COMP 8006 - Assignment #3 Annex

Mario Enriquez

British Columbia Institute of Technology

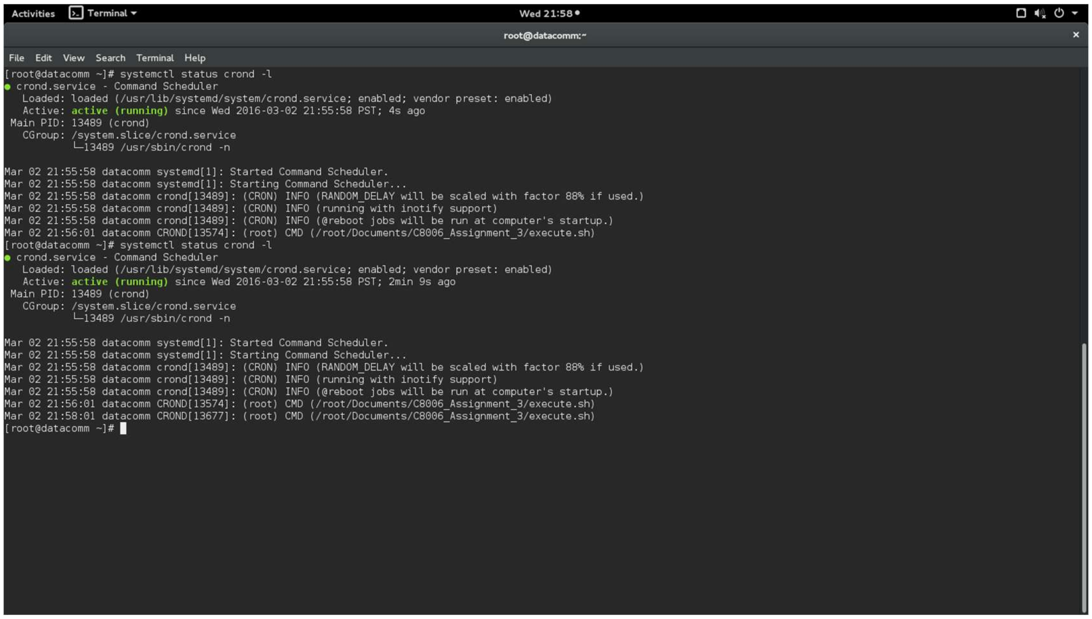
COMP 8005, COMP 6D

Aman Abdullah

2016-03-03

Contents

Test 1

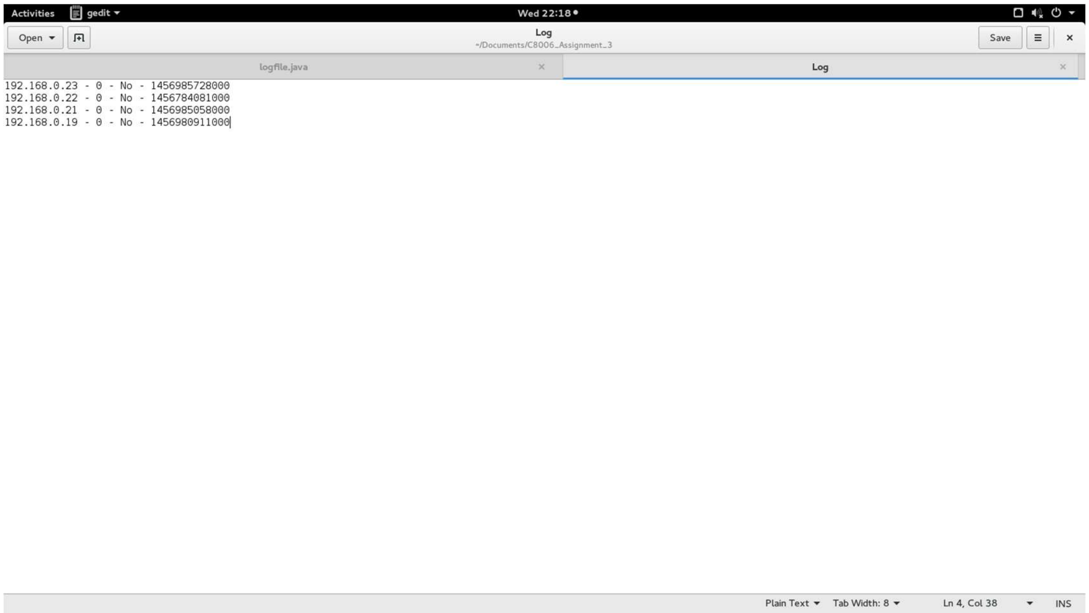


```
[root@datacomm ~]# systemctl status crond -l
● crond.service - Command Scheduler
   Loaded: loaded (/usr/lib/systemd/system/crond.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2016-03-02 21:55:58 PST; 4s ago
 Main PID: 13489 (crond)
   CGroup: /system.slice/crond.service
           └─13489 /usr/sbin/crond -n

Mar 02 21:55:58 datacomm systemd[1]: Started Command Scheduler.
Mar 02 21:55:58 datacomm systemd[1]: Starting Command Scheduler...
Mar 02 21:55:58 datacomm crond[13489]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 88% if used.)
Mar 02 21:55:58 datacomm crond[13489]: (CRON) INFO (running with inotify support)
Mar 02 21:55:58 datacomm crond[13489]: (CRON) INFO (@reboot jobs will be run at computer's startup.)
Mar 02 21:56:01 datacomm CROND[13574]: (root) CMD (/root/Documents/C8006_Assignment_3/execute.sh)
[root@datacomm ~]# systemctl status crond -l
