.28 ms  
64 bytes from 172.40.100.4: icmp seq=19 ttl=62 time=1.27 ms  
64 bytes from 172.40.100.4: icmp seq=20 ttl=62 time=1.28 ms  
64 bytes from 172.40.100.4: icmp seq=21 ttl=62 time=1.28 ms  
64 bytes from 172.40.100.4: icmp seq=22 ttl=62 time=1.29 ms  
"  
... 172.40.100.4 ping statistics ...  
22 packets transmitted, 22 received, 0% packet loss, time 2138 ms  
rtt min/avg/max/mdev = 1.263/1.304/1.344/0.042 ms  
[User12@A ~]
```

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

No.	Time	Source	Destination	Protocol	Length	Info
3	3.371852454	172.40.50.3	172.10.30.13	ICMP	64	98 Echo (ping) request id=0xe0e75, seq=1/256, ttl=64
4	3.373171080	172.10.30.13	172.40.50.3	ICMP	64	98 Echo (ping) reply id=0xe0e75, seq=1/256, ttl=62
6	4.373275276	172.40.50.3	172.10.30.13	ICMP	64	98 Echo (ping) request id=0xe0e75, seq=2/512, ttl=64
7	4.374593801	172.10.30.13	172.40.50.3	ICMP	64	98 Echo (ping) reply id=0xe0e75, seq=2/512, ttl=62
9	5.374749493	172.40.50.3	172.10.30.13	ICMP	64	98 Echo (ping) request id=0xe0e75, seq=3/768, ttl=64
10	5.376041681	172.10.30.13	172.40.50.3	ICMP	64	98 Echo (ping) reply id=0xe0e75, seq=3/768, ttl=62
12	6.376199384	172.40.50.3	172.10.30.13	ICMP	64	98 Echo (ping) request id=0xe0e75, seq=4/1024, ttl=64
13	6.377472185	172.10.30.13	172.40.50.3	ICMP	64	98 Echo (ping) reply id=0xe0e75, seq=4/1024, ttl=62
14	7.377590524	172.40.50.3	172.10.30.13	ICMP	64	98 Echo (ping) request id=0xe0e75, seq=5/1280, ttl=64
15	7.378097003	172.10.30.13	172.40.50.3	ICMP	64	98 Echo (ping) reply id=0xe0e75, seq=5/1280, ttl=62
16	8.378085768	172.40.50.3	172.10.30.13	ICMP	64	98 Echo (ping) request id=0xe0e75, seq=6/1536, ttl=64

- D.1 ping D.2, ping allowed

No.	Time	Source	Destination	Protocol	Length	Info
5	4.080629347	172.40.50.3	172.40.100.4	ICMP	98	Echo (ping) request id=0xce75, seq=1/256, ttl=64
6	4.080811067	172.40.100.4	172.40.50.3	ICMP	98	Echo (ping) reply id=0xce75, seq=1/256, ttl=64
25	5.079765847	172.40.50.3	172.40.100.4	ICMP	98	Echo (ping) request id=0xce75, seq=2/512, ttl=64
26	5.079894476	172.40.100.4	172.40.50.3	ICMP	98	Echo (ping) reply id=0xce75, seq=2/512, ttl=64
27	6.079758784	172.40.50.3	172.40.100.4	ICMP	98	Echo (ping) request id=0xce75, seq=3/768, ttl=64
28	6.079915721	172.40.100.4	172.40.50.3	ICMP	98	Echo (ping) reply id=0xce75, seq=3/768, ttl=64
30	7.079803739	172.40.50.3	172.40.100.4	ICMP	98	Echo (ping) request id=0xce75, seq=4/1024, ttl=64
31	7.079981781	172.40.100.4	172.40.50.3	ICMP	98	Echo (ping) reply id=0xce75, seq=4/1024, ttl=64
32	8.079737755	172.40.50.3	172.40.100.4	ICMP	98	Echo (ping) request id=0xce75, seq=5/1280, ttl=64
