Project 1

CS 2371

Benjamin Nye
Brandon Shelton
Bridgett Tijerina
Jacob Lopez

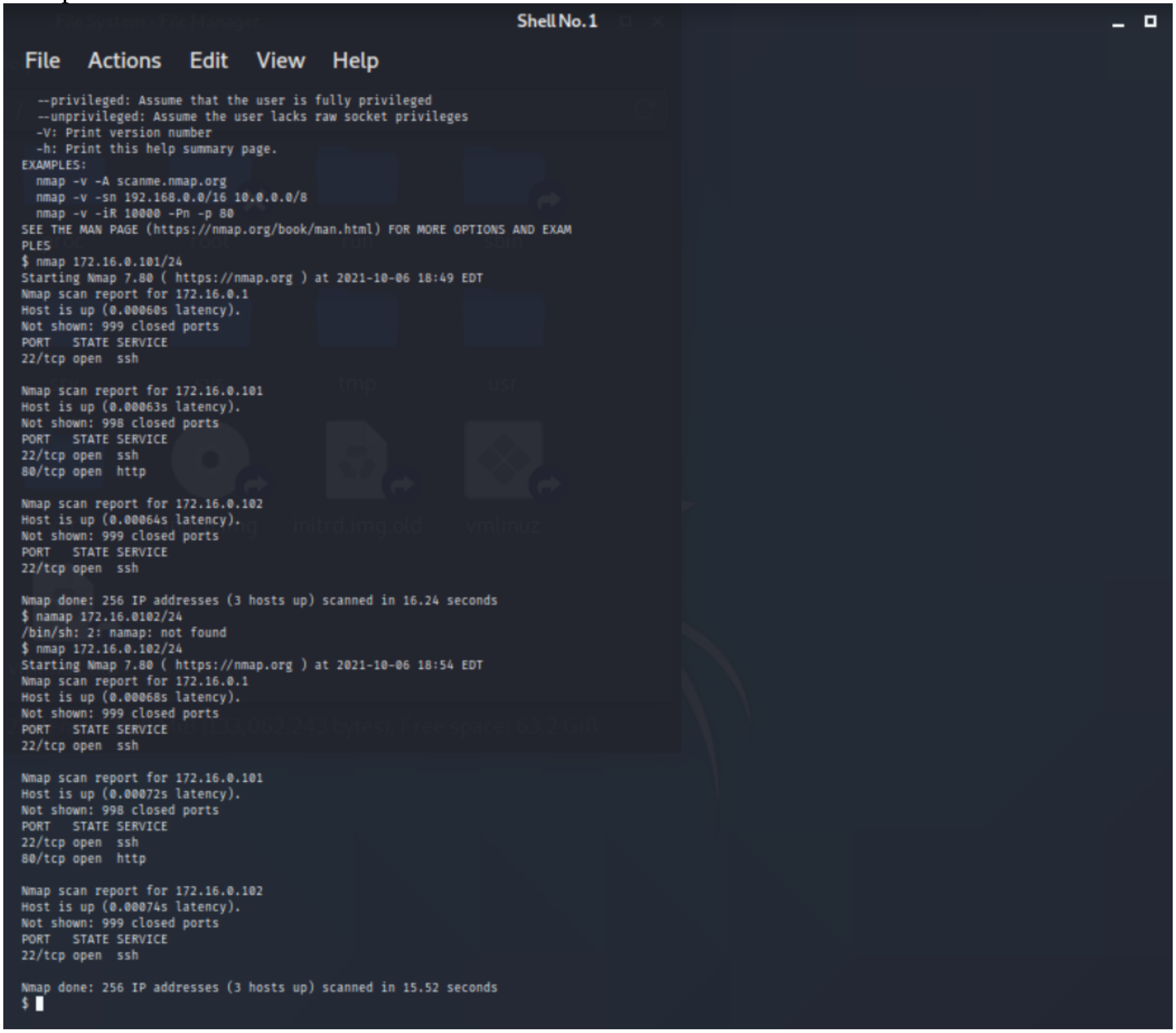
Section I (Introduction) – Benjamin:

For Project 1, our group created, implemented, and tested a network security policy for a company’s server. The roles of the members in our group were for each of us to complete a task and section of the report. Task I was completed by each group member individually. Task II was completed by Jacob, Task III was completed by Brandon, and Task IV was completed by Bridgett. For the report, Benjamin completed sections I and V, Jacob completed section II, Brandon completed section III, and Bridgett completed section IV. As a group we met on Zoom and in the computer lab to discuss the project and work on the tasks. When not meeting, we used GroupMe to coordinate and ask each other questions when we needed assistance.

Section II (Task II) – Jake:

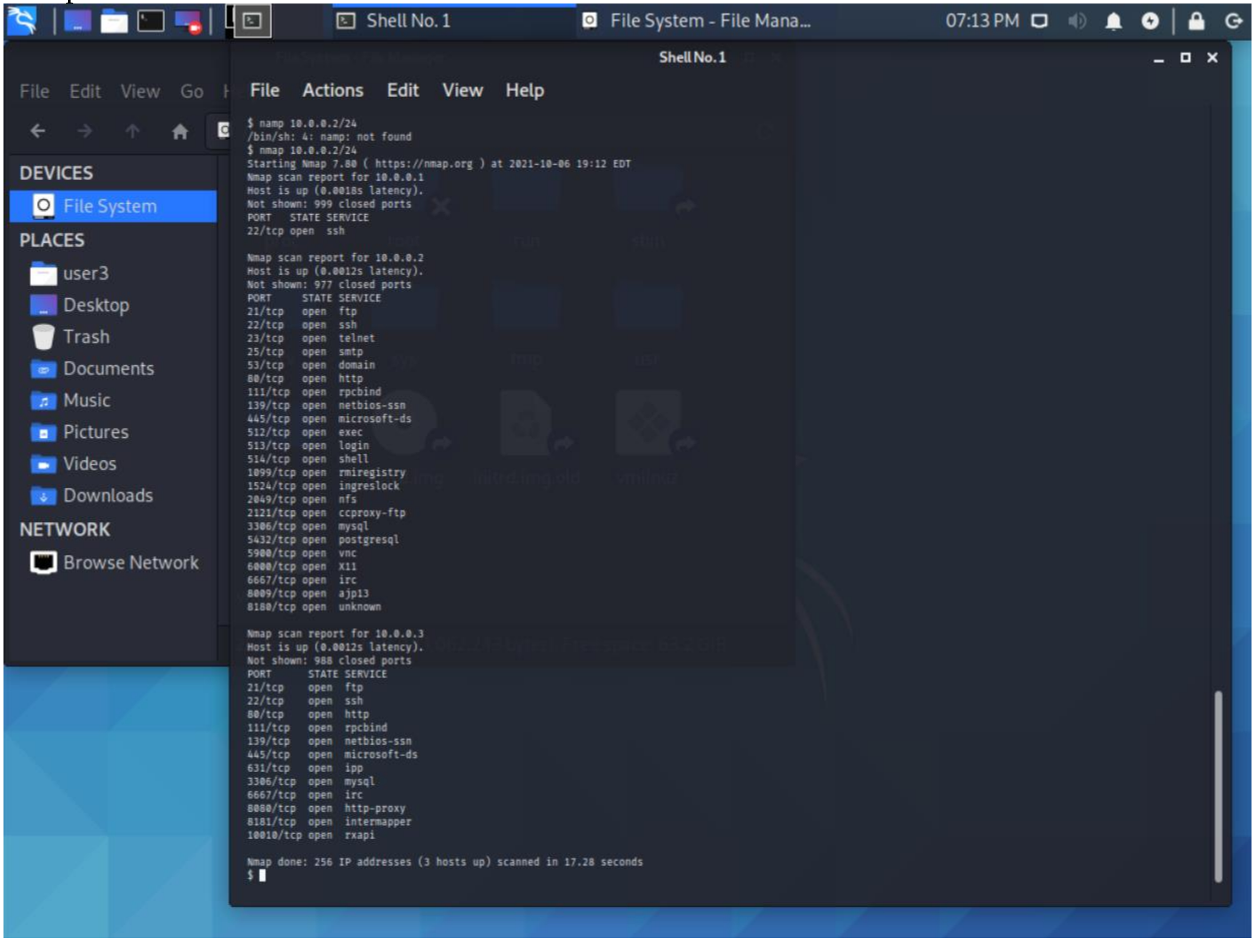
<u>Part a & b:</u> Show the Nmap commands to scan the computers and the service ports and the discovered IPs and services in Network A and B.