● crond.service - Command Scheduler
   Loaded: loaded (/usr/lib/systemd/system/crond.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2016-03-02 21:55:58 PST; 2min 9s ago
 Main PID: 13489 (crond)
   CGroup: /system.slice/crond.service
           └─13489 /usr/sbin/crond -n

Mar 02 21:55:58 datacomm systemd[1]: Started Command Scheduler.
Mar 02 21:55:58 datacomm systemd[1]: Starting Command Scheduler...
Mar 02 21:55:58 datacomm crond[13489]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 88% if used.)
Mar 02 21:55:58 datacomm crond[13489]: (CRON) INFO (running with inotify support)
Mar 02 21:55:58 datacomm crond[13489]: (CRON) INFO (@reboot jobs will be run at computer's startup.)
Mar 02 21:56:01 datacomm CROND[13574]: (root) CMD (/root/Documents/C8006_Assignment_3/execute.sh)
Mar 02 21:58:01 datacomm CROND[13677]: (root) CMD (/root/Documents/C8006_Assignment_3/execute.sh)
[root@datacomm ~]#
```

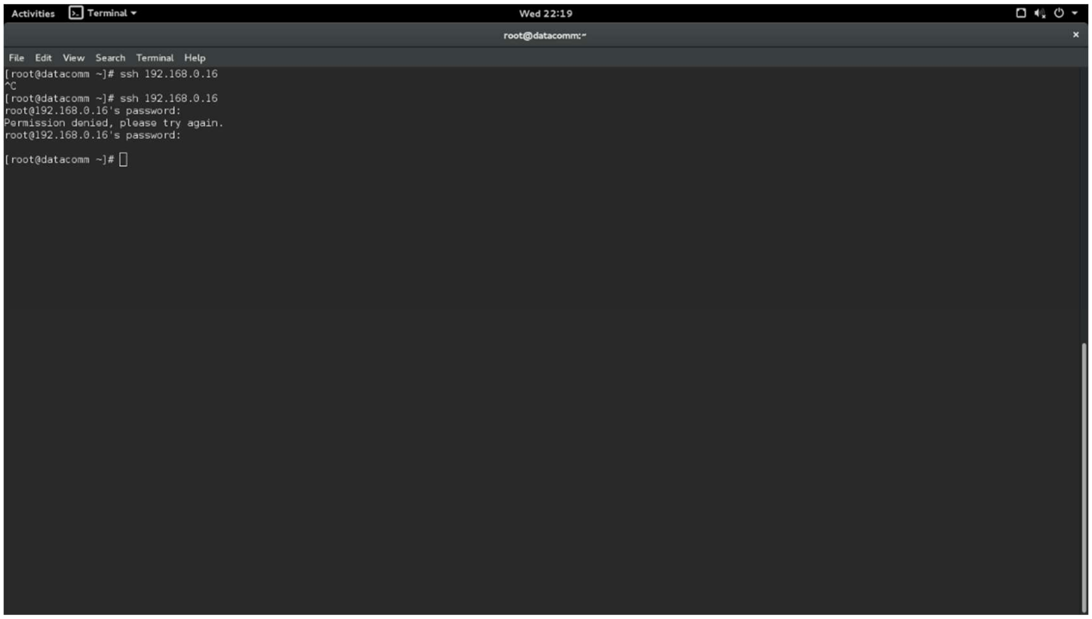
Figure 1 Cron logs



```
192.168.0.23 - 0 - No - 1456985728000
192.168.0.22 - 0 - No - 1456784081000
192.168.0.21 - 0 - No - 1456985058000
192.168.0.19 - 0 - No - 1456980911000
```