33	8.079905980	172.40.100.4	172.40.50.3	ICMP	98	Echo (ping) reply id=0xce75, seq=5/1280, ttl=64
35	9.079805924	172.40.50.3	172.40.100.4	ICMP	98	Echo (ping) request id=0xce75, seq=6/1536, ttl=64

- D.2 ping A.D, ping allowed

No.	Time	Source	Destination	Protocol	Length	Info
10	1.388499885	172.40.100.4	172.10.30.13	ICMP	98	Echo (ping) request id=0x1416, seq=1/256, ttl=64
11	1.389793312	172.10.30.13	172.40.100.4	ICMP	98	Echo (ping) reply id=0x1416, seq=1/256, ttl=62
13	2.389897311	172.40.100.4	172.10.30.13	ICMP	98	Echo (ping) request id=0x1416, seq=2/512, ttl=64
14	2.391220246	172.10.30.13	172.40.100.4	ICMP	98	Echo (ping) reply id=0x1416, seq=2/512, ttl=62
15	3.391348727	172.40.100.4	172.10.30.13	ICMP	98	Echo (ping) request id=0x1416, seq=3/768, ttl=64
16	3.392672958	172.10.30.13	172.40.100.4	ICMP	98	Echo (ping) reply id=0x1416, seq=3/768, ttl=62
18	4.392820215	172.40.100.4	172.10.30.13	ICMP	98	Echo (ping) request id=0x1416, seq=4/1024, ttl=64
19	4.394098490	172.10.30.13	172.40.100.4	ICMP	98	Echo (ping) reply id=0x1416, seq=4/1024, ttl=62
20	5.394249336	172.40.100.4	172.10.30.13	ICMP	98	Echo (ping) request id=0x1416, seq=5/1280, ttl=64
21	5.395466696	172.10.30.13	172.40.100.4	ICMP	98	Echo (ping) reply id=0x1416, seq=5/1280, ttl=62

- D.2 ping D.1, ping allowed

No.	Time	Source	Destination	Protocol	Length	Info
14	7.246277155	172.40.100.4	172.40.50.3	ICMP	98	Echo (ping) request id=0xb015, seq=1/256, ttl=64
15	7.246432220	172.40.50.3	172.40.100.4	ICMP	98	Echo (ping) reply id=0xb015, seq=1/256, ttl=64
17	8.246442011	172.40.100.4	172.40.50.3	ICMP	98	Echo (ping) request id=0xb015, seq=2/512, ttl=64
18	8.246613333	172.40.50.3	172.40.100.4	ICMP	98	Echo (ping) reply id=0xb015, seq=2/512, ttl=64
19	9.246441732	172.40.100.4	172.40.50.3	ICMP	98	Echo (ping) request id=0xb015, seq=3/768, ttl=64
20	9.246589985	172.40.50.3	172.40.100.4	ICMP	98	Echo (ping) reply id=0xb015, seq=3/768, ttl=64
22	10.246440466	172.40.100.4	172.40.50.3	ICMP	98	Echo (ping) request id=0xb015, seq=4/1024, ttl=64
23	10.246568823	172.40.50.3	172.40.100.4	ICMP	98	Echo (ping) reply id=0xb015, seq=4/1024, ttl=64
24	11.246441500	172.40.100.4	172.40.50.3	ICMP	98	Echo (ping) request id=0xb015, seq=5/1280, ttl=64
25	11.246673000	172.40.50.3	172.40.100.4	ICMP	98	Echo (ping) reply id=0xb015, seq=5/1280, ttl=64

- A.D ping D.1, ping allowed

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.10.30.13	172.40.50.3	ICMP	98	Echo (ping) request id=0x800b, seq=1/256, ttl=64
2	0.001265248	172.40.50.3	172.10.30.13	ICMP	98	Echo (ping) reply id=0x800b, seq=1/256, ttl=62
