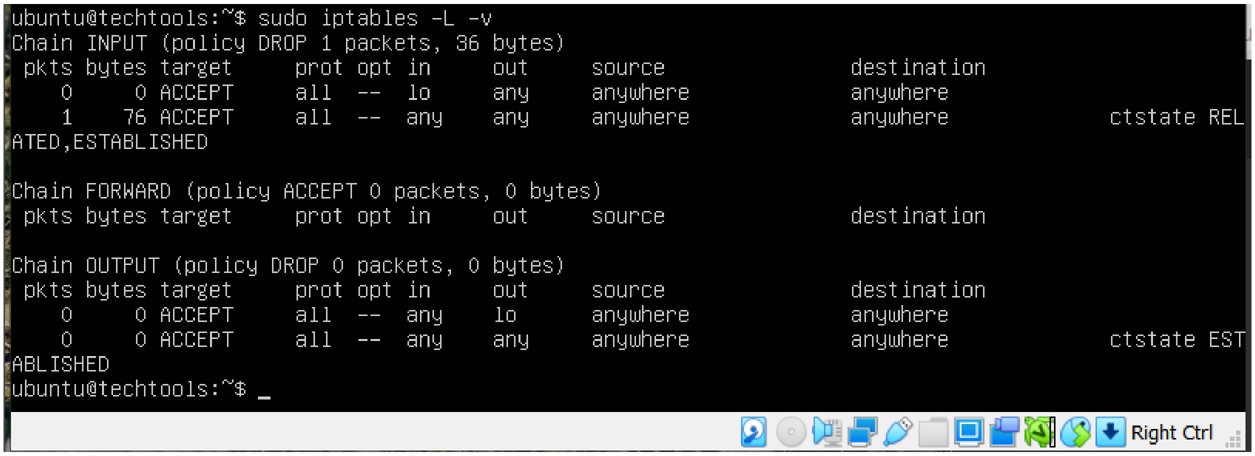
Matthew Zaldana
SID: 027008928

CECS 303 – Lab 3

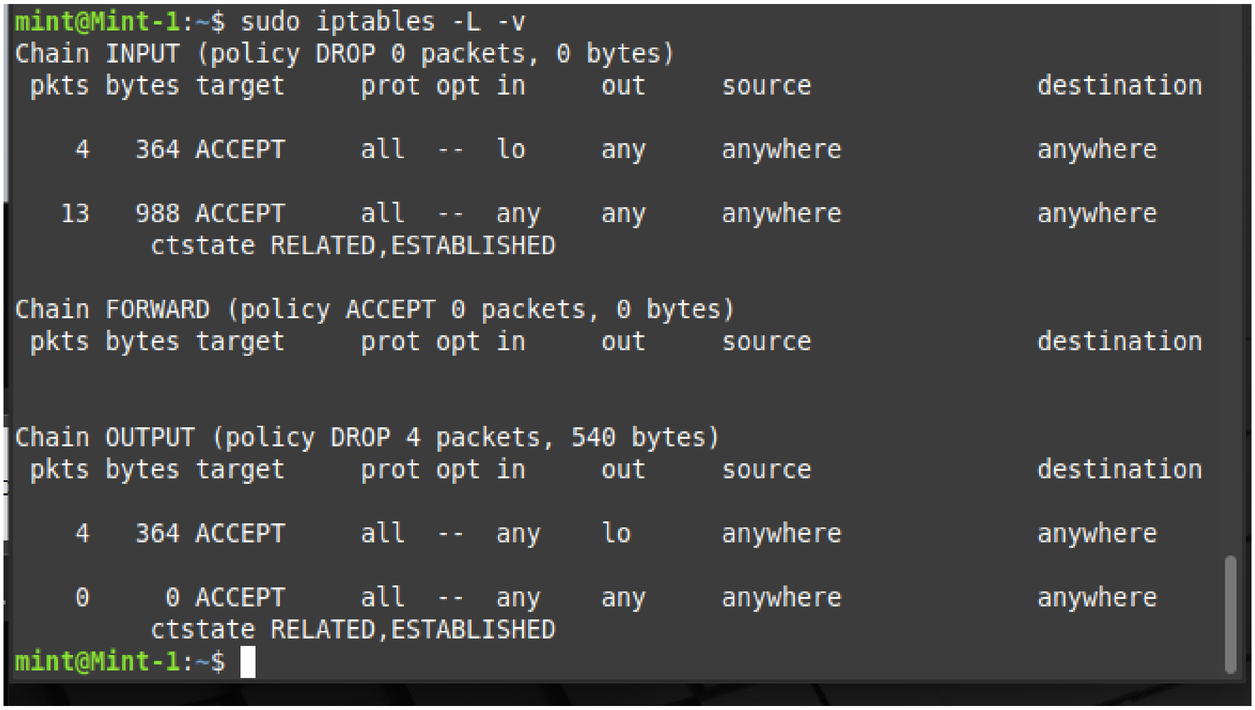
1.