Figure 2 Server Logs

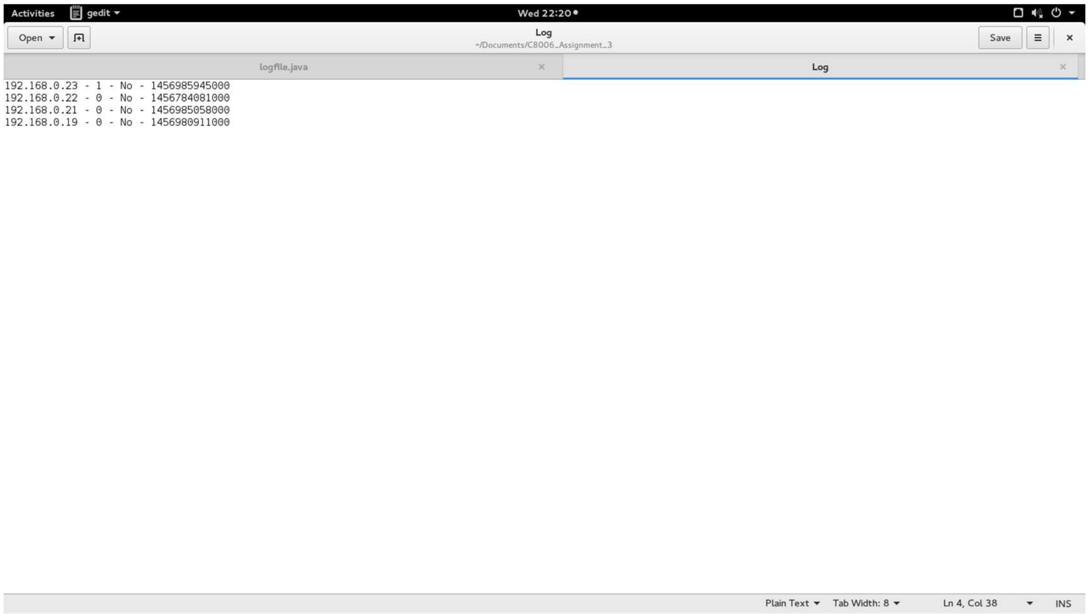
Test 2



```
[root@datacomm ~]# ssh 192.168.0.16
^C
[root@datacomm ~]# ssh 192.168.0.16
root@192.168.0.16's password:
Permission denied, please try again.
root@192.168.0.16's password:

[root@datacomm ~]# 
```