Nmap of Kali from Kali:



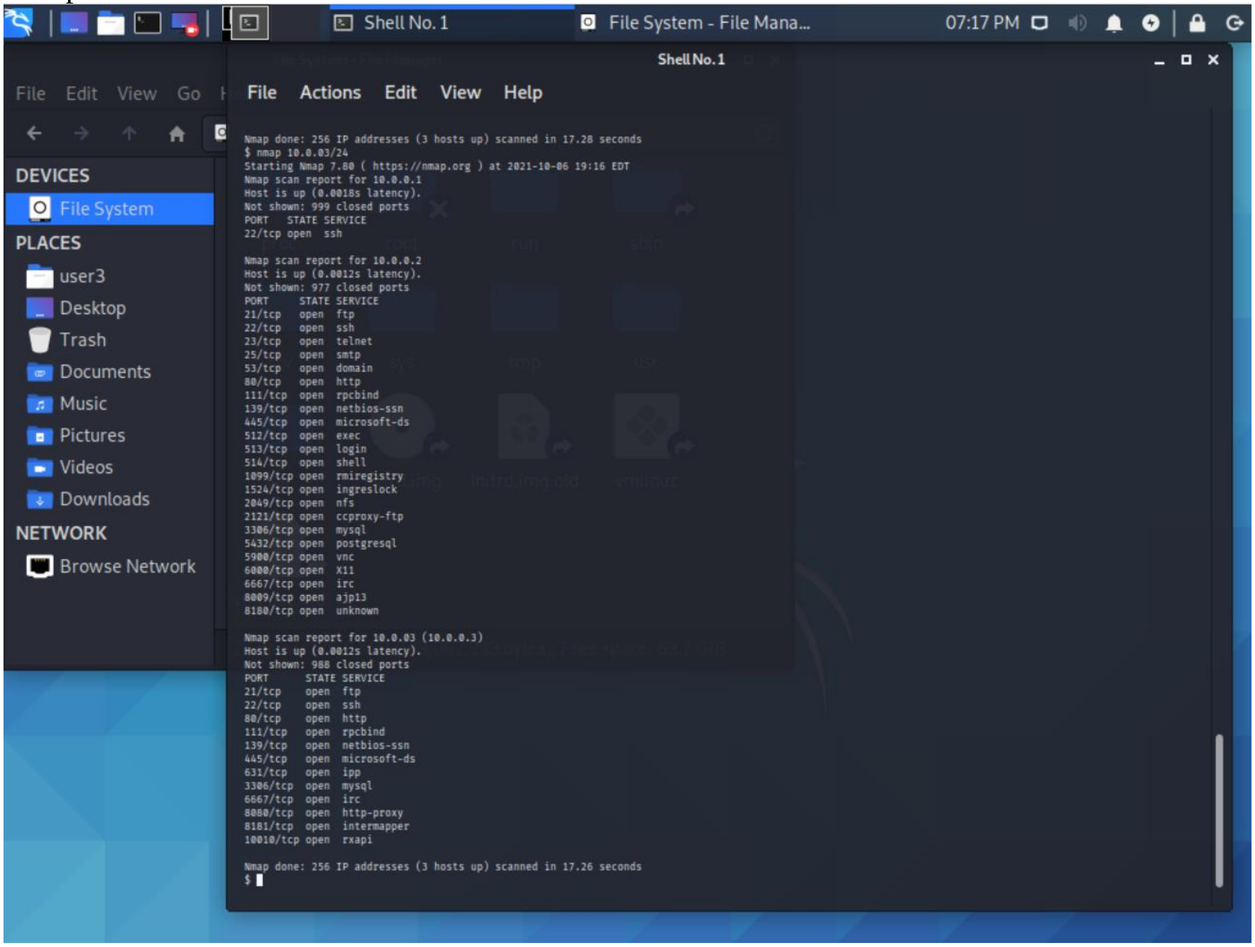
```
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAM
PLES
$ nmap 172.16.0.101/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-06 18:49 EDT
Nmap scan report for 172.16.0.1
Host is up (0.00060s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 172.16.0.101
Host is up (0.00063s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 172.16.0.102
Host is up (0.00064s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 16.24 seconds
$ namap 172.16.0102/24
/bin/sh: 2: namap: not found
$ nmap 172.16.0.102/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-06 18:54 EDT
Nmap scan report for 172.16.0.1
Host is up (0.00068s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 172.16.0.101
Host is up (0.00072s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 172.16.0.102
Host is up (0.00074s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 15.52 seconds
$
```

Nmap from Kali of Meta2:



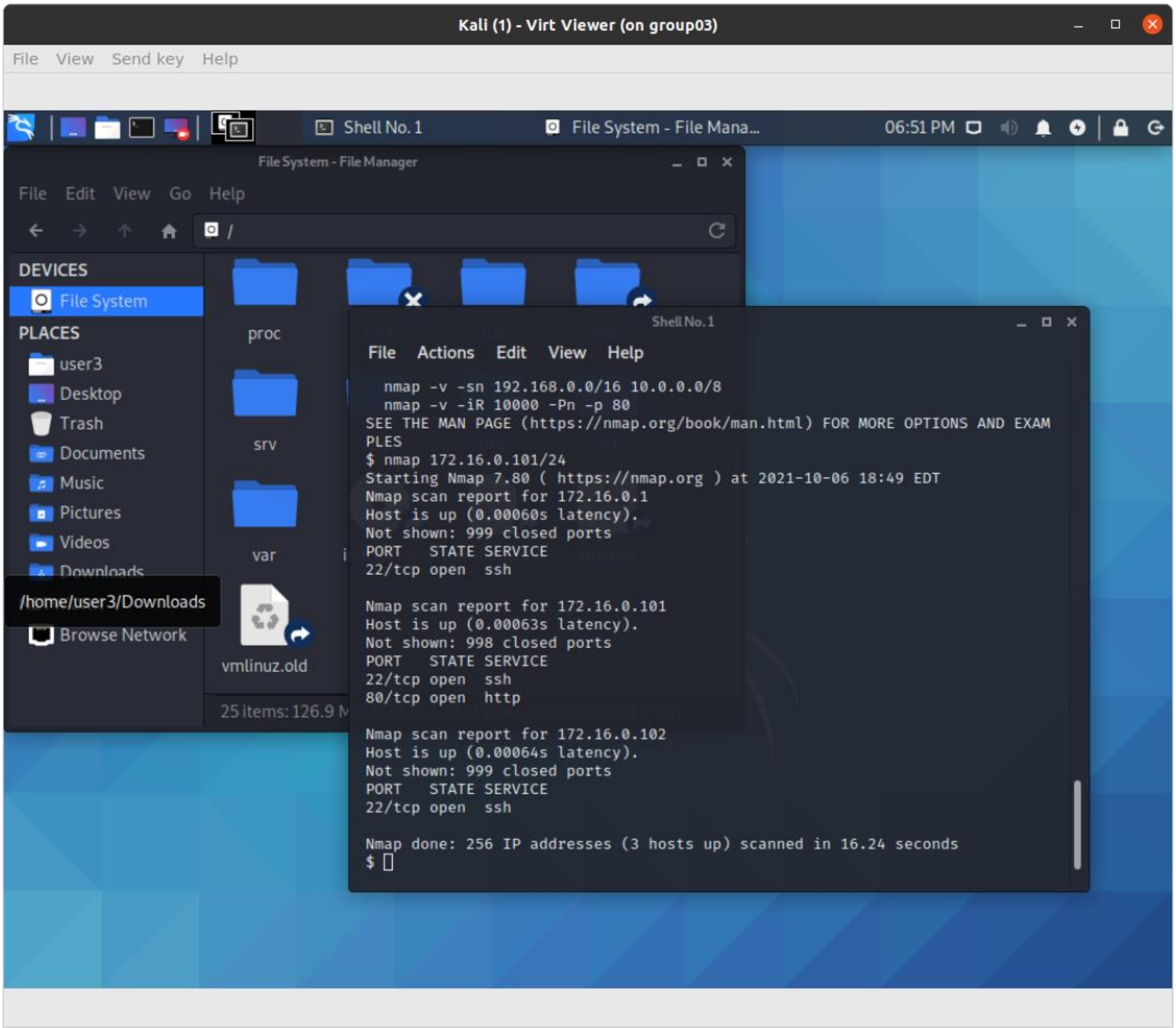
```
$ namp 10.0.0.2/24
/bin/sh: 4: namp: not found
$ nmap 10.0.0.2/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-06 19:12 EDT
Nmap scan report for 10.0.0.1
Host is up (0.0018s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.0.0.2
Host is up (0.0012s latency).
Not shown: 977 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  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap scan report for 10.0.0.3
Host is up (0.0012s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
6667/tcp  open  irc
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
10010/tcp open  rxapi

Nmap done: 256 IP addresses (3 hosts up) scanned in 17.28 seconds
$ █
```

Nmap from kali of Meta3:



```
Nmap done: 256 IP addresses (3 hosts up) scanned in 17.28 seconds
$ nmap 10.0.03/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-06 19:16 EDT
Nmap scan report for 10.0.0.1
Host is up (0.0018s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.0.0.2
Host is up (0.0012s latency).
Not shown: 977 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  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap scan report for 10.0.03 (10.0.0.3)
Host is up (0.0012s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
6667/tcp  open  irc
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
10010/tcp open  rxapi

Nmap done: 256 IP addresses (3 hosts up) scanned in 17.26 seconds
$ 
```