3	1.001402060	172.10.30.13	172.40.50.3	ICMP	98	Echo (ping) request id=0x800b, seq=2/512, ttl=64
4	1.002657757	172.40.50.3	172.10.30.13	ICMP	98	Echo (ping) reply id=0x800b, seq=2/512, ttl=62
5	2.002802510	172.10.30.13	172.40.50.3	ICMP	98	Echo (ping) request id=0x800b, seq=3/768, ttl=64
6	2.004055152	172.40.50.3	172.10.30.13	ICMP	98	Echo (ping) reply id=0x800b, seq=3/768, ttl=62
7	3.004199870	172.10.30.13	172.40.50.3	ICMP	98	Echo (ping) request id=0x800b, seq=4/1024, ttl=64
8	3.005466614	172.40.50.3	172.10.30.13	ICMP	98	Echo (ping) reply id=0x800b, seq=4/1024, ttl=62
9	4.005607718	172.10.30.13	172.40.50.3	ICMP	98	Echo (ping) request id=0x800b, seq=5/1280, ttl=64

- A.D ping D.2, ping allowed

No.	Time	Source	Destination	Protocol	Length	Info
10	4.096882957	172.40.100.4	172.10.30.13	ICMP	98	Echo (ping) reply id=0x940b, seq=5/1280, ttl=64
11	5.097804451	172.10.30.13	172.40.100.4	ICMP	98	Echo (ping) request id=0x940b, seq=6/1536, ttl=64
12	5.0988259795	172.40.100.4	172.10.30.13	ICMP	98	Echo (ping) reply id=0x940b, seq=6/1536, ttl=64
13	6.0988318798	172.10.30.13	172.40.100.4	ICMP	98	Echo (ping) request id=0x940b, seq=7/1792, ttl=64
14	6.099596817	172.40.100.4	172.10.30.13	ICMP	98	Echo (ping) reply id=0x940b, seq=7/1792, ttl=64
15	7.099718721	172.10.30.13	172.40.100.4	ICMP	98	Echo (ping) request id=0x940b, seq=8/2048, ttl=64
16	7.010999409	172.40.100.4	172.10.30.13	ICMP	98	Echo (ping) reply id=0x940b, seq=8/2048, ttl=64
17	8.011121220	172.10.30.13	172.40.100.4	ICMP	98	Echo (ping) request id=0x940b, seq=9/2304, ttl=64

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.

The screenshot shows a software interface for managing firewall policies. At the top, there are tabs for 'Create Firewall' and 'Edit Firewall Policy', with 'Edit Firewall Policy' being active. Below the tabs is a toolbar with icons for 'Add', 'Edit...', 'Delete', 'Move Up', 'Move Down', 'Cut', 'Copy', 'Paste', and 'Rule Flow Diagram'. The main area displays two tables under the heading 'Traffic Classification'.

**Table 1: ccp-policy-ccp-cls-1 (External to Internal)**

ID	Source	Destination	Action	Rule Options
1	any	172.40.50.3	D	Drop
2	any	172.40.100.4	http https	Inspect

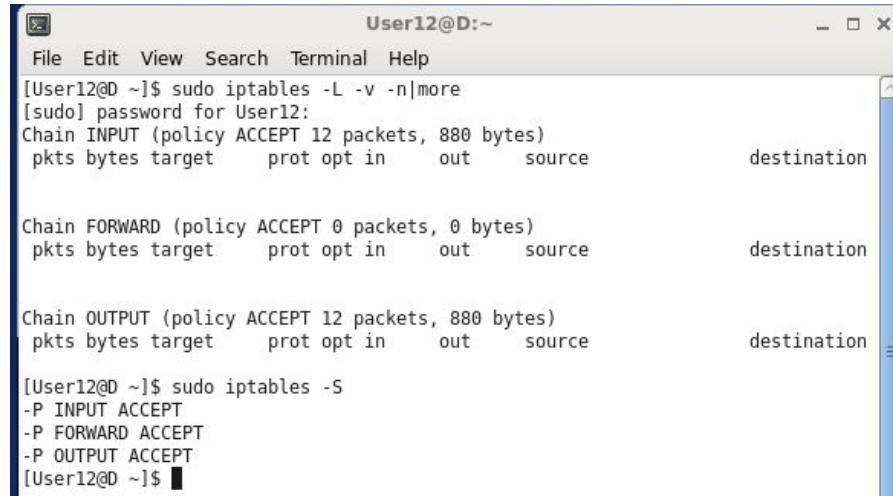
**Table 2: ccp-policy-ccp-cls-2 (Internal to External)**

ID	Source	Destination	Action	Rule Options
1	172.40.100.4	any	icmp	Inspect
2	172.40.50.3	any	http https icmp	Inspect
3	172.40.100.4	any	C	Drop
4	172.40.50.3	172.40.100.4	http https ssh	Inspect

- 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.