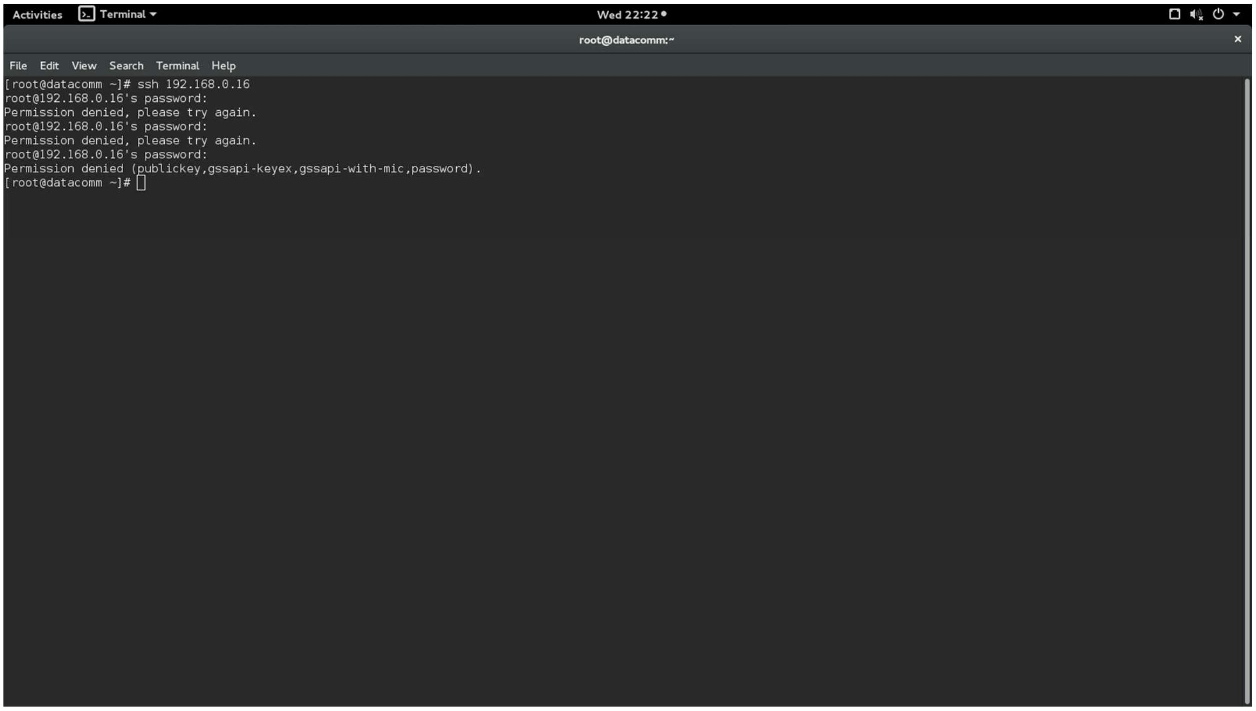
Figure 3 Client 192.168.0.23 Attempts



```
192.168.0.23 - 1 - No - 1456985945000
192.168.0.22 - 0 - No - 1456784081000
192.168.0.21 - 0 - No - 1456985058000
192.168.0.19 - 0 - No - 1456980911000
```