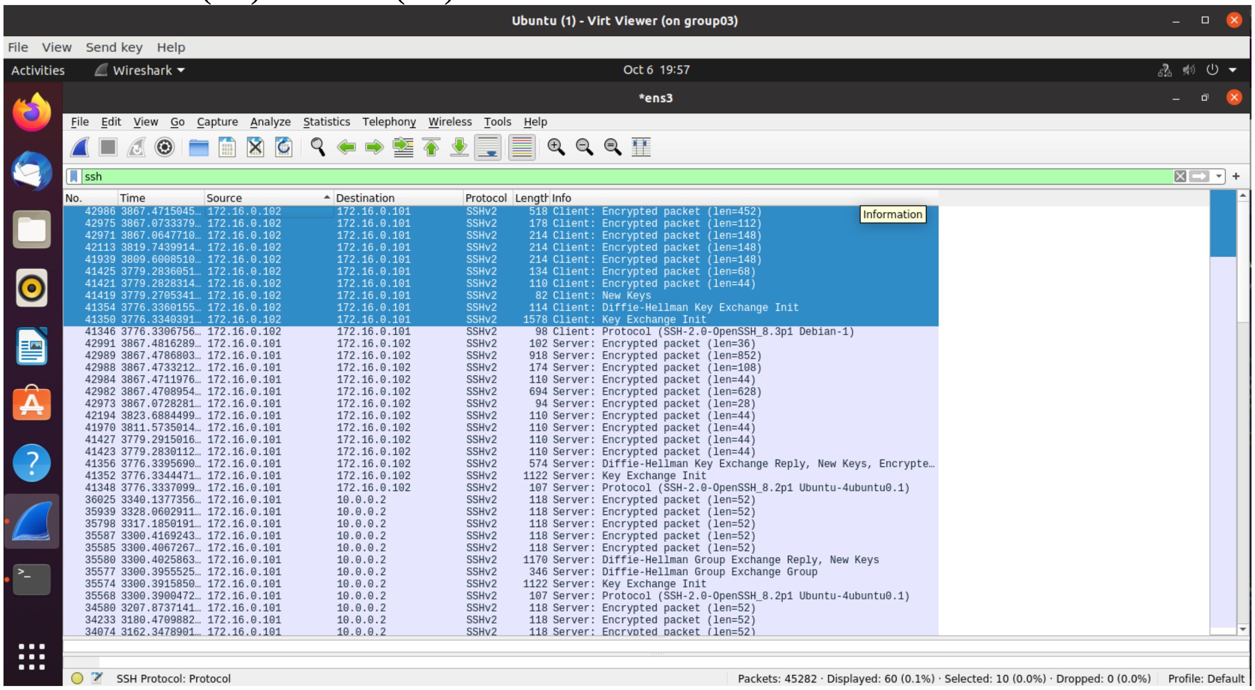
Nmap from Kali of Ubuntu:



```
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAM
PLES
$ nmap 172.16.0.101/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-06 18:49 EDT
Nmap scan report for 172.16.0.1
Host is up (0.00060s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 172.16.0.101
Host is up (0.00063s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 172.16.0.102
Host is up (0.00064s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 16.24 seconds
$ 
```

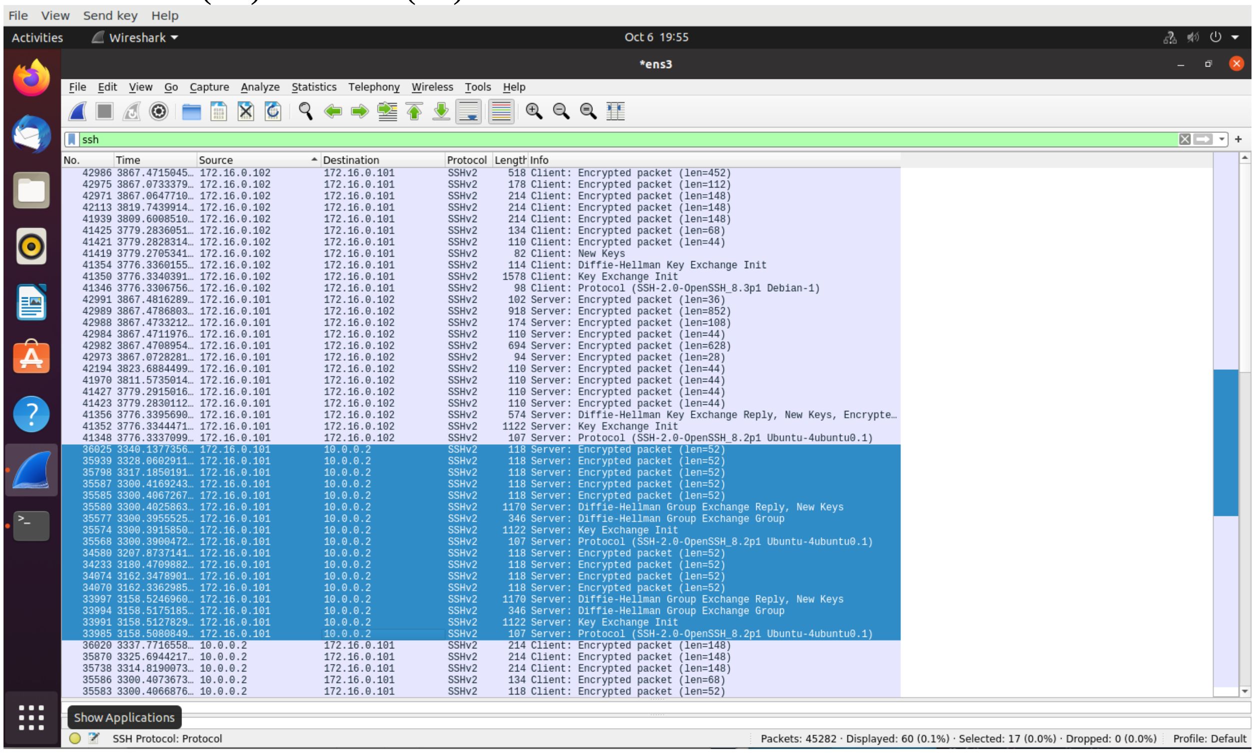
<u>Part c & d:</u> Show the Wireshark results of checking the web service between B.1 and A.1, and between A.2 and A.1 and the Wireshark results of checking the ping between B.1 and A.1, and between A.2 and A.1.

SSH of Ubuntu(A1) from Kali(A2):


Ubuntu (1) - Virt Viewer (on group03)
File View Send key Help
Activities
Wireshark
Oct 6 19:57
*ens3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Information

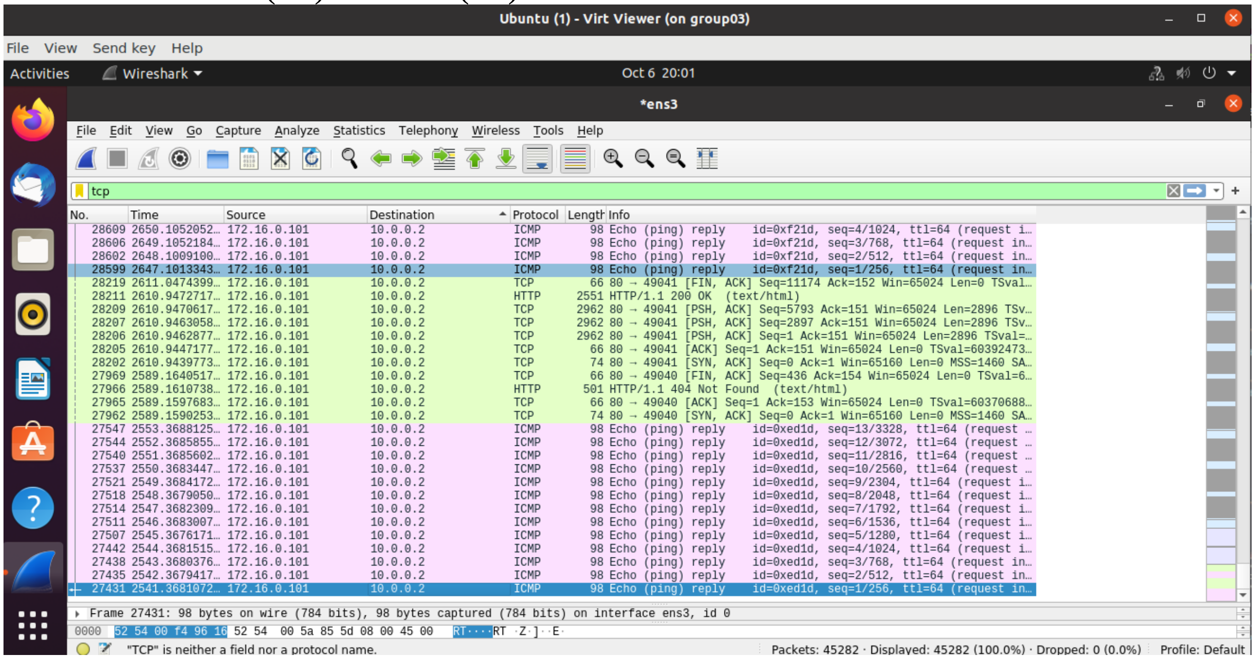
```
ssh

No.   Time          Source        Destination   Protocol Length Info
42986 3867.4715045… 172.16.0.102  172.16.0.101  SSHv2     518 Client: Encrypted packet (len=452)
42975 3867.0733379… 172.16.0.102  172.16.0.101  SSHv2     178 Client: Encrypted packet (len=112)
42971 3867.0647710… 172.16.0.102  172.16.0.101  SSHv2     214 Client: Encrypted packet (len=148)
42113 3819.7439914… 172.16.0.102  172.16.0.101  SSHv2     214 Client: Encrypted packet (len=148)
41939 3809.6008510… 172.16.0.102  172.16.0.101  SSHv2     214 Client: Encrypted packet (len=148)
41425 3779.2836051… 172.16.0.102  172.16.0.101  SSHv2     134 Client: Encrypted packet (len=68)
41421 3779.2828314… 172.16.0.102  172.16.0.101  SSHv2     110 Client: Encrypted packet (len=44)
41419 3779.2705341… 172.16.0.102  172.16.0.101  SSHv2      82 Client: New Keys
41354 3776.3360155… 172.16.0.102  172.16.0.101  SSHv2     114 Client: Diffie-Hellman Key Exchange Init
41350 3776.3340391… 172.16.0.102  172.16.0.101  SSHv2    1578 Client: Key Exchange Init
41346 3776.3306756… 172.16.0.102  172.16.0.101  SSHv2      98 Client: Protocol (SSH-2.0-OpenSSH_8.3p1 Debian-1)
42991 3867.4816289… 172.16.0.101  172.16.0.102  SSHv2     102 Server: Encrypted packet (len=36)
42989 3867.4786803… 172.16.0.101  172.16.0.102  SSHv2     918 Server: Encrypted packet (len=852)
42988 3867.4733212… 172.16.0.101  172.16.0.102  SSHv2     174 Server: Encrypted packet (len=108)
42984 3867.4711976… 172.16.0.101  172.16.0.102  SSHv2     110 Server: Encrypted packet (len=44)
42982 3867.4708954… 172.16.0.101  172.16.0.102  SSHv2     694 Server: Encrypted packet (len=628)
42973 3867.0728281… 172.16.0.101  172.16.0.102  SSHv2      94 Server: Encrypted packet (len=28)
42194 3823.6884499… 172.16.0.101  172.16.0.102  SSHv2     110 Server: Encrypted packet (len=44)
41970 3811.5735014… 172.16.0.101  172.16.0.102  SSHv2     110 Server: Encrypted packet (len=44)
41427 3779.2915016… 172.16.0.101  172.16.0.102  SSHv2     110 Server: Encrypted packet (len=44)
41423 3779.2830112… 172.16.0.101  172.16.0.102  SSHv2     110 Server: Encrypted packet (len=44)
41356 3776.3395690… 172.16.0.101  172.16.0.102  SSHv2     574 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypte…
41352 3776.3344471… 172.16.0.101  172.16.0.102  SSHv2    1122 Server: Key Exchange Init
41348 3776.3337099… 172.16.0.101  172.16.0.102  SSHv2     107 Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1)
36025 3340.1377356… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
35939 3328.0602911… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
35798 3317.1850191… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
35587 3300.4169243… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
35585 3300.4067267… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
35580 3300.4025863… 172.16.0.101  10.0.0.2      SSHv2    1170 Server: Diffie-Hellman Group Exchange Reply, New Keys
35577 3300.3955525… 172.16.0.101  10.0.0.2      SSHv2     346 Server: Diffie-Hellman Group Exchange Group
35574 3300.3915850… 172.16.0.101  10.0.0.2      SSHv2    1122 Server: Key Exchange Init
35568 3300.3900472… 172.16.0.101  10.0.0.2      SSHv2     107 Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1)
34580 3207.8737141… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
34233 3180.4709882… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
34074 3162.3478901… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)

SSH Protocol: Protocol      Packets: 45282 · Displayed: 60 (0.1%) · Selected: 10 (0.0%) · Dropped: 0 (0.0%)      Profile: Default
```