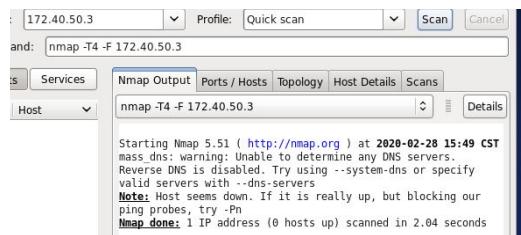


```
User12@D:~$ sudo iptables -L -v -n|more
[sudo] password for User12:
Chain INPUT (policy ACCEPT 12 packets, 880 bytes)
 pkts bytes target     prot opt in     out    source          destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out    source          destination
Chain OUTPUT (policy ACCEPT 12 packets, 880 bytes)
 pkts bytes target     prot opt in     out    source          destination
[User12@D ~]$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
[User12@D ~]$
```

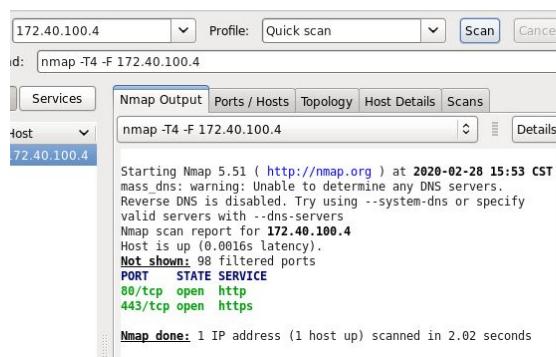
## Section IV (Task IV): Test the implementation of the security policy

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:

```

    172.10.30.13 Profile: Quick scan Scan Cancel
    and: nmap -T4 -F 172.10.30.13
    Services Nmap Output Ports / Hosts Topology Host Details Scans
    Host 172.10.30.13
    172.40.100.4
    Starting Nmap 5.51 ( http://nmap.org ) at 2020-02-28 14:45 CST
    Nmap scan report for 172.10.30.13
    Host is up (0.0014s latency).
    Not shown: 98 filtered ports
    PORT      STATE SERVICE
    80/tcp    open  http
    443/tcp   open  https

    Nmap done: 1 IP address (1 host up) scanned in 18.41 seconds
  
```

- D.1 to D.2:

```

    172.40.100.4 Profile: Quick scan Scan Cancel
    and: nmap -T4 -F 172.40.100.4
    Services Nmap Output Ports / Hosts Topology Host Details Scans
    Host 172.10.30.13
    172.40.100.4
    Starting Nmap 5.51 ( http://nmap.org ) at 2020-02-28 14:48 CST
    Nmap scan report for 172.40.100.4
    Host is up (0.00017s latency).