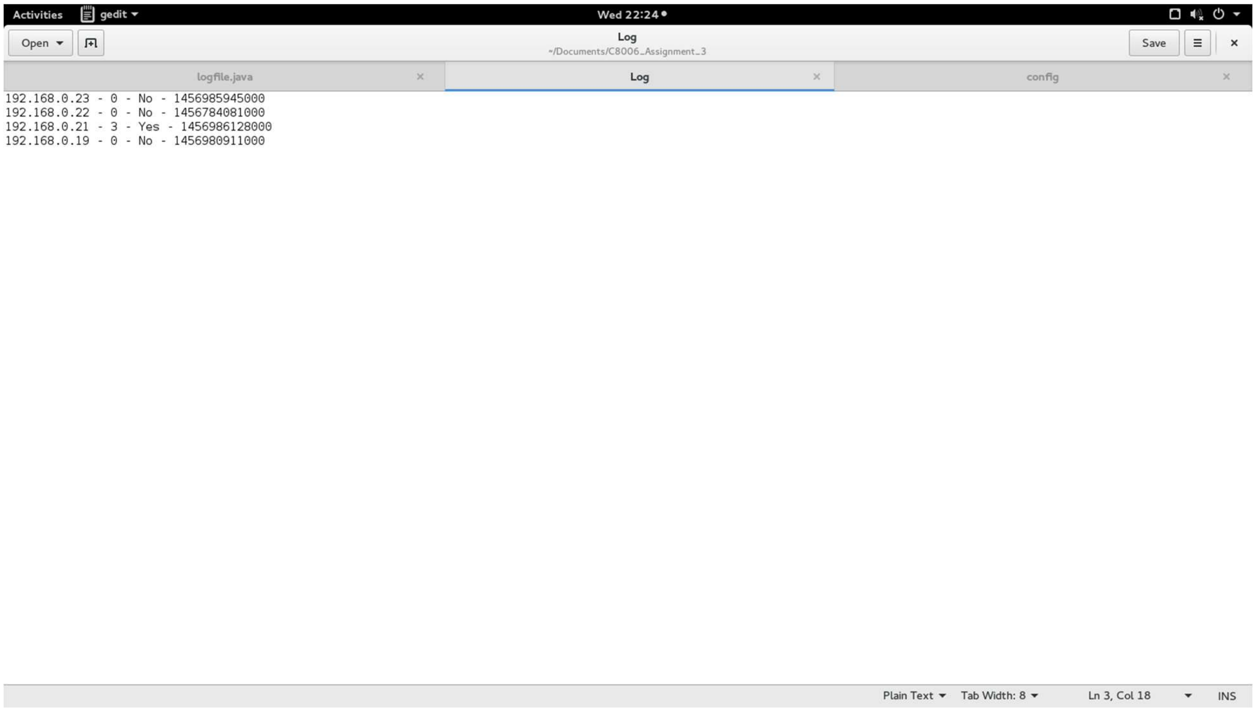
Figure 4 Logs from the Server

Test 3



```
[root@datacomm ~]# ssh 192.168.0.16
root@192.168.0.16's password:
Permission denied, please try again.
root@192.168.0.16's password:
Permission denied, please try again.
root@192.168.0.16's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@datacomm ~]# 
```

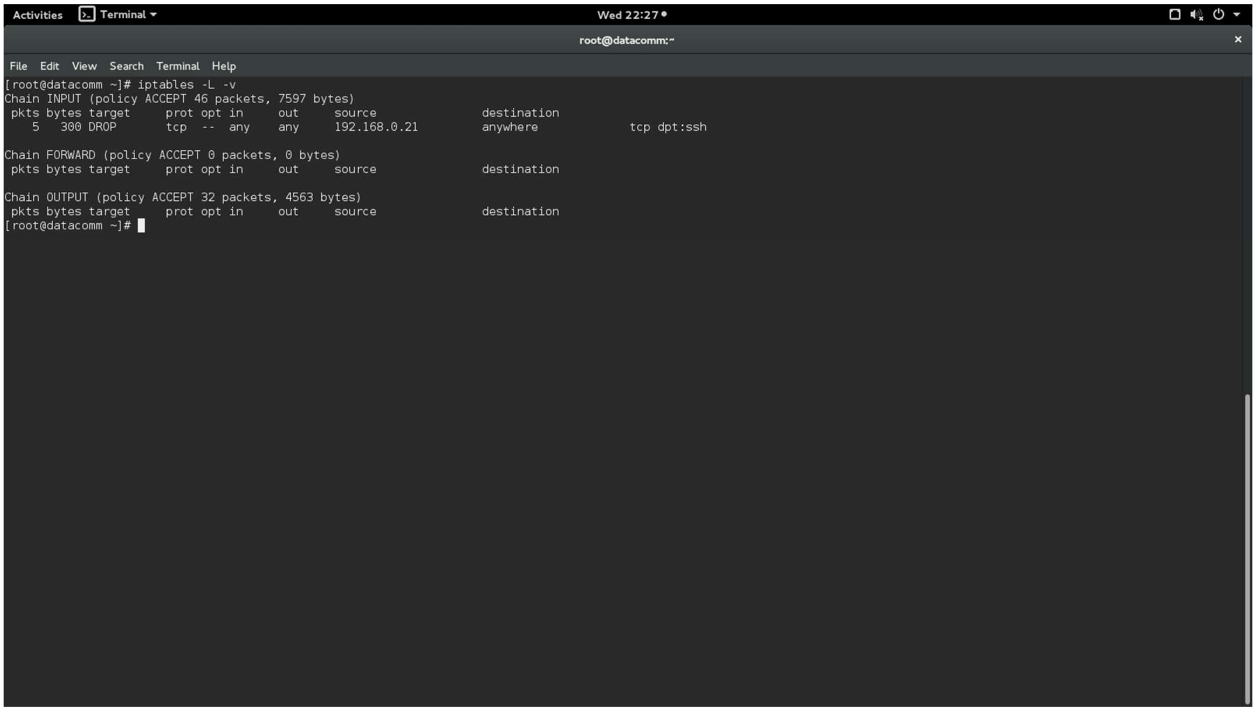
Figure 5 Client 192.168.0.21



```
192.168.0.23 - 0 - No - 1456985945000
192.168.0.22 - 0 - No - 1456784081000
192.168.0.21 - 3 - Yes - 1456986128000
192.168.0.19 - 0 - No - 1456980911000
```