SSH of Ubuntu(A1) from Meta(B1):



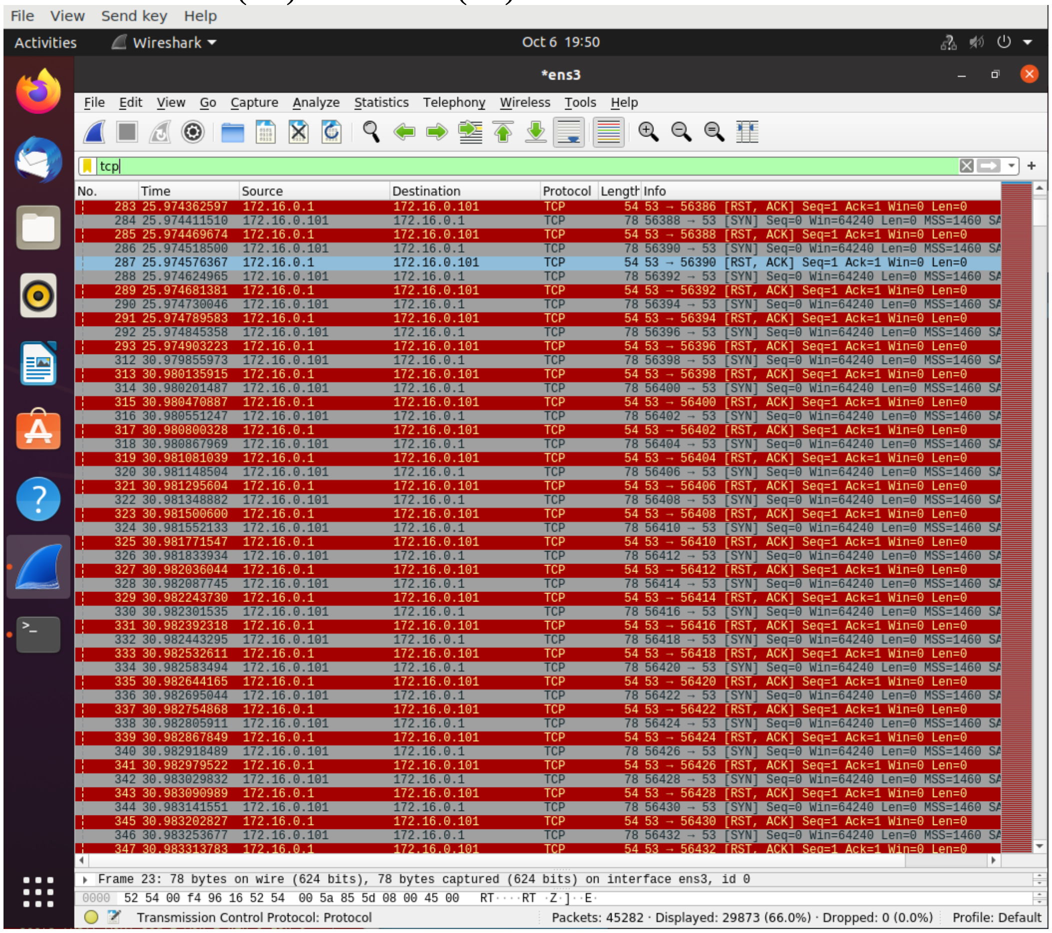
```
ssh

No.   Time          Source        Destination   Protocol Length Info
42986 3867.4715045… 172.16.0.102  172.16.0.101  SSHv2     518 Client: Encrypted packet (len=452)
42975 3867.0733379… 172.16.0.102  172.16.0.101  SSHv2     178 Client: Encrypted packet (len=112)
42971 3867.0647710… 172.16.0.102  172.16.0.101  SSHv2     214 Client: Encrypted packet (len=148)
42113 3819.7439914… 172.16.0.102  172.16.0.101  SSHv2     214 Client: Encrypted packet (len=148)
41939 3809.6008510… 172.16.0.102  172.16.0.101  SSHv2     214 Client: Encrypted packet (len=148)
41425 3779.2836051… 172.16.0.102  172.16.0.101  SSHv2     134 Client: Encrypted packet (len=68)
41421 3779.2828314… 172.16.0.102  172.16.0.101  SSHv2     110 Client: Encrypted packet (len=44)
41419 3779.2705341… 172.16.0.102  172.16.0.101  SSHv2      82 Client: New Keys
41354 3776.3360155… 172.16.0.102  172.16.0.101  SSHv2     114 Client: Diffie-Hellman Key Exchange Init
41350 3776.3340391… 172.16.0.102  172.16.0.101  SSHv2    1578 Client: Key Exchange Init
41346 3776.3306756… 172.16.0.102  172.16.0.101  SSHv2      98 Client: Protocol (SSH-2.0-OpenSSH_8.3p1 Debian-1)
42991 3867.4816289… 172.16.0.101  172.16.0.102  SSHv2     102 Server: Encrypted packet (len=36)
42989 3867.4786803… 172.16.0.101  172.16.0.102  SSHv2     918 Server: Encrypted packet (len=852)
42988 3867.4733212… 172.16.0.101  172.16.0.102  SSHv2     174 Server: Encrypted packet (len=108)
42984 3867.4711976… 172.16.0.101  172.16.0.102  SSHv2     110 Server: Encrypted packet (len=44)
42982 3867.4708954… 172.16.0.101  172.16.0.102  SSHv2     694 Server: Encrypted packet (len=628)
42973 3867.0728281… 172.16.0.101  172.16.0.102  SSHv2      94 Server: Encrypted packet (len=28)
42194 3823.6884499… 172.16.0.101  172.16.0.102  SSHv2     110 Server: Encrypted packet (len=44)
41970 3811.5735014… 172.16.0.101  172.16.0.102  SSHv2     110 Server: Encrypted packet (len=44)
41427 3779.2915016… 172.16.0.101  172.16.0.102  SSHv2     110 Server: Encrypted packet (len=44)
41423 3779.2830112… 172.16.0.101  172.16.0.102  SSHv2     110 Server: Encrypted packet (len=44)
41356 3776.3395690… 172.16.0.101  172.16.0.102  SSHv2     574 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypte…
41352 3776.3344471… 172.16.0.101  172.16.0.102  SSHv2    1122 Server: Key Exchange Init
41348 3776.3337099… 172.16.0.101  172.16.0.102  SSHv2     107 Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1)
36025 3340.1377356… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
35939 3328.0602911… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
35798 3317.1850191… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
35587 3300.4169243… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
35585 3300.4067267… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
35580 3300.4025863… 172.16.0.101  10.0.0.2      SSHv2    1170 Server: Diffie-Hellman Group Exchange Reply, New Keys
35577 3300.3955525… 172.16.0.101  10.0.0.2      SSHv2     346 Server: Diffie-Hellman Group Exchange Group
35574 3300.3915850… 172.16.0.101  10.0.0.2      SSHv2    1122 Server: Key Exchange Init
35568 3300.3900472… 172.16.0.101  10.0.0.2      SSHv2     107 Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1)
34580 3207.8737141… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
34233 3180.4709882… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
34074 3162.3478901… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
34070 3162.3362985… 172.16.0.101  10.0.0.2      SSHv2     118 Server: Encrypted packet (len=52)
33997 3158.5246960… 172.16.0.101  10.0.0.2      SSHv2    1170 Server: Diffie-Hellman Group Exchange Reply, New Keys
33994 3158.5175185… 172.16.0.101  10.0.0.2      SSHv2     346 Server: Diffie-Hellman Group Exchange Group
33991 3158.5127829… 172.16.0.101  10.0.0.2      SSHv2    1122 Server: Key Exchange Init
33985 3158.5080849… 172.16.0.101  10.0.0.2      SSHv2     107 Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1)
36020 3337.7716558… 10.0.0.2      172.16.0.101  SSHv2     214 Client: Encrypted packet (len=148)
35870 3325.6944217… 10.0.0.2      172.16.0.101  SSHv2     214 Client: Encrypted packet (len=148)
35738 3314.8190073… 10.0.0.2      172.16.0.101  SSHv2     214 Client: Encrypted packet (len=148)
35586 3300.4073673… 10.0.0.2      172.16.0.101  SSHv2     134 Client: Encrypted packet (len=68)
35583 3300.4066876… 10.0.0.2      172.16.0.101  SSHv2     118 Client: Encrypted packet (len=52)

SSH Protocol: Protocol      Packets: 45282 · Displayed: 60 (0.1%) · Selected: 17 (0.0%) · Dropped: 0 (0.0%)      Profile: Default
```