    Not shown: 97 closed ports
    PORT      STATE SERVICE
    22/tcp    open  ssh
    80/tcp    open  http
    443/tcp   open  https
    MAC Address: B0:83:FE:91:B6:DF (Unknown)

    Nmap done: 1 IP address (1 host up) scanned in 16.60 seconds
  
```

- D.2 to A.D:

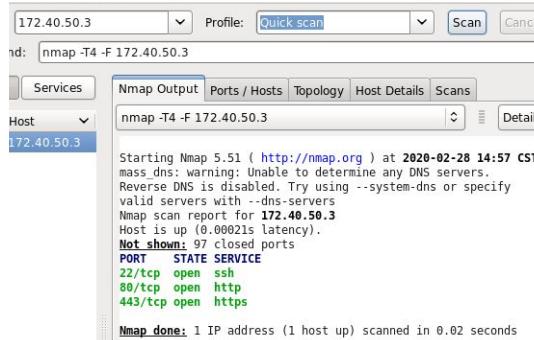
```

    172.10.30.13 Profile: Quick scan Scan Cancel
    and: nmap -T4 -F 172.10.30.13
    Services Nmap Output Ports / Hosts Topology Host Details Scans
    Host 172.40.50.3
    Starting Nmap 5.51 ( http://nmap.org ) at 2020-02-28 14:59 CST
    mass_dns: warning: Unable to determine any DNS servers.
    Reverse DNS is disabled. Try using --system-dns or specify
    valid servers with --dns-servers
    Note: Host seems down. If it is really up, but blocking our
    ping probes, try -Fn

    Nmap done: 1 IP address (0 hosts up) scanned in 2.02 seconds
  
```

# CS 4371 - COMPUTER SECURITY (Project 1)

- 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

o.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	172.10.30.13	172.40.50.3	TCP	74	40682 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK PERM=1 TSval=9925282 TSecr=0 WS=128
2	0.0999781814	172.10.30.13	172.40.50.3	TCP	74	[TCP Retransmission] 40682 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK PERM=1 TSval=99262 TSecr=0 WS=128
3	2.0999801749	172.10.30.13	172.40.50.3	TCP	74	[TCP Retransmission] 40682 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK PERM=1 TSval=99282 TSecr=0 WS=128
4	4.0999744809	b0:83:fe:91:b0:d2	Cisco 83:al:c9	ARP	42	Who has 172.10.0.1? Tell 172.10.30.13
5	5.0000006619	Cisco 83:al:c9	b0:83:fe:91:b0:d2	ARP	60	172.10.0.1 is at 40:55:39:83:al:c9
6	6.0999815634	172.10.30.13	172.40.50.3	TCP	74	[TCP Retransmission] 40682 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK PERM=1 TSval=99322 TSecr=0 WS=128
7	14.0999778095	172.10.30.13	172.40.50.3	TCP	74	[TCP Retransmission] 40682 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK PERM=1 TSval=99402 TSecr=0 WS=128

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

1 0.0000000000	172.10.30.13	172.40.100.4	TCP	74	47604 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK PERM=1 TSval=108845
2 0.001515929	172.40.100.4	172.10.30.13	TCP	74	47604 > 47604 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1452 SACK PERM=1 TSval=108845 TSecr=108845
3 0.001527489	172.10.30.13	172.40.100.4	TCP	66	47604 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=10884557 TSecr=198205
4 0.001561941	172.10.30.13	172.40.100.4	HTTP	229	GET / HTTP/1.0
5 0.002841823	172.40.100.4	172.10.30.13	TCP	66	47604 > 47604 [ACK] Seq=1 Ack=1 Win=15616 Len=0 TSval=108205942 TSecr=108
6 0.003642984	172.40.100.4	172.10.30.13	TCP	2946	[TCP segment of a reassembled PDU]
7 0.003647557	172.10.30.13	172.40.100.4	TCP	66	47604 > http [ACK] Seq=164 Ack=2881 Win=17536 Len=0 TSval=10804559 TSecr=1

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

1 0.0000000000	172.40.50.3	172.10.30.13	TCP	74	56932 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK PERM=1 TSval=108845
2 0.001525287	172.10.30.13	172.40.50.3	TCP	74	http > 56932 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1452 SACK PERM=1 TSval=10845729
3 0.001536560	172.40.50.3	172.10.30.13	TCP	66	56932 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=108608486 TSecr=198205