Figure 6 Server Log after maximum number of retries reached

Test 3.1 Attempt to connect again

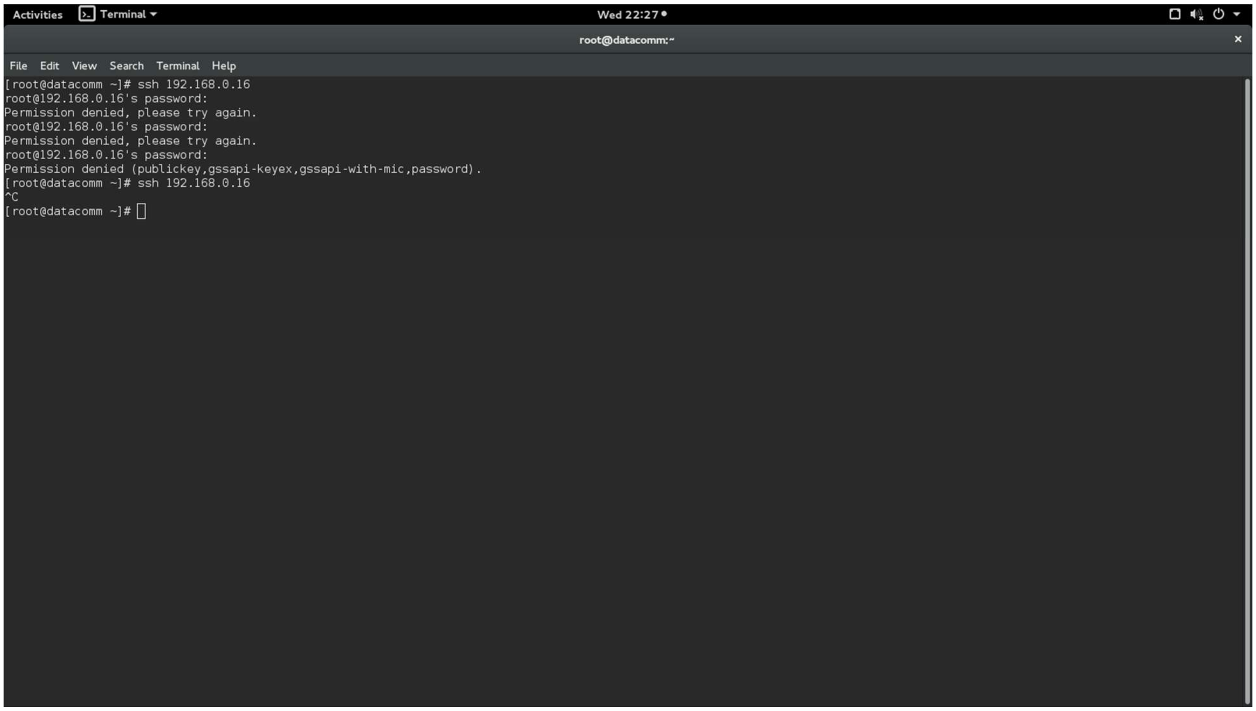


```
[root@datacomm ~]# iptables -L -v
Chain INPUT (policy ACCEPT 46 packets, 7597 bytes)
 pkts bytes target     prot opt in     out     source               destination
    5   300 DROP       tcp  --  any    any     192.168.0.21         anywhere             tcp dpt:ssh

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

Chain OUTPUT (policy ACCEPT 32 packets, 4563 bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@datacomm ~]# 
```