TCP FROM Ubuntu(A1) from Kali(A2):


Ubuntu (1) - Virt Viewer (on group03)
File View Send key Help
Activities
Wireshark
Oct 6 20:01
*ens3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

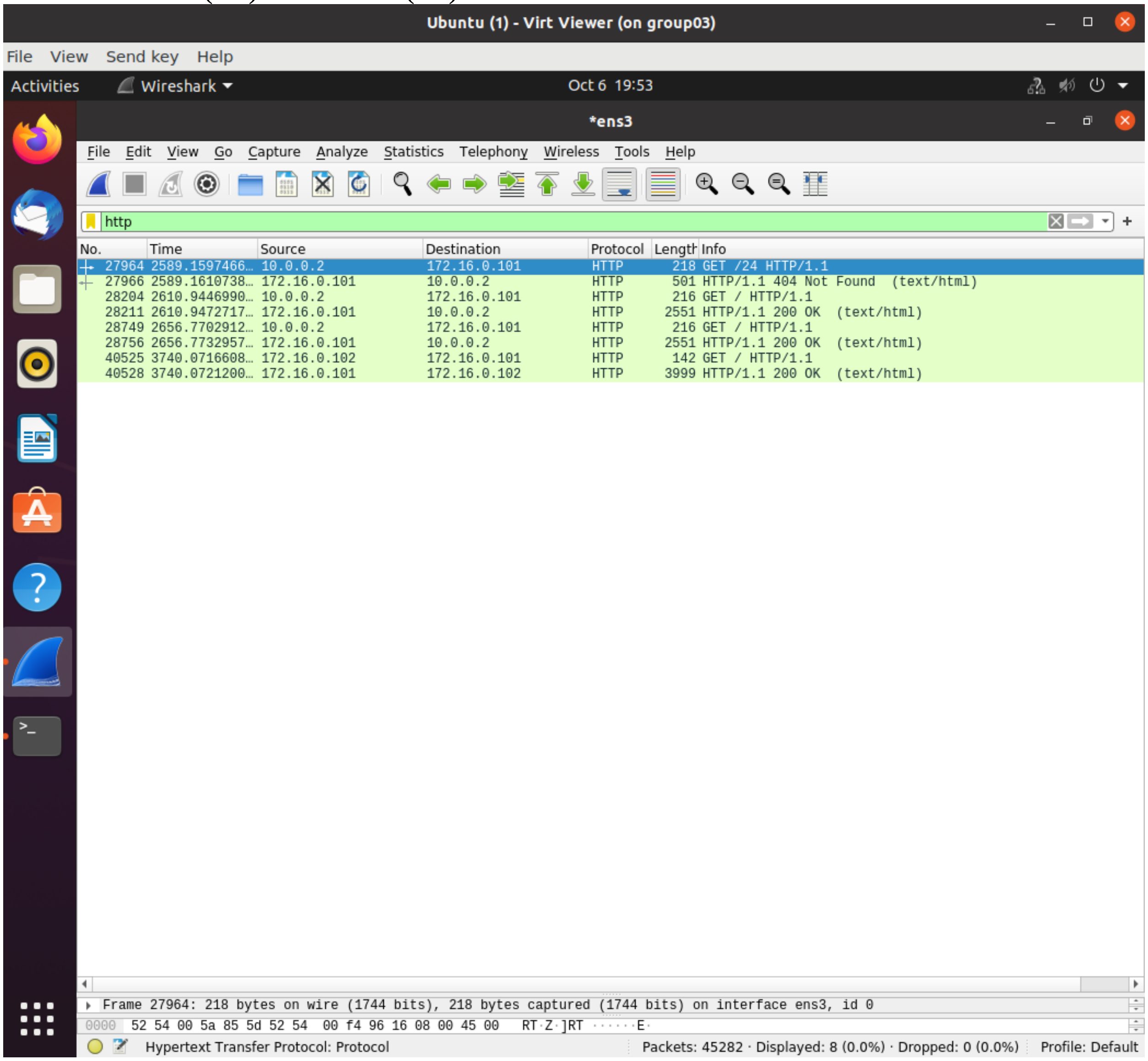
```
tcp

No.   Time          Source        Destination  Protocol Length Info
28609 2650.1052052… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xf21d, seq=4/1024, ttl=64 (request i…
28606 2649.1052184… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xf21d, seq=3/768, ttl=64 (request in…
28602 2648.1009100… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xf21d, seq=2/512, ttl=64 (request in…
28599 2647.1013343… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xf21d, seq=1/256, ttl=64 (request in…
28219 2611.0474399… 172.16.0.101  10.0.0.2     TCP        66 80 → 49041 [FIN, ACK] Seq=11174 Ack=152 Win=65024 Len=0 TSval…
28211 2610.9472717… 172.16.0.101  10.0.0.2     HTTP     2551 HTTP/1.1 200 OK  (text/html)
28209 2610.9470617… 172.16.0.101  10.0.0.2     TCP      2962 80 → 49041 [PSH, ACK] Seq=5793 Ack=151 Win=65024 Len=2896 TSv…
28207 2610.9463058… 172.16.0.101  10.0.0.2     TCP      2962 80 → 49041 [PSH, ACK] Seq=2897 Ack=151 Win=65024 Len=2896 TSv…
28206 2610.9462877… 172.16.0.101  10.0.0.2     TCP      2962 80 → 49041 [PSH, ACK] Seq=1 Ack=151 Win=65024 Len=2896 TSval=…
28205 2610.9447177… 172.16.0.101  10.0.0.2     TCP        66 80 → 49041 [ACK] Seq=1 Ack=151 Win=65024 Len=0 TSval=60392473…
28202 2610.9439773… 172.16.0.101  10.0.0.2     TCP        74 80 → 49041 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
27969 2589.1640517… 172.16.0.101  10.0.0.2     TCP        66 80 → 49040 [FIN, ACK] Seq=436 Ack=154 Win=65024 Len=0 TSval=6…
27966 2589.1610738… 172.16.0.101  10.0.0.2     HTTP      501 HTTP/1.1 404 Not Found  (text/html)
27965 2589.1597683… 172.16.0.101  10.0.0.2     TCP        66 80 → 49040 [ACK] Seq=1 Ack=153 Win=65024 Len=0 TSval=60370688…
27962 2589.1590253… 172.16.0.101  10.0.0.2     TCP        74 80 → 49040 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
27547 2553.3688125… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=13/3328, ttl=64 (request …
27544 2552.3685855… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=12/3072, ttl=64 (request …
27540 2551.3685602… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=11/2816, ttl=64 (request …
27537 2550.3683447… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=10/2560, ttl=64 (request …
27521 2549.3684172… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=9/2304, ttl=64 (request i…
27518 2548.3679050… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=8/2048, ttl=64 (request i…
27514 2547.3682309… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=7/1792, ttl=64 (request i…
27511 2546.3683007… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=6/1536, ttl=64 (request i…
27507 2545.3676171… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=5/1280, ttl=64 (request i…
27442 2544.3681515… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=4/1024, ttl=64 (request i…
27438 2543.3680376… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=3/768, ttl=64 (request in…
27435 2542.3679417… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=2/512, ttl=64 (request in…
27431 2541.3681072… 172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=1/256, ttl=64 (request in…

▸ Frame 27431: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface ens3, id 0
0000  52 54 00 f4 96 16 52 54  00 5a 85 5d 08 00 45 00   RT····RT ·Z·]··E·
"TCP" is neither a field nor a protocol name.     Packets: 45282 · Displayed: 45282 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

TCP from Ubuntu(A1) from Meta2(B1):


File View Send key Help
Activities
Wireshark
Oct 6 19:50
*ens3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

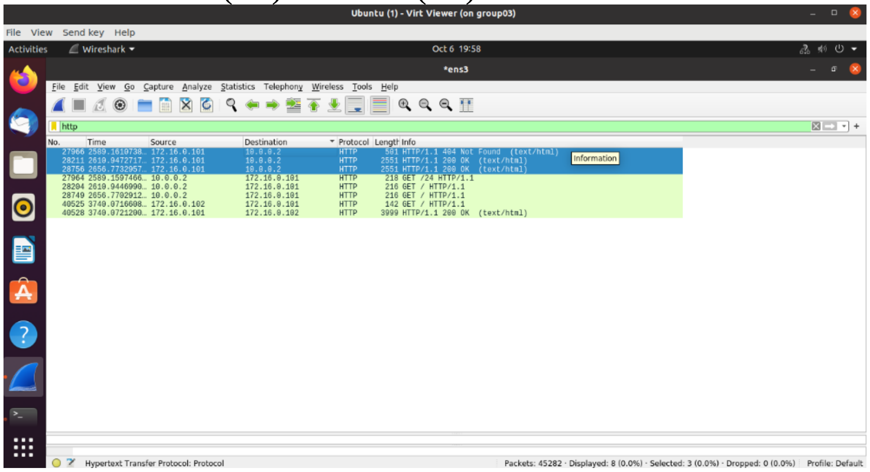
```
tcp

