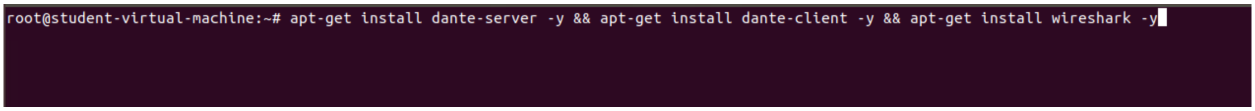
Network Security and Forensics
CSEC.462.01

Lab 3

Student: Wissam El Labban

Table of Contents

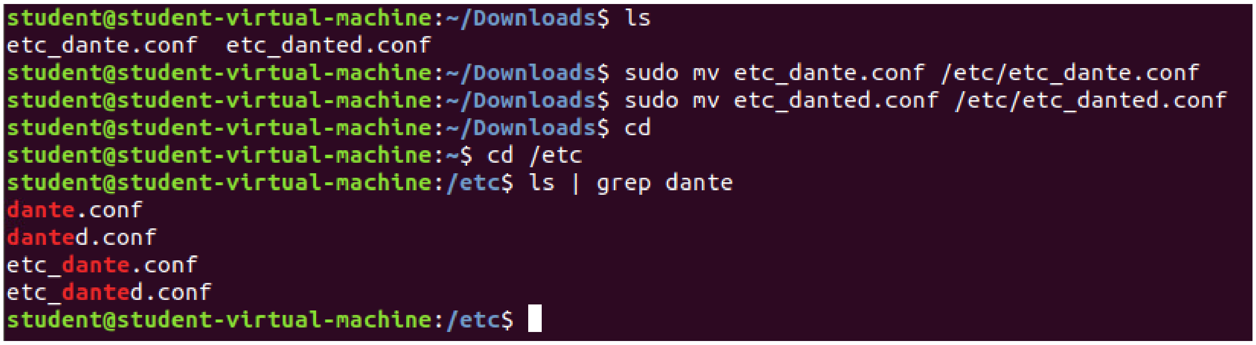
Installing Dante Server on Ubuntu



```
root@student-virtual-machine:~# apt-get install dante-server -y && apt-get install dante-client -y && apt-get install wireshark -y
```

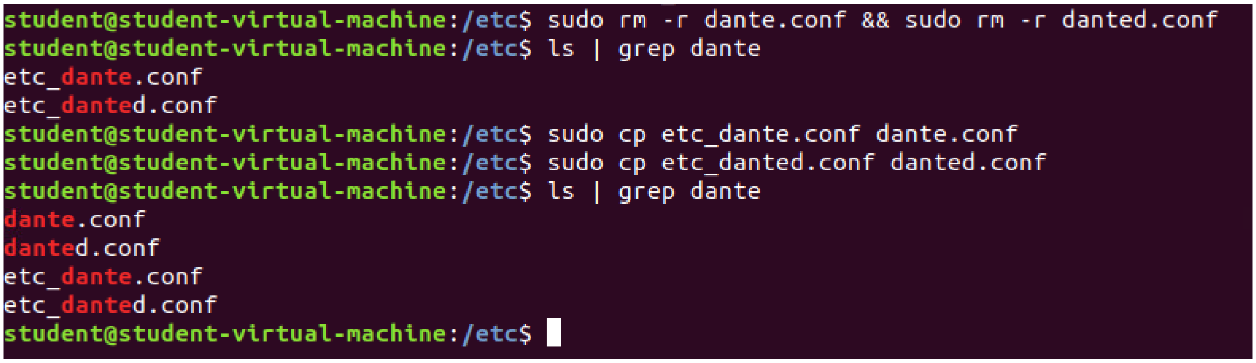
Using the command above, I installed the Dante server, client, and wireshark.

Downloading and moving the conf files to the /etc directory



```
student@student-virtual-machine:~/Downloads$ ls
etc_dante.conf  etc_danted.conf
student@student-virtual-machine:~/Downloads$ sudo mv etc_dante.conf /etc/etc_dante.conf
student@student-virtual-machine:~/Downloads$ sudo mv etc_danted.conf /etc/etc_danted.conf
student@student-virtual-machine:~/Downloads$ cd
student@student-virtual-machine:~$ cd /etc
student@student-virtual-machine:/etc$ ls | grep dante
dante.conf
danted.conf
etc_dante.conf
etc_danted.conf
student@student-virtual-machine:/etc$ 
```

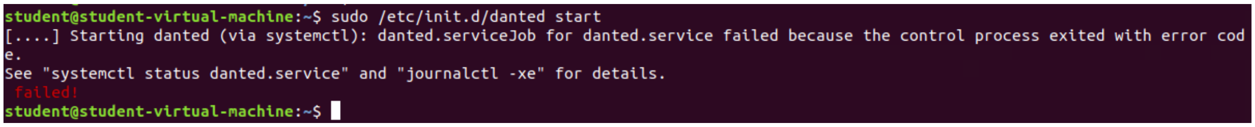
After downloading the config files from mycourses, I moved them into the etc directory.



```
student@student-virtual-machine:/etc$ sudo rm -r dante.conf && sudo rm -r danted.conf
student@student-virtual-machine:/etc$ ls | grep dante
etc_dante.conf
etc_danted.conf
student@student-virtual-machine:/etc$ sudo cp etc_dante.conf dante.conf
student@student-virtual-machine:/etc$ sudo cp etc_danted.conf danted.conf
student@student-virtual-machine:/etc$ ls | grep dante
dante.conf
danted.conf
etc_dante.conf
etc_danted.conf
student@student-virtual-machine:/etc$ 
```