ubuntu server 1



```
ubuntu@techtools:~$ sudo iptables -L -v
Chain INPUT (policy DROP 1 packets, 36 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
    1    76 ACCEPT     all  --  any    any     anywhere             anywhere             ctstate REL
ATED,ESTABLISHED

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  any    lo      anywhere             anywhere
    0     0 ACCEPT     all  --  any    any     anywhere             anywhere             ctstate EST
ABLISHED
ubuntu@techtools:~$ _
```

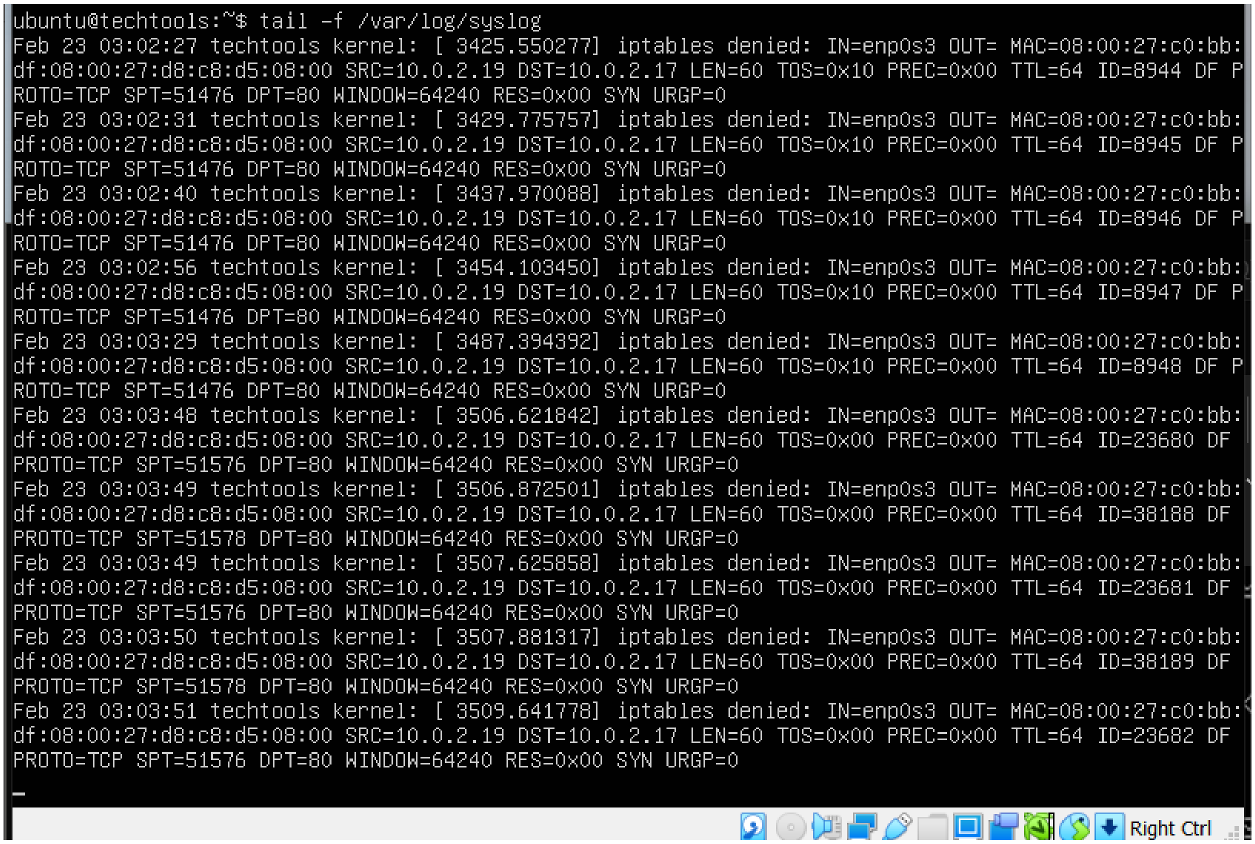
mint



```
mint@Mint-1:~$ sudo iptables -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    4   364 ACCEPT     all  --  lo     any     anywhere             anywhere

   13   988 ACCEPT     all  --  any    any     anywhere             anywhere
         ctstate RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy DROP 4 packets, 540 bytes)
 pkts bytes target     prot opt in     out     source               destination

    4   364 ACCEPT     all  --  any    lo      anywhere             anywhere

    0     0 ACCEPT     all  --  any    any     anywhere             anywhere
         ctstate RELATED,ESTABLISHED
mint@Mint-1:~$ 
```