No. Time         Source        Destination   Protocol Length Info
283 25.974362597 172.16.0.1    172.16.0.101  TCP        54 53 → 56386 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
284 25.974411510 172.16.0.101  172.16.0.1    TCP        78 56388 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
285 25.974469674 172.16.0.1    172.16.0.101  TCP        54 53 → 56388 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
286 25.974518500 172.16.0.101  172.16.0.1    TCP        78 56390 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
287 25.974576367 172.16.0.1    172.16.0.101  TCP        54 53 → 56390 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
288 25.974624965 172.16.0.101  172.16.0.1    TCP        78 56392 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
289 25.974681381 172.16.0.1    172.16.0.101  TCP        54 53 → 56392 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
290 25.974730046 172.16.0.101  172.16.0.1    TCP        78 56394 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
291 25.974789583 172.16.0.1    172.16.0.101  TCP        54 53 → 56394 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
292 25.974845358 172.16.0.101  172.16.0.1    TCP        78 56396 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
293 25.974903223 172.16.0.1    172.16.0.101  TCP        54 53 → 56396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
312 30.979855973 172.16.0.101  172.16.0.1    TCP        78 56398 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
313 30.980135915 172.16.0.1    172.16.0.101  TCP        54 53 → 56398 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
314 30.980201487 172.16.0.101  172.16.0.1    TCP        78 56400 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
315 30.980470887 172.16.0.1    172.16.0.101  TCP        54 53 → 56400 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
316 30.980551247 172.16.0.101  172.16.0.1    TCP        78 56402 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
317 30.980800328 172.16.0.1    172.16.0.101  TCP        54 53 → 56402 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
318 30.980867969 172.16.0.101  172.16.0.1    TCP        78 56404 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
319 30.981081039 172.16.0.1    172.16.0.101  TCP        54 53 → 56404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
320 30.981148504 172.16.0.101  172.16.0.1    TCP        78 56406 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
321 30.981295604 172.16.0.1    172.16.0.101  TCP        54 53 → 56406 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
322 30.981348882 172.16.0.101  172.16.0.1    TCP        78 56408 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
323 30.981500600 172.16.0.1    172.16.0.101  TCP        54 53 → 56408 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
324 30.981552133 172.16.0.101  172.16.0.1    TCP        78 56410 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
325 30.981771547 172.16.0.1    172.16.0.101  TCP        54 53 → 56410 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
326 30.981833934 172.16.0.101  172.16.0.1    TCP        78 56412 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
327 30.982036044 172.16.0.1    172.16.0.101  TCP        54 53 → 56412 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
328 30.982087745 172.16.0.101  172.16.0.1    TCP        78 56414 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
329 30.982243730 172.16.0.1    172.16.0.101  TCP        54 53 → 56414 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
330 30.982301535 172.16.0.101  172.16.0.1    TCP        78 56416 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
331 30.982392318 172.16.0.1    172.16.0.101  TCP        54 53 → 56416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
332 30.982443295 172.16.0.101  172.16.0.1    TCP        78 56418 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
333 30.982532611 172.16.0.1    172.16.0.101  TCP        54 53 → 56418 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
334 30.982583494 172.16.0.101  172.16.0.1    TCP        78 56420 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
335 30.982644165 172.16.0.1    172.16.0.101  TCP        54 53 → 56420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
336 30.982695044 172.16.0.101  172.16.0.1    TCP        78 56422 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
337 30.982754868 172.16.0.1    172.16.0.101  TCP        54 53 → 56422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
338 30.982805911 172.16.0.101  172.16.0.1    TCP        78 56424 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
339 30.982867849 172.16.0.1    172.16.0.101  TCP        54 53 → 56424 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
340 30.982918489 172.16.0.101  172.16.0.1    TCP        78 56426 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
341 30.982979522 172.16.0.1    172.16.0.101  TCP        54 53 → 56426 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
342 30.983029832 172.16.0.101  172.16.0.1    TCP        78 56428 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
343 30.983090989 172.16.0.1    172.16.0.101  TCP        54 53 → 56428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
344 30.983141551 172.16.0.101  172.16.0.1    TCP        78 56430 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
345 30.983202827 172.16.0.1    172.16.0.101  TCP        54 53 → 56430 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
346 30.983253677 172.16.0.101  172.16.0.1    TCP        78 56432 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
347 30.983313783 172.16.0.1    172.16.0.101  TCP        54 53 → 56432 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

▸ Frame 23: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface ens3, id 0
0000  52 54 00 f4 96 16 52 54  00 5a 85 5d 08 00 45 00   RT····RT ·Z·]··E·
Transmission Control Protocol: Protocol     Packets: 45282 · Displayed: 29873 (66.0%) · Dropped: 0 (0.0%)   Profile: Default
```

HTTP of Ubuntu(A1) from Meta2(B1):


Ubuntu (1) - Virt Viewer (on group03)
File View Send key Help
Activities
Wireshark
Oct 6 19:53
*ens3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Hypertext Transfer Protocol: Protocol
Packets: 45282 · Displayed: 8 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

```
http
No.   Time            Source        Destination   Protocol Length Info
27964 2589.1597466…  10.0.0.2      172.16.0.101  HTTP      218 GET /24 HTTP/1.1
27966 2589.1610738…  172.16.0.101  10.0.0.2      HTTP      501 HTTP/1.1 404 Not Found  (text/html)
28204 2610.9446990…  10.0.0.2      172.16.0.101  HTTP      216 GET / HTTP/1.1
28211 2610.9472717…  172.16.0.101  10.0.0.2      HTTP     2551 HTTP/1.1 200 OK  (text/html)
28749 2656.7702912…  10.0.0.2      172.16.0.101  HTTP      216 GET / HTTP/1.1
28756 2656.7732957…  172.16.0.101  10.0.0.2      HTTP     2551 HTTP/1.1 200 OK  (text/html)
40525 3740.0716608…  172.16.0.102  172.16.0.101  HTTP      142 GET / HTTP/1.1
40528 3740.0721200…  172.16.0.101  172.16.0.102  HTTP     3999 HTTP/1.1 200 OK  (text/html)

Frame 27964: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface ens3, id 0
0000  52 54 00 5a 85 5d 52 54  00 f4 96 16 08 00 45 00   RT·Z·]RT ······E·
```

HTTP of Ubuntu(A1) from Kali(A2):


Ubuntu (1) - Virt Viewer (on group03)
File View Send key Help
Activities
Wireshark
Oct 6 19:58
*ens3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Information
Hypertext Transfer Protocol: Protocol
Packets: 45282 · Displayed: 8 (0.0%) · Selected: 3 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

```
http
No.   Time            Source        Destination   Protocol Length Info
27966 2589.1610738…  172.16.0.101  10.0.0.2      HTTP      501 HTTP/1.1 404 Not Found  (text/html)
28211 2610.9472717…  172.16.0.101  10.0.0.2      HTTP     2551 HTTP/1.1 200 OK  (text/html)
28756 2656.7732957…  172.16.0.101  10.0.0.2      HTTP     2551 HTTP/1.1 200 OK  (text/html)
27964 2589.1597466…  10.0.0.2      172.16.0.101  HTTP      218 GET /24 HTTP/1.1
28204 2610.9446990…  10.0.0.2      172.16.0.101  HTTP      216 GET / HTTP/1.1
28749 2656.7702912…  10.0.0.2      172.16.0.101  HTTP      216 GET / HTTP/1.1
40525 3740.0716608…  172.16.0.102  172.16.0.101  HTTP      142 GET / HTTP/1.1
40528 3740.0721200…  172.16.0.101  172.16.0.102  HTTP     3999 HTTP/1.1 200 OK  (text/html)
```

Section III (Task III) – Brandon:

Part a:

Below is the Access Control Matrix for Task III of Project 1

	Server	**Workstations (Internal Network)**	**External**
Server	N/A	ping	ping
Workstations (Internal Network)	ssh, https, ping	ping	https, ping
External	https	N/A	N/A

Part b:

We cannot fully implement g: “The workstations and the server can ping to any other computers,” as we do not know any security policies or rules in place on external networks.

Part c:

```
-A INPUT –m conntrack –ctstate RELATED,ESTABLISHED –j ACCEPT
```

Allow incoming already established or packets related to others that have been accepted to pass

```
-A INPUT –s 172.16.0.0/24 -p tcp –m tcp –dport 22 –m conntrack –ctstate NEW,ESTABLISHED –j ACCEPT
```

Allow incoming ssh traffic from 172.16.0.0/24 specifically, new connections and already established ones

```
-A INPUT –p tcp –m multiport –dports 80,443 –m conntrack –ctstate NEW,ESTABLISHED –j ACCEPT
```

Allow incoming http and https connections

```
-A INPUT –s 172.16.0.0/24 -d 172.16.0.0/24 -p tcmp –m icmp –icmp-type 8 –m state –state NEW,RELATED,ESTABLISHED –j ACCEPT
```

Allow incoming ping requests to the server only from the internal network ip addresses

```
-A INPUT –p icmp –m icmp –icmp-type 8 –j drop
```

Drop incoming ping requests from any other source

```
-A OUTPUT –m conntrack –ctstate ESTABLISHED –j ACCEPT
```

Allow outgoing established connections

```
-A OUTPUT –p tcp –m tcp –sport 22 –m conntrack –ctstate ESTABLISHED –j ACCEPT
```

Allow outgoing ssh established traffic

```
-A OUTPUT –p tcp –m multiport –dports 80,443 –m conntrack –ctstate ESTABLISHED –j ACCEPT
```

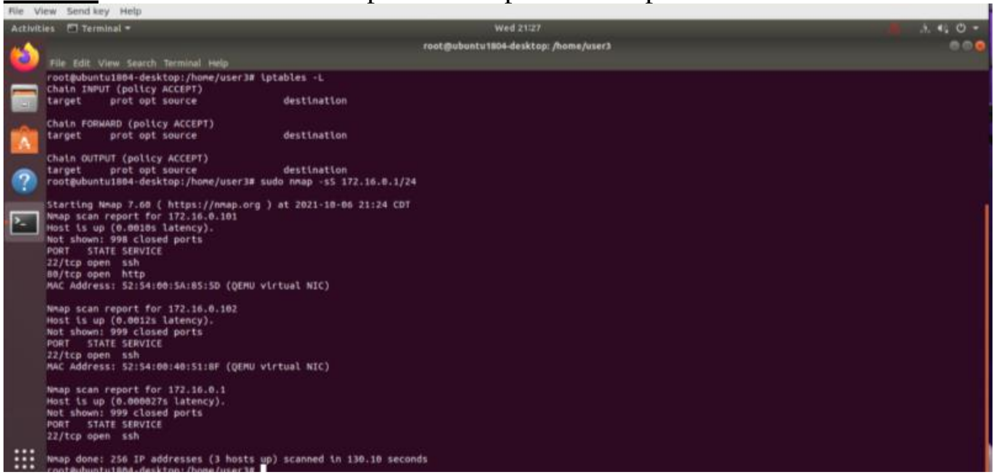
Allow outgoing http and https established traffic

```
-A OUTPUT –s 172.16.0.0/24 -d 172.16.0.0/24 -p icmp –m icmp –icmp-type 0 –m state –state RELATED,ESTABLISHED –j ACCEPT
```

Allow outgoing echo replies from server to internal network ip addresses only

Section IV (Task IV) – Bridgett:

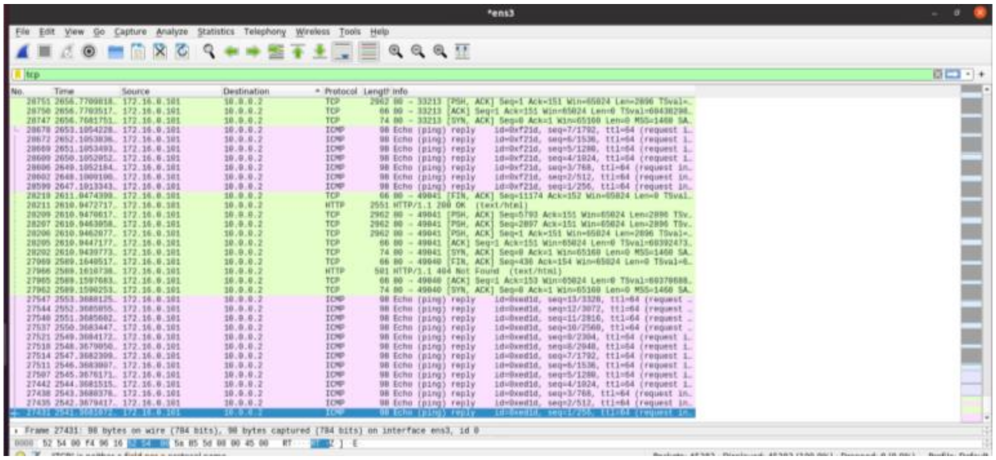
Part a: Screenshot of the exposed computers and ports of Network A.



```
root@ubuntu1804-desktop:/home/user3# 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
root@ubuntu1804-desktop:/home/user3# sudo nmap -sS 172.16.0.1/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-10-06 21:24 CDT
Nmap scan report for 172.16.0.101
Host is up (0.0010s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 52:54:00:5A:85:5D (QEMU virtual NIC)

Nmap scan report for 172.16.0.102
Host is up (0.0012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 52:54:00:40:51:8F (QEMU virtual NIC)

Nmap scan report for 172.16.0.1
Host is up (0.000027s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 130.10 seconds
root@ubuntu1804-desktop:/home/user3#
```

File View Send key Help
Activities
Terminal
Wed 21:27
root@ubuntu1804-desktop: /home/user3
File Edit View Search Terminal Help

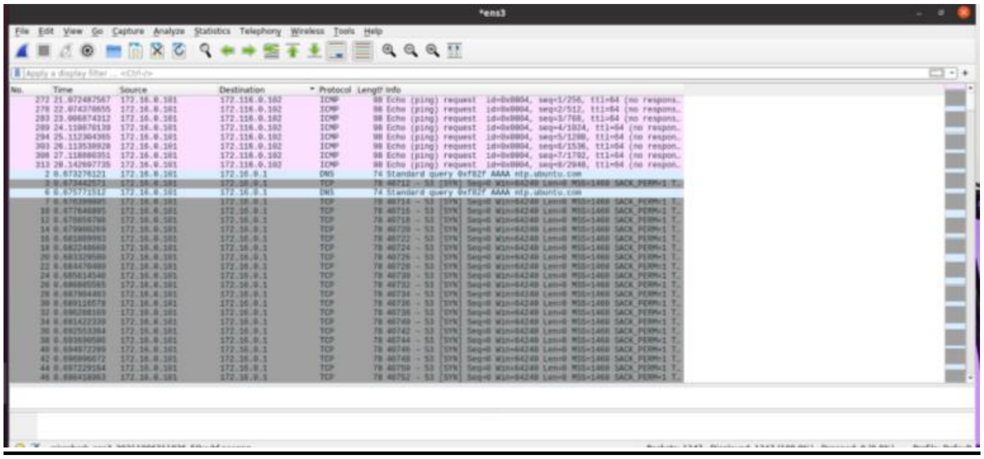
Part b: Screenshot of the Wireshark results of checking the web service between B.1 and A.1, and between A.2 and A.1.



*ens3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp
No.   Time            Source        Destination  Protocol Length Info
28751 2656.7709818…  172.16.0.101  10.0.0.2     TCP      2962 80 → 33213 [PSH, ACK] Seq=1 Ack=151 Win=65024 Len=2896 TSval=…
28750 2656.7703517…  172.16.0.101  10.0.0.2     TCP        66 80 → 33213 [ACK] Seq=1 Ack=151 Win=65024 Len=0 TSval=60438298…
28747 2656.7681751…  172.16.0.101  10.0.0.2     TCP        74 80 → 33213 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
28678 2653.1054228…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xf21d, seq=7/1792, ttl=64 (request i…
28672 2652.1053836…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xf21d, seq=6/1536, ttl=64 (request i…
28669 2651.1053493…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xf21d, seq=5/1280, ttl=64 (request i…
28609 2650.1052052…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xf21d, seq=4/1024, ttl=64 (request i…
28606 2649.1052184…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xf21d, seq=3/768, ttl=64 (request in…
28602 2648.1009100…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xf21d, seq=2/512, ttl=64 (request in…
28599 2647.1013343…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xf21d, seq=1/256, ttl=64 (request in…
28219 2611.0474399…  172.16.0.101  10.0.0.2     TCP        66 80 → 49041 [FIN, ACK] Seq=11174 Ack=152 Win=65024 Len=0 TSval…
28211 2610.9472717…  172.16.0.101  10.0.0.2     HTTP     2551 HTTP/1.1 200 OK  (text/html)
28209 2610.9470617…  172.16.0.101  10.0.0.2     TCP      2962 80 → 49041 [PSH, ACK] Seq=5793 Ack=151 Win=65024 Len=2896 TSv…
28207 2610.9463058…  172.16.0.101  10.0.0.2     TCP      2962 80 → 49041 [PSH, ACK] Seq=2897 Ack=151 Win=65024 Len=2896 TSv…
28206 2610.9462077…  172.16.0.101  10.0.0.2     TCP      2962 80 → 49041 [PSH, ACK] Seq=1 Ack=151 Win=65024 Len=2896 TSval=…
28205 2610.9447177…  172.16.0.101  10.0.0.2     TCP        66 80 → 49041 [ACK] Seq=1 Ack=151 Win=65024 Len=0 TSval=60392473…
28202 2610.9439773…  172.16.0.101  10.0.0.2     TCP        74 80 → 49041 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
27969 2589.1640517…  172.16.0.101  10.0.0.2     TCP        66 80 → 49040 [FIN, ACK] Seq=436 Ack=154 Win=65024 Len=0 TSval=6…
27966 2589.1610738…  172.16.0.101  10.0.0.2     HTTP      501 HTTP/1.1 404 Not Found  (text/html)
27965 2589.1597683…  172.16.0.101  10.0.0.2     TCP        66 80 → 49040 [ACK] Seq=1 Ack=153 Win=65024 Len=0 TSval=60370688…
27962 2589.1590253…  172.16.0.101  10.0.0.2     TCP        74 80 → 49040 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA…
27547 2553.3688125…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=13/3328, ttl=64 (request …
27544 2552.3685055…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=12/3072, ttl=64 (request …
27540 2551.3685602…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=11/2816, ttl=64 (request …
27537 2550.3683447…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=10/2560, ttl=64 (request …
27521 2549.3684172…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=9/2304, ttl=64 (request i…
27518 2548.3679050…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=8/2048, ttl=64 (request i…
27514 2547.3682309…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=7/1792, ttl=64 (request i…
27511 2546.3683007…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=6/1536, ttl=64 (request i…
27507 2545.3676171…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=5/1280, ttl=64 (request i…
27442 2544.3681515…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=4/1024, ttl=64 (request i…
27438 2543.3680378…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=3/768, ttl=64 (request in…
27435 2542.3679417…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=2/512, ttl=64 (request in…
27431 2541.3681072…  172.16.0.101  10.0.0.2     ICMP       98 Echo (ping) reply    id=0xed1d, seq=1/256, ttl=64 (request in…

› Frame 27431: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface ens3, id 0
0000  52 54 00 f4 96 16 52 54 00 5a 85 5d 08 00 45 00   RT····RT ·Z·]··E·
```