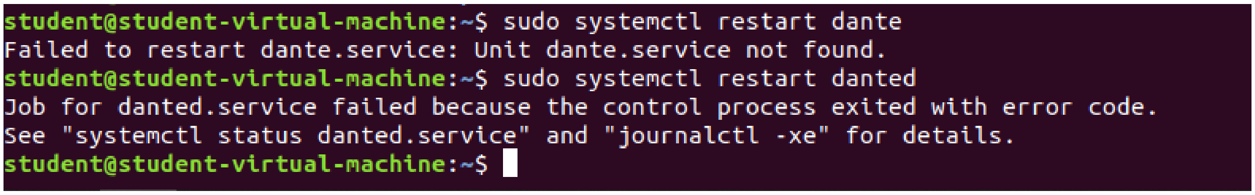
I removed the original files and copied the contents of the downloaded files into new config files. The names of the new files should be the same as the original config files if they are to be used by the dante services.

Starting the Dante server



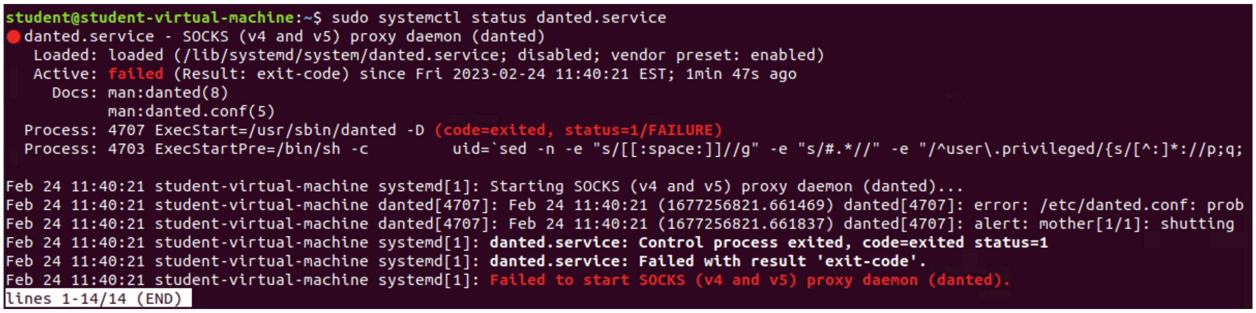
```
student@student-virtual-machine:~$ sudo /etc/init.d/danted start
[....] Starting danted (via systemctl): danted.serviceJob for danted.service failed because the control process exited with error cod
e.
See "systemctl status danted.service" and "journalctl -xe" for details.
 failed!
student@student-virtual-machine:~$ 
```

I cannot start the dante service since there is an error.

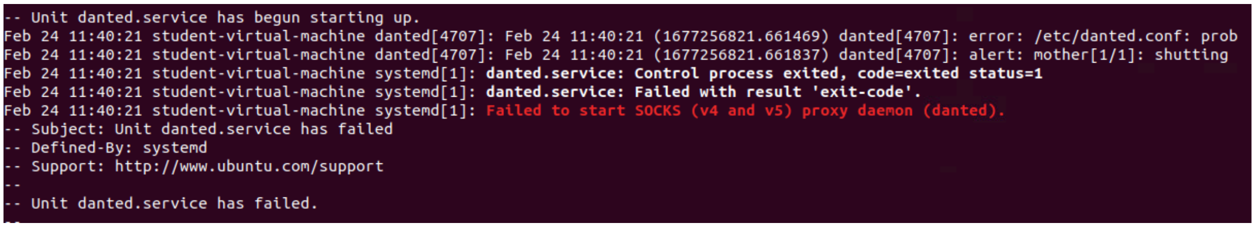


```
student@student-virtual-machine:~$ sudo systemctl restart dante
Failed to restart dante.service: Unit dante.service not found.
student@student-virtual-machine:~$ sudo systemctl restart danted
Job for danted.service failed because the control process exited with error code.
See "systemctl status danted.service" and "journalctl -xe" for details.
student@student-virtual-machine:~$ 
```

Attempting a restart also gives the same error.

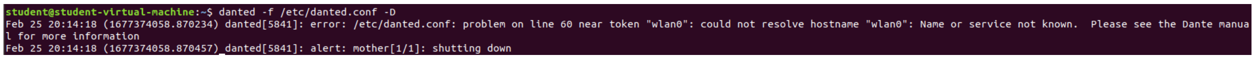


```
student@student-virtual-machine:~$ sudo systemctl status danted.service
● danted.service - SOCKS (v4 and v5) proxy daemon (danted)
   Loaded: loaded (/lib/systemd/system/danted.service; disabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Fri 2023-02-24 11:40:21 EST; 1min 47s ago
     Docs: man:danted(8)
           man:danted.conf(5)
  Process: 4707 ExecStart=/usr/sbin/danted -D (code=exited, status=1/FAILURE)
  Process: 4703 ExecStartPre=/bin/sh -c         uid=`sed -n -e "s/[[:space:]]//g" -e "s/#.*//" -e "/^user\.privileged/{s/[^:]*://p;q;

Feb 24 11:40:21 student-virtual-machine systemd[1]: Starting SOCKS (v4 and v5) proxy daemon (danted)...
Feb 24 11:40:21 student-virtual-machine danted[4707]: Feb 24 11:40:21 (1677256821.661469) danted[4707]: error: /etc/danted.conf: prob
Feb 24 11:40:21 student-virtual-machine danted[4707]: Feb 24 11:40:21 (1677256821.661837) danted[4707]: alert: mother[1/1]: shutting
Feb 24 11:40:21 student-virtual-machine systemd[1]: danted.service: Control process exited, code=exited status=1
Feb 24 11:40:21 student-virtual-machine systemd[1]: danted.service: Failed with result 'exit-code'.
Feb 24 11:40:21 student-virtual-machine systemd[1]: Failed to start SOCKS (v4 and v5) proxy daemon (danted).
lines 1-14/14 (END)
```