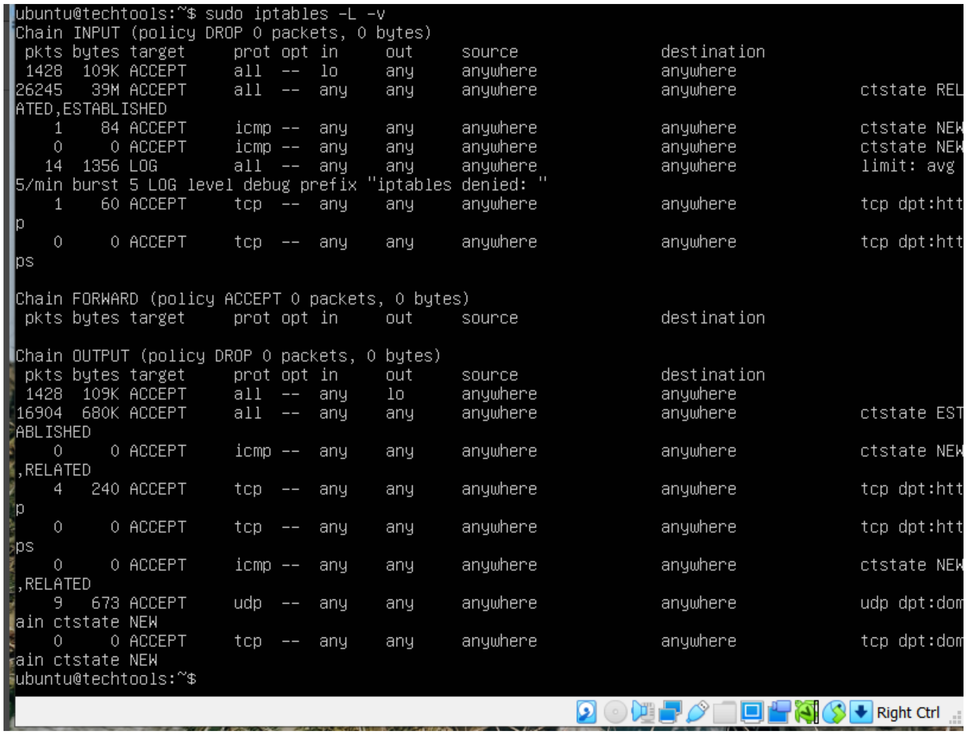
Matthew Zaldana
SID: 027008928

2. Tail command



```
ubuntu@techtools:~$ tail -f /var/log/syslog
Feb 23 03:02:27 techtools kernel: [ 3425.550277] iptables denied: IN=enp0s3 OUT= MAC=08:00:27:c0:bb:
df:08:00:27:d8:c8:d5:08:00 SRC=10.0.2.19 DST=10.0.2.17 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=8944 DF P
ROTO=TCP SPT=51476 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0
Feb 23 03:02:31 techtools kernel: [ 3429.775757] iptables denied: IN=enp0s3 OUT= MAC=08:00:27:c0:bb:
df:08:00:27:d8:c8:d5:08:00 SRC=10.0.2.19 DST=10.0.2.17 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=8945 DF P
ROTO=TCP SPT=51476 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0
Feb 23 03:02:40 techtools kernel: [ 3437.970088] iptables denied: IN=enp0s3 OUT= MAC=08:00:27:c0:bb:
df:08:00:27:d8:c8:d5:08:00 SRC=10.0.2.19 DST=10.0.2.17 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=8946 DF P
ROTO=TCP SPT=51476 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0
Feb 23 03:02:56 techtools kernel: [ 3454.103450] iptables denied: IN=enp0s3 OUT= MAC=08:00:27:c0:bb:
df:08:00:27:d8:c8:d5:08:00 SRC=10.0.2.19 DST=10.0.2.17 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=8947 DF P
ROTO=TCP SPT=51476 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0
Feb 23 03:03:29 techtools kernel: [ 3487.394392] iptables denied: IN=enp0s3 OUT= MAC=08:00:27:c0:bb:
df:08:00:27:d8:c8:d5:08:00 SRC=10.0.2.19 DST=10.0.2.17 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=8948 DF P