Part c: Screenshot of the Wireshark results of checking the ping between B.1 and A.1, and between A.2 and A.1.

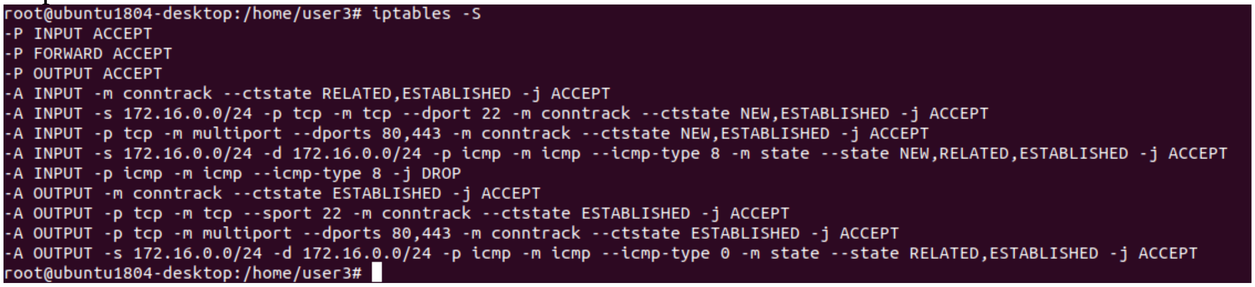


*ens3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
Apply a display filter … <Ctrl-/>
No.  Time          Source        Destination    Protocol Length Info
 272 21.072487567  172.16.0.101  172.116.0.102  ICMP     98 Echo (ping) request  id=0x0004, seq=1/256, ttl=64 (no respons…
 278 22.074370655  172.16.0.101  172.116.0.102  ICMP     98 Echo (ping) request  id=0x0004, seq=2/512, ttl=64 (no respons…
 283 23.006874312  172.16.0.101  172.116.0.102  ICMP     98 Echo (ping) request  id=0x0004, seq=3/768, ttl=64 (no respons…
 289 24.110870139  172.16.0.101  172.116.0.102  ICMP     98 Echo (ping) request  id=0x0004, seq=4/1024, ttl=64 (no respon…
 294 25.112304365  172.16.0.101  172.116.0.102  ICMP     98 Echo (ping) request  id=0x0004, seq=5/1280, ttl=64 (no respon…
 303 26.113530928  172.16.0.101  172.116.0.102  ICMP     98 Echo (ping) request  id=0x0004, seq=6/1536, ttl=64 (no respon…
 308 27.118880351  172.16.0.101  172.116.0.102  ICMP     98 Echo (ping) request  id=0x0004, seq=7/1792, ttl=64 (no respon…
 313 28.142097735  172.16.0.101  172.116.0.102  ICMP     98 Echo (ping) request  id=0x0004, seq=8/2048, ttl=64 (no respon…
   2 0.673276121   172.16.0.101  172.16.0.1     DNS      74 Standard query 0xf82f AAAA ntp.ubuntu.com
   3 0.673442571   172.16.0.101  172.16.0.1     TCP      78 40712 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
   6 0.675771512   172.16.0.101  172.16.0.1     DNS      74 Standard query 0xf82f AAAA ntp.ubuntu.com
   7 0.676390805   172.16.0.101  172.16.0.1     TCP      78 40714 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  10 0.677648885   172.16.0.101  172.16.0.1     TCP      78 40716 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  12 0.678056780   172.16.0.101  172.16.0.1     TCP      78 40718 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  14 0.679900269   172.16.0.101  172.16.0.1     TCP      78 40720 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  16 0.681009991   172.16.0.101  172.16.0.1     TCP      78 40722 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  18 0.682248660   172.16.0.101  172.16.0.1     TCP      78 40724 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  20 0.683329580   172.16.0.101  172.16.0.1     TCP      78 40726 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  22 0.684470480   172.16.0.101  172.16.0.1     TCP      78 40728 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  24 0.685614540   172.16.0.101  172.16.0.1     TCP      78 40730 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  26 0.686065565   172.16.0.101  172.16.0.1     TCP      78 40732 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  28 0.687904403   172.16.0.101  172.16.0.1     TCP      78 40734 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  30 0.689116578   172.16.0.101  172.16.0.1     TCP      78 40736 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  32 0.690298169   172.16.0.101  172.16.0.1     TCP      78 40738 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  34 0.691422339   172.16.0.101  172.16.0.1     TCP      78 40740 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  36 0.692553304   172.16.0.101  172.16.0.1     TCP      78 40742 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  38 0.693690586   172.16.0.101  172.16.0.1     TCP      78 40744 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  40 0.694972299   172.16.0.101  172.16.0.1     TCP      78 40746 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  42 0.696096672   172.16.0.101  172.16.0.1     TCP      78 40748 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  44 0.697229154   172.16.0.101  172.16.0.1     TCP      78 40750 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
  46 0.698418963   172.16.0.101  172.16.0.1     TCP      78 40752 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T…
```

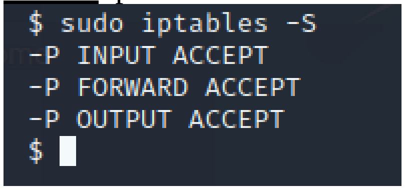
Section V – Benjamin:

R iptables:



```
root@ubuntu1804-desktop:/home/user3# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 172.16.0.0/24 -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A INPUT -s 172.16.0.0/24 -d 172.16.0.0/24 -p icmp -m icmp --icmp-type 8 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j DROP
-A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A OUTPUT -s 172.16.0.0/24 -d 172.16.0.0/24 -p icmp -m icmp --icmp-type 0 -m state --state RELATED,ESTABLISHED -j ACCEPT
root@ubuntu1804-desktop:/home/user3#
```

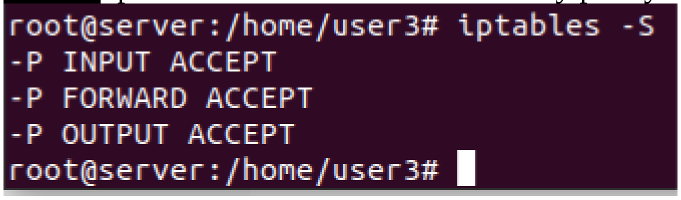
Part a: iptables rules to enforce the security policy in A.1 that is not implemented in R



```
$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
$
```

-P INPUT ACCEPT: Accepts all new traffic that is within network or made it through the router
-P FORWARD ACCEPT: Allows for any connection not for A.1.
-P OUTPUT ACCEPT: Allows all outgoing connections from A.1.

Part b: iptables rules to enforce the security policy in A.1 that is not implemented in R



```
root@server:/home/user3# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
root@server:/home/user3#
```

-P INPUT ACCEPT: Accepts all new traffic that is within network or made it through the router
-P FORWARD ACCEPT: Allows for any connection not for A.2.
-P OUTPUT ACCEPT: Allows all outgoing connections from A.2.

Part c:

The security policy of not allowing anyone to carry a device and users have accounts on A.1 is not secure. Based on the iptables from above A.1 is allowed to make outgoing connections to external computers. Therefor, someone could potentially access A.1 with their user account and send the data to external computers since they can access the data with their user accounts.