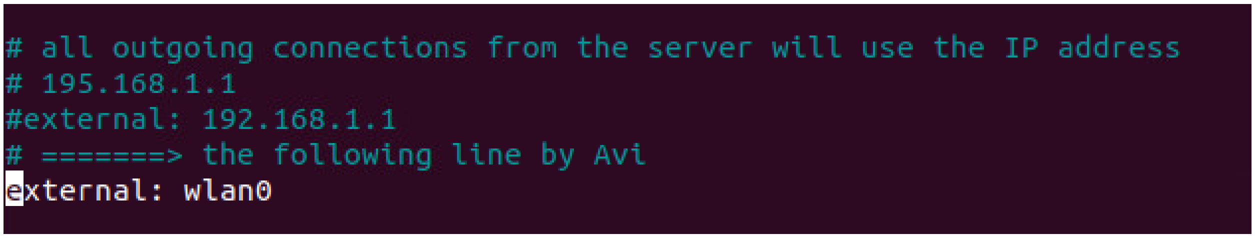
```
-- Unit danted.service has begun starting up.
Feb 24 11:40:21 student-virtual-machine danted[4707]: Feb 24 11:40:21 (1677256821.661469) danted[4707]: error: /etc/danted.conf: prob
Feb 24 11:40:21 student-virtual-machine danted[4707]: Feb 24 11:40:21 (1677256821.661837) danted[4707]: alert: mother[1/1]: shutting
Feb 24 11:40:21 student-virtual-machine systemd[1]: danted.service: Control process exited, code=exited status=1
Feb 24 11:40:21 student-virtual-machine systemd[1]: danted.service: Failed with result 'exit-code'.
Feb 24 11:40:21 student-virtual-machine systemd[1]: Failed to start SOCKS (v4 and v5) proxy daemon (danted).
-- Subject: Unit danted.service has failed
-- Defined-By: systemd
-- Support: http://www.ubuntu.com/support
--
-- Unit danted.service has failed.
```

After running systemctl status and journal -xe, I can tell that there is an exit code issue which indicates that there is a problem in the config files.



```
student@student-virtual-machine:~$ danted -f /etc/danted.conf -D
Feb 25 20:14:18 (1677374058.870234) danted[5841]: error: /etc/danted.conf: problem on line 60 near token "wlan0": could not resolve hostname "wlan0": Name or service not known.  Please see the Dante manua
l for more information
Feb 25 20:14:18 (1677374058.870457) danted[5841]: alert: mother[1/1]: shutting down
```

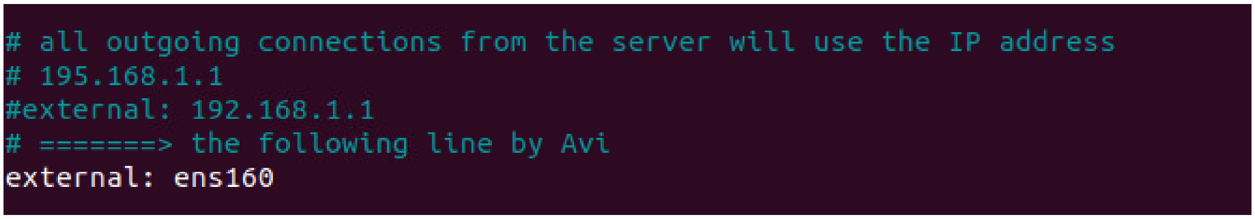
Using the command above, I checked the danted.conf file for syntax errors.



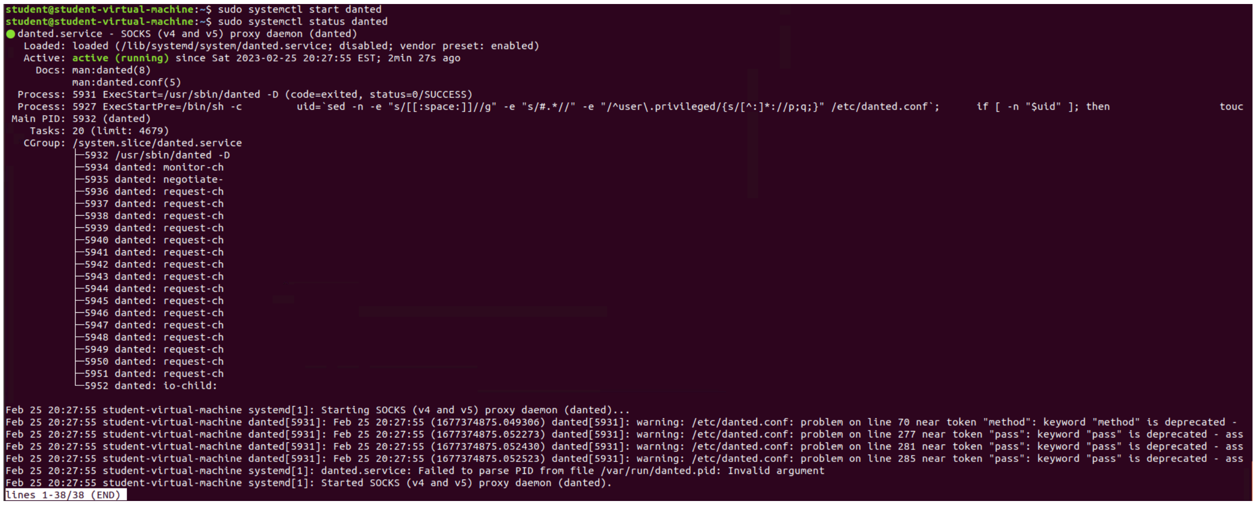
```
# all outgoing connections from the server will use the IP address
# 195.168.1.1
#external: 192.168.1.1
# =======> the following line by Avi
external: wlan0
```

I found that this was the line that was causing the issue.