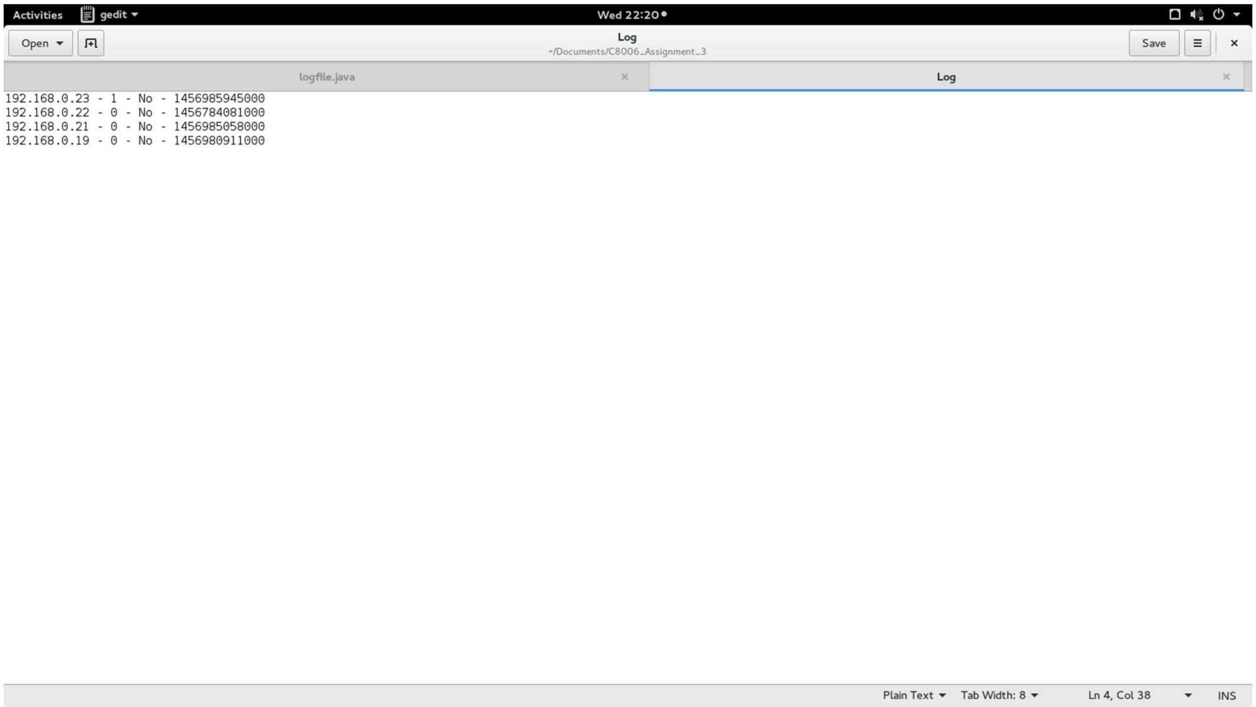
Figure 7 Iptables after blocking an user



```
[root@datacomm ~]# ssh 192.168.0.16
root@192.168.0.16's password:
Permission denied, please try again.
root@192.168.0.16's password:
Permission denied, please try again.
root@192.168.0.16's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@datacomm ~]# ssh 192.168.0.16
^C
[root@datacomm ~]# 
```

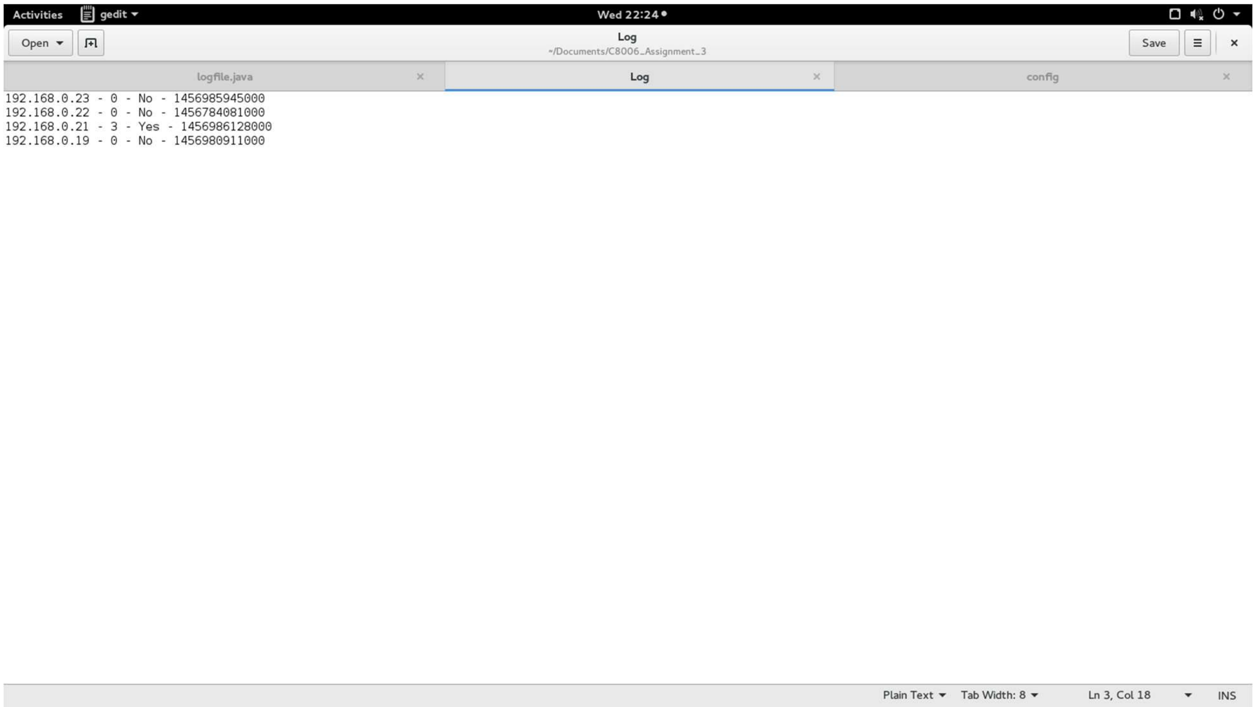
Figure 8 Failure to login since port is closed