ROTO=TCP SPT=51476 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0
Feb 23 03:03:48 techtools kernel: [ 3506.621842] iptables denied: IN=enp0s3 OUT= MAC=08:00:27:c0:bb:
df:08:00:27:d8:c8:d5:08:00 SRC=10.0.2.19 DST=10.0.2.17 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=23680 DF
PROTO=TCP SPT=51576 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0
Feb 23 03:03:49 techtools kernel: [ 3506.872501] iptables denied: IN=enp0s3 OUT= MAC=08:00:27:c0:bb:
df:08:00:27:d8:c8:d5:08:00 SRC=10.0.2.19 DST=10.0.2.17 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=38188 DF
PROTO=TCP SPT=51578 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0
Feb 23 03:03:49 techtools kernel: [ 3507.625858] iptables denied: IN=enp0s3 OUT= MAC=08:00:27:c0:bb:
df:08:00:27:d8:c8:d5:08:00 SRC=10.0.2.19 DST=10.0.2.17 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=23681 DF
PROTO=TCP SPT=51576 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0
Feb 23 03:03:50 techtools kernel: [ 3507.881317] iptables denied: IN=enp0s3 OUT= MAC=08:00:27:c0:bb:
df:08:00:27:d8:c8:d5:08:00 SRC=10.0.2.19 DST=10.0.2.17 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=38189 DF
PROTO=TCP SPT=51578 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0
Feb 23 03:03:51 techtools kernel: [ 3509.641778] iptables denied: IN=enp0s3 OUT= MAC=08:00:27:c0:bb:
df:08:00:27:d8:c8:d5:08:00 SRC=10.0.2.19 DST=10.0.2.17 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=23682 DF
PROTO=TCP SPT=51576 DPT=80 WINDOW=64240 RES=0x00 SYN URGP=0
_
```