I changed it to ens160 (the name if the Ubuntu NIC)

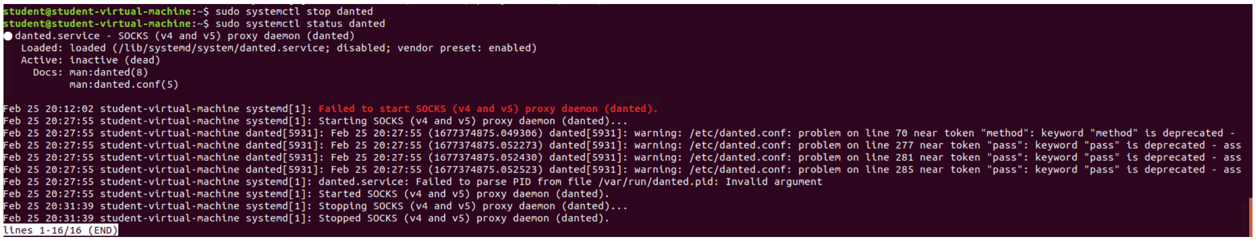


```
# all outgoing connections from the server will use the IP address
# 195.168.1.1
#external: 192.168.1.1
# =======> the following line by Avi
external: ens160
```



```
student@student-virtual-machine:~$ sudo systemctl start danted
student@student-virtual-machine:~$ sudo systemctl status danted
● danted.service - SOCKS (v4 and v5) proxy daemon (danted)
   Loaded: loaded (/lib/systemd/system/danted.service; disabled; vendor preset: enabled)
   Active: active (running) since Sat 2023-02-25 20:27:55 EST; 2min 27s ago
     Docs: man:danted(8)
           man:danted.conf(5)
  Process: 5931 ExecStart=/usr/sbin/danted -D (code=exited, status=0/SUCCESS)
  Process: 5927 ExecStartPre=/bin/sh -c         uid=`sed -n -e "s/[[:space:]]//g" -e "s/#.*//" -e "/^user\.privileged/{s/[^:]*://p;q;}" /etc/danted.conf`;      if [ -n "$uid" ]; then                 touc
 Main PID: 5932 (danted)
    Tasks: 20 (limit: 4679)
   CGroup: /system.slice/danted.service
           ├─5932 /usr/sbin/danted -D
           ├─5934 danted: monitor-ch
           ├─5935 danted: negotiate-
           ├─5936 danted: request-ch
           ├─5937 danted: request-ch
           ├─5938 danted: request-ch
           ├─5939 danted: request-ch
           ├─5940 danted: request-ch
           ├─5941 danted: request-ch
           ├─5942 danted: request-ch
           ├─5943 danted: request-ch
           ├─5944 danted: request-ch
           ├─5945 danted: request-ch
           ├─5946 danted: request-ch
           ├─5947 danted: request-ch
           ├─5948 danted: request-ch
           ├─5949 danted: request-ch
           ├─5950 danted: request-ch
           ├─5951 danted: request-ch
           └─5952 danted: io-child:

Feb 25 20:27:55 student-virtual-machine systemd[1]: Starting SOCKS (v4 and v5) proxy daemon (danted)...
Feb 25 20:27:55 student-virtual-machine danted[5931]: Feb 25 20:27:55 (1677374875.049306) danted[5931]: warning: /etc/danted.conf: problem on line 70 near token "method": keyword "method" is deprecated -
Feb 25 20:27:55 student-virtual-machine danted[5931]: Feb 25 20:27:55 (1677374875.052273) danted[5931]: warning: /etc/danted.conf: problem on line 277 near token "pass": keyword "pass" is deprecated - ass
Feb 25 20:27:55 student-virtual-machine danted[5931]: Feb 25 20:27:55 (1677374875.052430) danted[5931]: warning: /etc/danted.conf: problem on line 281 near token "pass": keyword "pass" is deprecated - ass
Feb 25 20:27:55 student-virtual-machine danted[5931]: Feb 25 20:27:55 (1677374875.052523) danted[5931]: warning: /etc/danted.conf: problem on line 285 near token "pass": keyword "pass" is deprecated - ass
Feb 25 20:27:55 student-virtual-machine systemd[1]: danted.service: Failed to parse PID from file /var/run/danted.pid: Invalid argument
Feb 25 20:27:55 student-virtual-machine systemd[1]: Started SOCKS (v4 and v5) proxy daemon (danted).
lines 1-38/38 (END)
```