4 0.001579975	172.40.50.3	172.10.30.13	HTTP	229	GET / HTTP/1.0
5 0.002843963	172.10.30.13	172.40.50.3	TCP	66	http > 56932 [ACK] Seq=1 Ack=164 Win=15616 Len=0 TSval=108205942 TSecr=108
6 0.003845054	172.10.30.13	172.40.50.3	TCP	1506	[TCP segment of a reassembled PDU]

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

2 0.679878104	172.40.50.3	172.10.30.13	TCP	74	47236 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK PERM=1 TSval=956908486 TSecr=8 W
3 0.6800038446	172.40.50.3	172.10.30.13	TCP	74	http > 47236 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1452 SACK PERM=1 TSval=108645729
4 0.6800037596	172.40.50.3	172.10.30.13	TCP	66	47236 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=108608486 TSecr=198205
5 0.6800070041	172.40.50.3	172.10.30.13	HTTP	229	GET / HTTP/1.0
6 0.6800326514	172.40.100.4	172.10.30.13	TCP	66	http > 47236 [ACK] Seq=1 Ack=164 Win=15616 Len=0 TSval=108457299 TSecr=956908486
7 0.6801103503	172.40.100.4	172.10.30.13	TCP	1514	[TCP segment of a reassembled PDU]
8 0.680110683	172.40.50.3	172.40.100.4	TCP	66	47236 > http [ACK] Seq=164 Ack=1449 Win=17536 Len=0 TSval=956908487 TSecr=108
9 0.6801200252	172.40.100.4	172.40.50.3	TCP	1514	[TCP segment of a reassembled PDU]

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

2 1.707232054	172.40.100.4	172.10.30.13	TCP	74	60826 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK PERM=1 TSval=19694
3 1.999793284	b0:aa:77:2b:75:3b	Spanning-tree-(for-bridge)STP	TCP	60	Conf. Root = 32768/0/b0:aa:77:2b:75:3b Cost = 0 Port = 0x0004
4 2.706894369	172.40.100.4	172.10.30.13	TCP	74	[TCP Retransmission] 60826 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SA
5 3.999677114	b0:aa:77:2b:75:3b	Spanning-tree-(for-bridge)STP	TCP	60	Conf. Root = 32768/0/b0:aa:77:2b:75:3b Cost = 0 Port = 0x0004
6 4.526931120	b0:aa:77:2b:75:46	LOOP	TCP	60	Reply
7 4.706865233	172.40.100.4	172.10.30.13	TCP	74	[TCP Retransmission] 60826 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SA
8 5.999527441	b0:aa:77:2b:75:3b	Spanning-tree-(for-bridge)STP	TCP	60	Conf. Root = 32768/0/b0:aa:77:2b:75:3b Cost = 0 Port = 0x0004

# CS 4371 - COMPUTER SECURITY (Project 1)

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

1 0.0000000000 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	TCP	74 55434 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 Tsv=196755258 Tsec=0 WS=1
4 2.441543007 172.40.50.3	TCP	74 http > 55434 [SYN ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 Tsv=196755258 Tsec=0 WS=1
5 2.441557523 172.40.100.4	TCP	66 55434 > [ACK] Seq=1 Ack=1 Win=14720 Len=0 Tsv=196755258 Tsec=0 WS=1
6 2.441599601 172.40.100.4	TCP	228 GET / HTTP/1.0
7 2.441879366 172.40.50.3	HTTP	66 http > 55434 [ACK] Seq=1 Ack=163 Win=15616 Len=0 Tsv=196755258 Tsec=0 WS=1
8 2.442458682 172.40.50.3	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=0xd10f, seq=4/1024, ttl=64
6 25.185617763 172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xdfbf, seq=5/1280, ttl=64
7 26.185597341 b0:83:fe:91:b0:d2	Cisco 83:al:c9	ARP	42 Who has 172.10.0.1? Tell 172.10.30.13
8 26.185626733 172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xf0f, seq=6/1536, ttl=64
9 26.185931853 Cisco 83:al:c9	b0:83:fe:91:b0:d2	ARP	60 172.10.0.1 is at 40:55:39:83:1:c9
10 27.185814356 172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xf0f, seq=7/1792, ttl=64