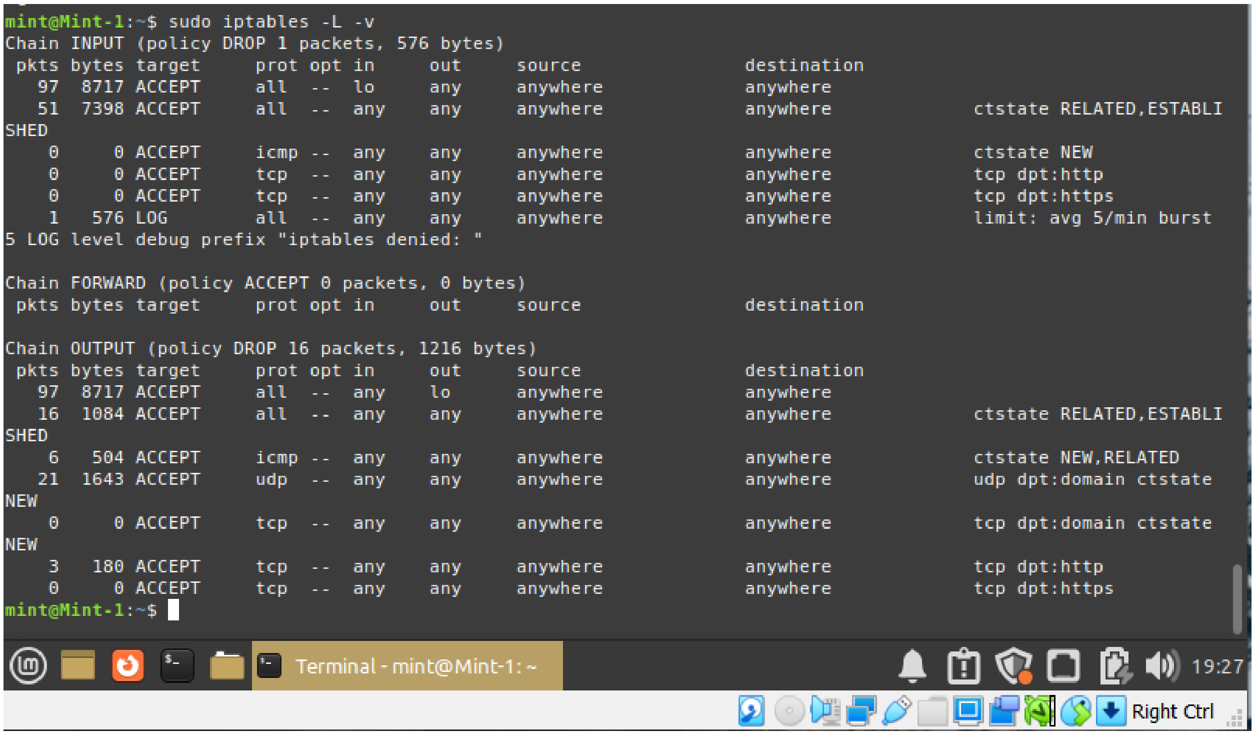
3. Iptables
ubuntu server



```
ubuntu@techtools:~$ sudo iptables -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1428  109K ACCEPT     all  --  lo     any     anywhere             anywhere
26245   39M ACCEPT     all  --  any    any     anywhere             anywhere             ctstate REL
ATED,ESTABLISHED
    1    84 ACCEPT     icmp --  any    any     anywhere             anywhere             ctstate NEW
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere             ctstate NEW
   14  1356 LOG        all  --  any    any     anywhere             anywhere             limit: avg
5/min burst 5 LOG level debug prefix "iptables denied: "
    1    60 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:htt
p
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:htt
ps

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1428  109K ACCEPT     all  --  any    lo      anywhere             anywhere
16904  680K ACCEPT     all  --  any    any     anywhere             anywhere             ctstate EST
ABLISHED
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere             ctstate NEW
,RELATED
    4   240 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:htt
p
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:htt
ps
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere             ctstate NEW
,RELATED
    9   673 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:dom
ain ctstate NEW
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:dom
ain ctstate NEW
ubuntu@techtools:~$
```

Matthew Zaldana
SID: 027008928

mint workstation



```
mint@Mint-1:~$ sudo iptables -L -v
Chain INPUT (policy DROP 1 packets, 576 bytes)
 pkts bytes target     prot opt in     out     source               destination
   97  8717 ACCEPT     all  --  lo     any     anywhere             anywhere
   51  7398 ACCEPT     all  --  any    any     anywhere             anywhere             ctstate RELATED,ESTABLI
SHED
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere             ctstate NEW
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:http
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:https
    1   576 LOG        all  --  any    any     anywhere             anywhere             limit: avg 5/min burst
5 LOG level debug prefix "iptables denied: "

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 16 packets, 1216 bytes)
 pkts bytes target     prot opt in     out     source               destination
   97  8717 ACCEPT     all  --  any    lo      anywhere             anywhere
   16  1084 ACCEPT     all  --  any    any     anywhere             anywhere             ctstate RELATED,ESTABLI
SHED
    6   504 ACCEPT     icmp --  any    any     anywhere             anywhere             ctstate NEW,RELATED
   21  1643 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:domain ctstate
NEW
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:domain ctstate
NEW
    3   180 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:http
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:https
mint@Mint-1:~$ 
```

Part 2

Command would be

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

This allows inbound traffic on port 80 which is the port for http requests