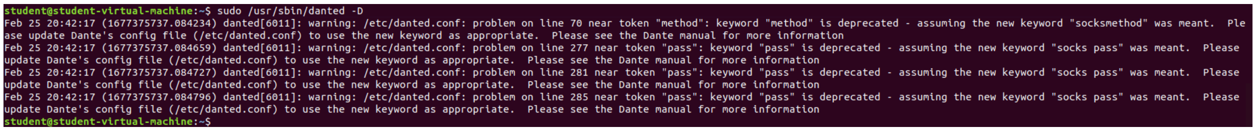
Starting the danted service is no problem now.



```
student@student-virtual-machine:~$ sudo systemctl stop danted
student@student-virtual-machine:~$ sudo systemctl status danted
● danted.service - SOCKS (v4 and v5) proxy daemon (danted)
   Loaded: loaded (/lib/systemd/system/danted.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:danted(8)
           man:danted.conf(5)

Feb 25 20:12:02 student-virtual-machine systemd[1]: Failed to start SOCKS (v4 and v5) proxy daemon (danted).
Feb 25 20:27:55 student-virtual-machine systemd[1]: Starting SOCKS (v4 and v5) proxy daemon (danted)...
Feb 25 20:27:55 student-virtual-machine danted[5931]: Feb 25 20:27:55 (1677374875.049306) danted[5931]: warning: /etc/danted.conf: problem on line 70 near token "method": keyword "method" is deprecated -
Feb 25 20:27:55 student-virtual-machine danted[5931]: Feb 25 20:27:55 (1677374875.052273) danted[5931]: warning: /etc/danted.conf: problem on line 277 near token "pass": keyword "pass" is deprecated - ass
Feb 25 20:27:55 student-virtual-machine danted[5931]: Feb 25 20:27:55 (1677374875.052430) danted[5931]: warning: /etc/danted.conf: problem on line 281 near token "pass": keyword "pass" is deprecated - ass
Feb 25 20:27:55 student-virtual-machine danted[5931]: Feb 25 20:27:55 (1677374875.052523) danted[5931]: warning: /etc/danted.conf: problem on line 285 near token "pass": keyword "pass" is deprecated - ass
Feb 25 20:27:55 student-virtual-machine systemd[1]: danted.service: Failed to parse PID from file /var/run/danted.pid: Invalid argument
Feb 25 20:27:55 student-virtual-machine systemd[1]: Started SOCKS (v4 and v5) proxy daemon (danted).
Feb 25 20:31:39 student-virtual-machine systemd[1]: Stopping SOCKS (v4 and v5) proxy daemon (danted)...
Feb 25 20:31:39 student-virtual-machine systemd[1]: Stopped SOCKS (v4 and v5) proxy daemon (danted).
lines 1-16/16 (END)
```

I now stopped the danted server.

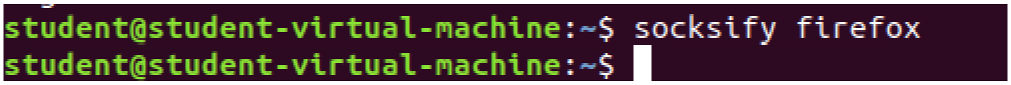
Bringing up danted server in debug mode



```
student@student-virtual-machine:~$ sudo /usr/sbin/danted -D
Feb 25 20:42:17 (1677375737.084234) danted[6011]: warning: /etc/danted.conf: problem on line 70 near token "method": keyword "method" is deprecated - assuming the new keyword "socksmethod" was meant.  Ple
ase update Dante's config file (/etc/danted.conf) to use the new keyword as appropriate.  Please see the Dante manual for more information
Feb 25 20:42:17 (1677375737.084659) danted[6011]: warning: /etc/danted.conf: problem on line 277 near token "pass": keyword "pass" is deprecated - assuming the new keyword "socks pass" was meant.  Please
update Dante's config file (/etc/danted.conf) to use the new keyword as appropriate.  Please see the Dante manual for more information
Feb 25 20:42:17 (1677375737.084727) danted[6011]: warning: /etc/danted.conf: problem on line 281 near token "pass": keyword "pass" is deprecated - assuming the new keyword "socks pass" was meant.  Please
update Dante's config file (/etc/danted.conf) to use the new keyword as appropriate.  Please see the Dante manual for more information
Feb 25 20:42:17 (1677375737.084796) danted[6011]: warning: /etc/danted.conf: problem on line 285 near token "pass": keyword "pass" is deprecated - assuming the new keyword "socks pass" was meant.  Please
update Dante's config file (/etc/danted.conf) to use the new keyword as appropriate.  Please see the Dante manual for more information
student@student-virtual-machine:~$
```

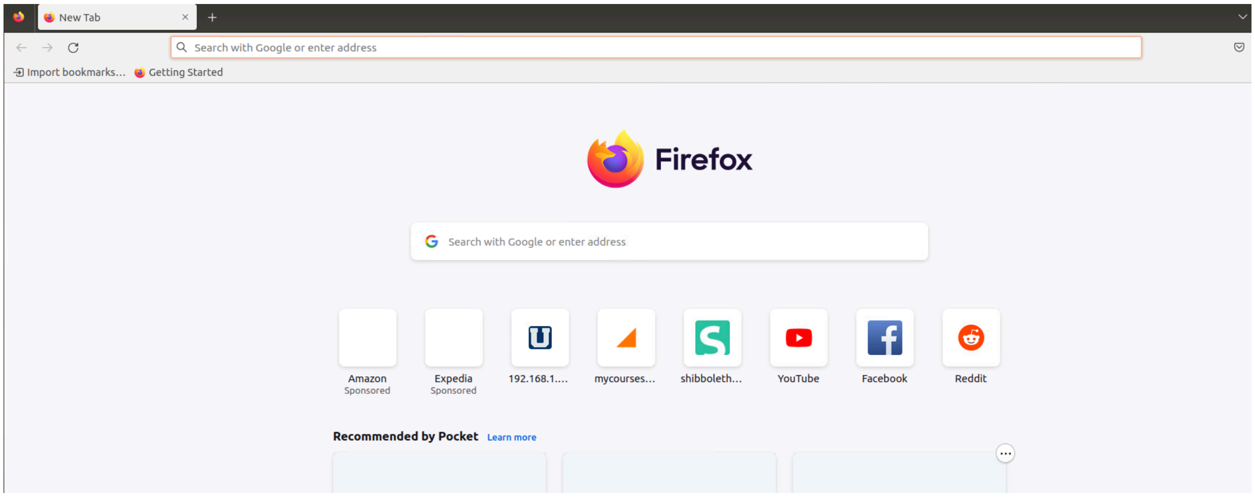
Using the command above, I started the server in debug mode. The -D flag is the debug flag and it lets the server run in debug mode where logs are verbosed and you can see more detailed information about the server's operation.