11 28.185557358 172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xf0f, seq=8/2048, ttl=64
12 29.185620995 172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xf0f, seq=9/2304, ttl=64
13 30.185621891 172.10.30.13	172.40.50.3	ICMP	98 Echo (ping) request id=0xf0f, 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 6.999145683 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 11.999176095 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 0.0000000000 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	ICMP	98 Echo (ping) request id=0xbff7, seq=1/256, ttl=64
3 1.085127726 172.10.30.13	ICMP	98 Echo (ping) reply id=0xbff7, seq=1/256, ttl=64
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 2.085290980 172.40.50.3	ICMP	98 Echo (ping) request id=0xbff7, seq=2/512, ttl=64
6 2.086658483 172.10.30.13	ICMP	98 Echo (ping) reply id=0xbff7, seq=2/512, ttl=64
7 3.086832478 172.40.50.3	ICMP	98 Echo (ping) request id=0xbff7, seq=3/768, ttl=64
8 3.088169166 172.10.30.13	ICMP	98 Echo (ping) reply id=0xbff7, seq=3/768, ttl=64
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	ICMP	98 Echo (ping) request id=0xbff7, seq=4/1024, ttl=64

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

1 0.0000000000 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 172.40.100.4	ICMP	98 Echo (ping) request id=0x9d7e, seq=1/256, ttl=64
3 0.266698514 172.40.100.4	ICMP	98 Echo (ping) reply id=0x9d7e, seq=1/256, ttl=64
4 1.265886444 172.40.50.3	ICMP	98 Echo (ping) request id=0x9d7e, seq=2/512, ttl=64
5 1.266064034 172.40.100.4	ICMP	98 Echo (ping) reply id=0x9d7e, seq=2/512, ttl=64
6 1.599864765 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	ICMP	98 Echo (ping) request id=0x9d7e, seq=3/768, ttl=64
8 2.266055946 172.40.100.4	ICMP	98 Echo (ping) reply id=0x9d7e, seq=3/768, ttl=64
9 3.26588436 172.40.50.3	ICMP	98 Echo (ping) request id=0x9d7e, seq=4/1024, ttl=64
10 3.26606988 172.40.100.4	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 4.085889552 172.40.50.3	ICMP	98 Echo (ping) request id=0x9d7e, seq=5/1280, ttl=64

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

1 0.0000000000 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 1.998328711 172.40.100.4	ICMP	98 Echo (ping) request id=0xb1f, seq=1/256, ttl=64
3 1.999823820 172.10.30.13	ICMP	98 Echo (ping) reply id=0xb1f, seq=1/256, ttl=64
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 2.999926057 172.40.100.4	ICMP	98 Echo (ping) request id=0xb1f, seq=2/512, ttl=64
6 2.911264958 172.10.30.13	ICMP	98 Echo (ping) reply id=0xb1f, seq=2/512, ttl=64
7 3.911392392 172.40.100.4	ICMP	98 Echo (ping) request id=0xb1f, seq=3/768, ttl=64

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

1 0.600000000	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 0.602606819	b0:aa:77:2b:75:38	LLC	60 U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x011D
3 1.739091362	172.40.100.4	ICMP	98 Echo (ping) request id=0x471f, seq=1/256, ttl=64
4 1.739255838	172.40.50.3	ICMP	98 Echo (ping) reply id=0x471f, seq=1/256, ttl=64
5 1.999871446	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
6 2.739234292	172.40.100.4	ICMP	98 Echo (ping) request id=0x471f, seq=2/512, ttl=64
7 2.739426698	172.40.50.3	ICMP	98 Echo (ping) reply id=0x471f, seq=2/512, ttl=64
8 3.739273028	172.40.100.4	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.