Socksify firefox



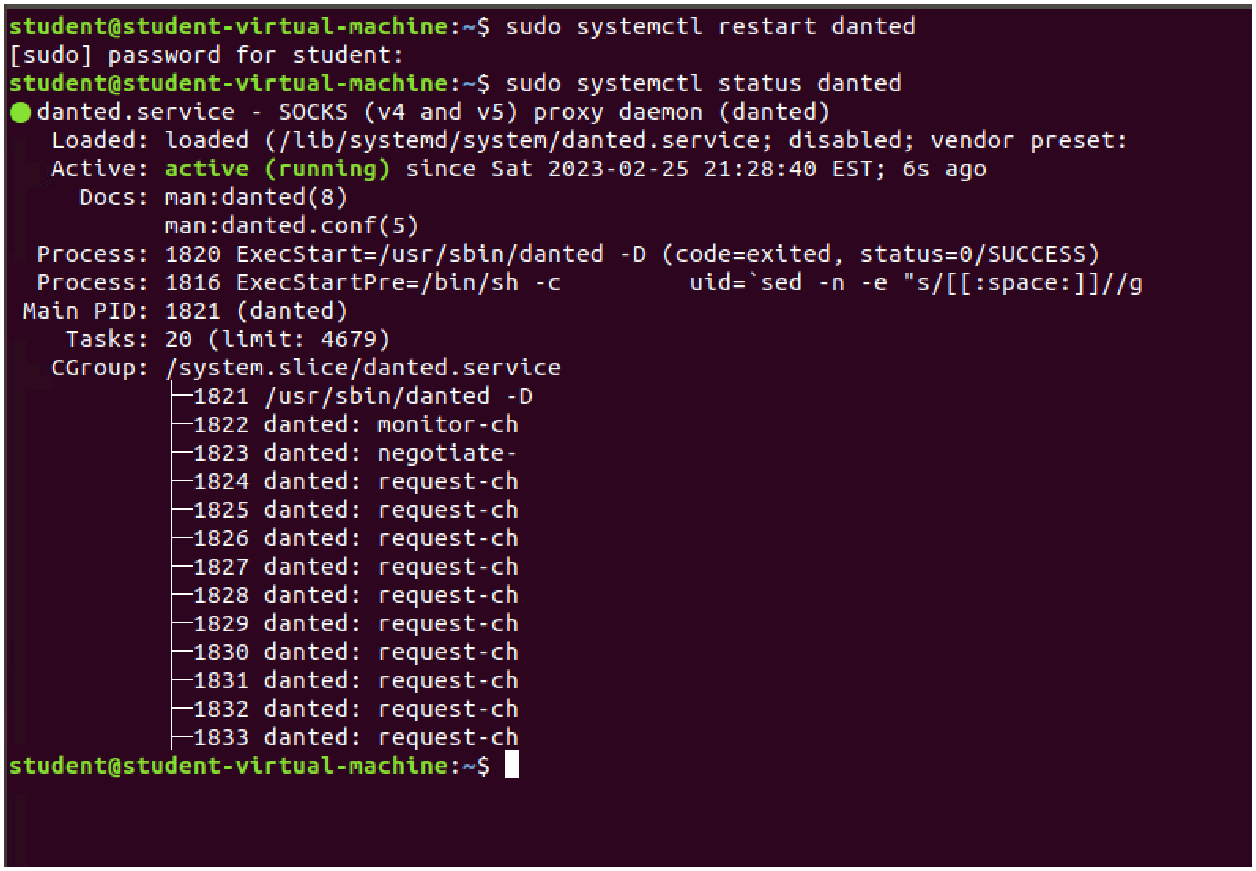
```
student@student-virtual-machine:~$ socksify firefox
student@student-virtual-machine:~$ 
```

After running the command, a firefox window pops up.



Any traffic that comes through this browser window will be redirected through the proxy server.

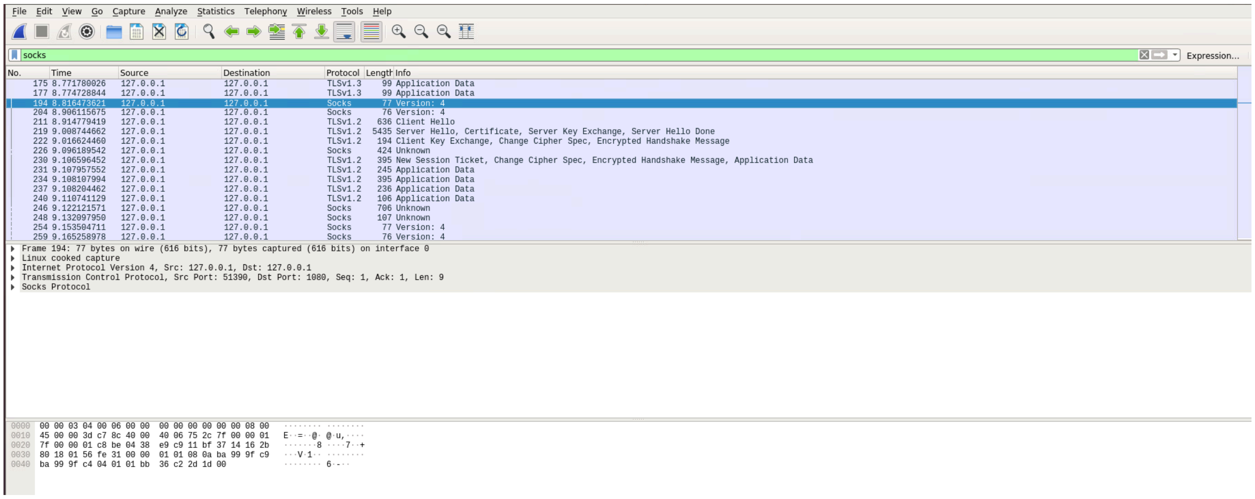
Observing Socks Traffic



```
student@student-virtual-machine:~$ sudo systemctl restart danted
[sudo] password for student:
student@student-virtual-machine:~$ sudo systemctl status danted
● danted.service - SOCKS (v4 and v5) proxy daemon (danted)
     Loaded: loaded (/lib/systemd/system/danted.service; disabled; vendor preset:
     Active: active (running) since Sat 2023-02-25 21:28:40 EST; 6s ago
       Docs: man:danted(8)
             man:danted.conf(5)
    Process: 1820 ExecStart=/usr/sbin/danted -D (code=exited, status=0/SUCCESS)
    Process: 1816 ExecStartPre=/bin/sh -c          uid=`sed -n -e "s/[[:space:]]//g
   Main PID: 1821 (danted)
      Tasks: 20 (limit: 4679)
     CGroup: /system.slice/danted.service
             ├─1821 /usr/sbin/danted -D
             ├─1822 danted: monitor-ch
             ├─1823 danted: negotiate-
             ├─1824 danted: request-ch
             ├─1825 danted: request-ch
             ├─1826 danted: request-ch
             ├─1827 danted: request-ch
             ├─1828 danted: request-ch
             ├─1829 danted: request-ch
             ├─1830 danted: request-ch
             ├─1831 danted: request-ch
             ├─1832 danted: request-ch
             ├─1833 danted: request-ch
student@student-virtual-machine:~$ 
```

Restarted the danted server

After I socksified firefox, I opened wireshark and went to a random website.



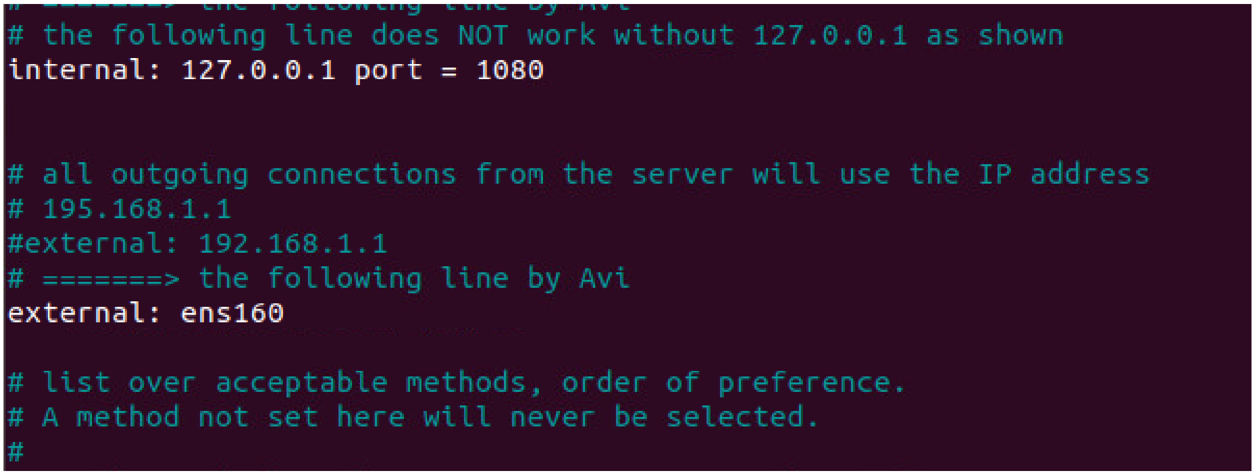
```
socks
```

```
No.    Time         Source       Destination  Protocol Length Info
   175 8.771780026  127.0.0.1    127.0.0.1    TLSv1.3    99 Application Data
   177 8.774728844  127.0.0.1    127.0.0.1    TLSv1.3    99 Application Data
   194 8.816473621  127.0.0.1    127.0.0.1    Socks      77 Version: 4
   204 8.906115675  127.0.0.1    127.0.0.1    Socks      76 Version: 4
   211 8.914779419  127.0.0.1    127.0.0.1    TLSv1.2   636 Client Hello
   219 9.008744662  127.0.0.1    127.0.0.1    TLSv1.2  5435 Server Hello, Certificate, Server Key Exchange, Server Hello Done
   222 9.016624460  127.0.0.1    127.0.0.1    TLSv1.2   194 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   226 9.096189542  127.0.0.1    127.0.0.1    Socks     424 Unknown
   230 9.106596452  127.0.0.1    127.0.0.1    TLSv1.2   395 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message, Application Data
   231 9.107957552  127.0.0.1    127.0.0.1    TLSv1.2   245 Application Data
   234 9.108107994  127.0.0.1    127.0.0.1    TLSv1.2   395 Application Data
   237 9.108204462  127.0.0.1    127.0.0.1    TLSv1.2   236 Application Data
   240 9.110741129  127.0.0.1    127.0.0.1    TLSv1.2   106 Application Data
   246 9.122121571  127.0.0.1    127.0.0.1    Socks     706 Unknown
   248 9.132097950  127.0.0.1    127.0.0.1    Socks     107 Unknown
   254 9.153504711  127.0.0.1    127.0.0.1    Socks      77 Version: 4
   259 9.165258978  127.0.0.1    127.0.0.1    Socks      76 Version: 4
```

```
▸ Frame 194: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ Transmission Control Protocol, Src Port: 51390, Dst Port: 1080, Seq: 1, Ack: 1, Len: 9
▸ Socks Protocol
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 00 3d c7 8c 40 00  40 06 75 2c 7f 00 00 01   E··=··@· @·u,····
0020  7f 00 00 01 c8 be 04 38  e9 c9 11 bf 37 14 16 2b   ·······8 ····7··+
0030  80 18 01 56 fe 31 00 00  01 01 08 0a ba 99 9f c9   ···V·1·· ········
0040  ba 99 9f c4 04 01 01 bb  36 c2 2d 1d 00            ········ 6·-··
```

The image above was captured on the loopback address on wireshark. It will not show up on the ens160 NIC.



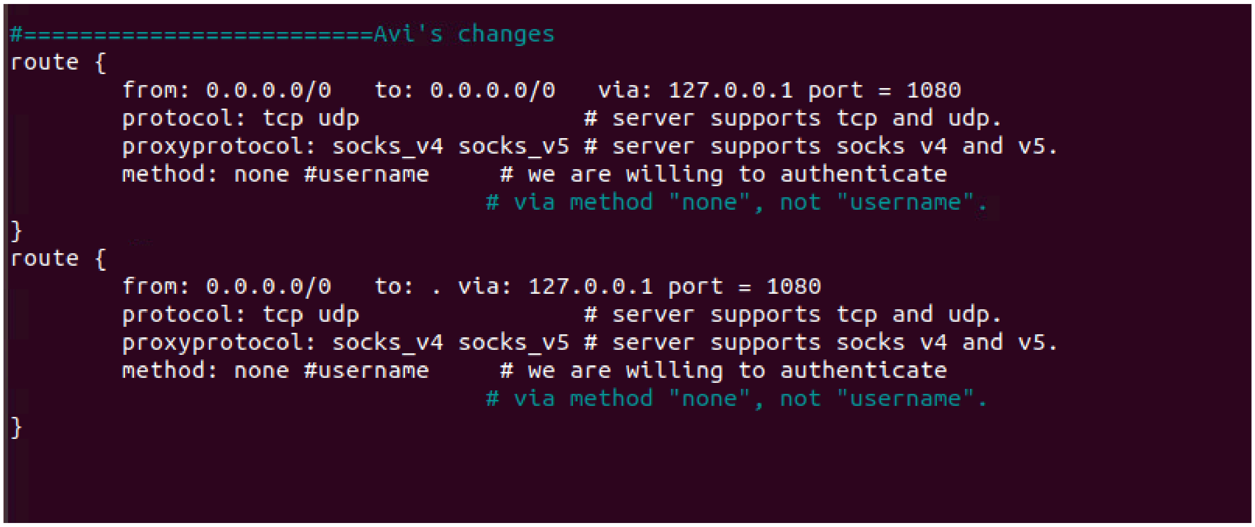
```
# =======> the following line by Avi
# the following line does NOT work without 127.0.0.1 as shown
internal: 127.0.0.1 port = 1080


# all outgoing connections from the server will use the IP address
# 195.168.1.1
#external: 192.168.1.1
# =======> the following line by Avi
external: ens160

# list over acceptable methods, order of preference.
# A method not set here will never be selected.
#
```

This configuration above means that the proxy server will only listen for connections on port 1080 on the loopback address while ens160 is the interface used to connect to the internet. No actual SOCKS packets will go through ens160.

No SOCKS packets will be picked up on the ens160 interface on wireshark since the dante server only allows socks traffic through the lo address 127.0.0.1

The proxy server is, in a sense, the lo address and the client is the machine itself.

Socks port, authentication, and 0.0.0.0./0 from dante.conf



```
#=========================Avi's changes
route {
        from: 0.0.0.0/0   to: 0.0.0.0/0   via: 127.0.0.1 port = 1080
        protocol: tcp udp                # server supports tcp and udp.
        proxyprotocol: socks_v4 socks_v5 # server supports socks v4 and v5.
        method: none #username     # we are willing to authenticate
                                  # via method "none", not "username".
}
route {
        from: 0.0.0.0/0   to: . via: 127.0.0.1 port = 1080
        protocol: tcp udp                # server supports tcp and udp.
        proxyprotocol: socks_v4 socks_v5 # server supports socks v4 and v5.
        method: none #username     # we are willing to authenticate
                                  # via method "none", not "username".
}
```

The socks server is connected on port 1080.

There is no authentication between the client and the proxy server. (method:none)

From: 0.0.0.0/0 means that all possible clients can connect to any destination through the socks proxy server.