Test 4



```
192.168.0.23 - 1 - No - 1456985945000
192.168.0.22 - 0 - No - 1456784081000
192.168.0.21 - 0 - No - 1456985058000
192.168.0.19 - 0 - No - 1456980911000
```

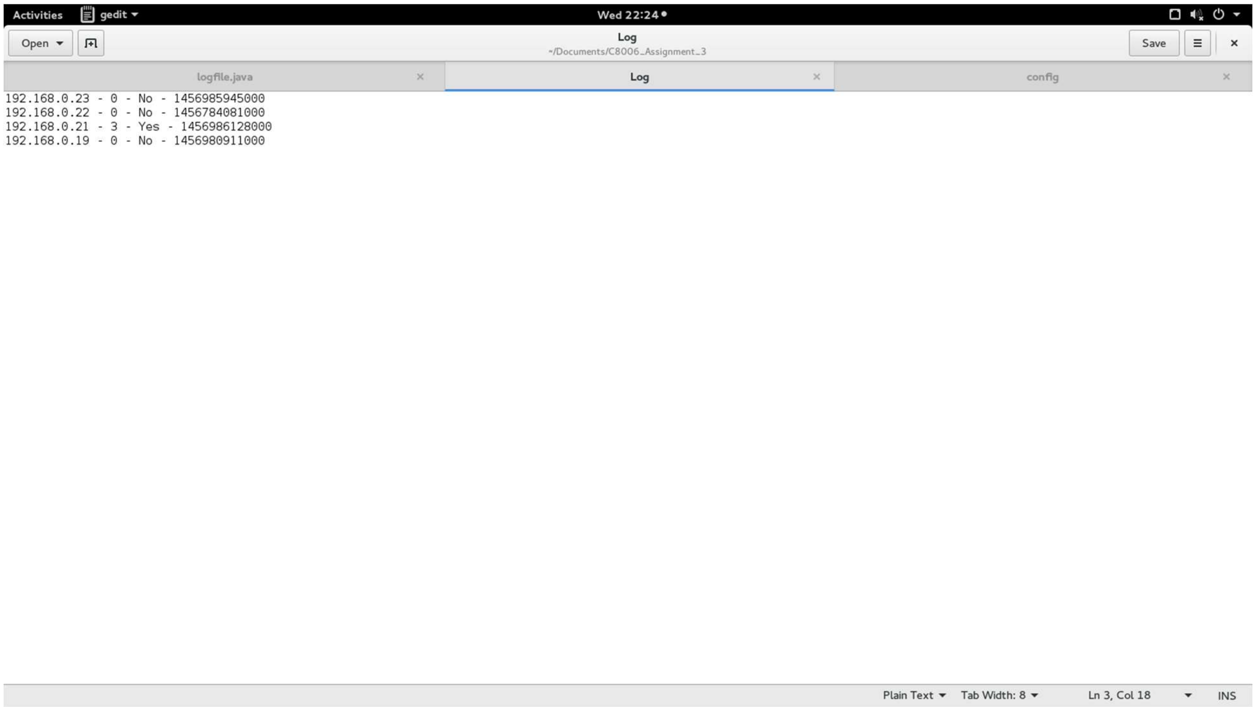
Figure 9 Log file after unsuccessful attempt



```
192.168.0.23 - 0 - No - 1456985945000
192.168.0.22 - 0 - No - 1456784081000
192.168.0.21 - 3 - Yes - 1456986128000
192.168.0.19 - 0 - No - 1456980911000
```

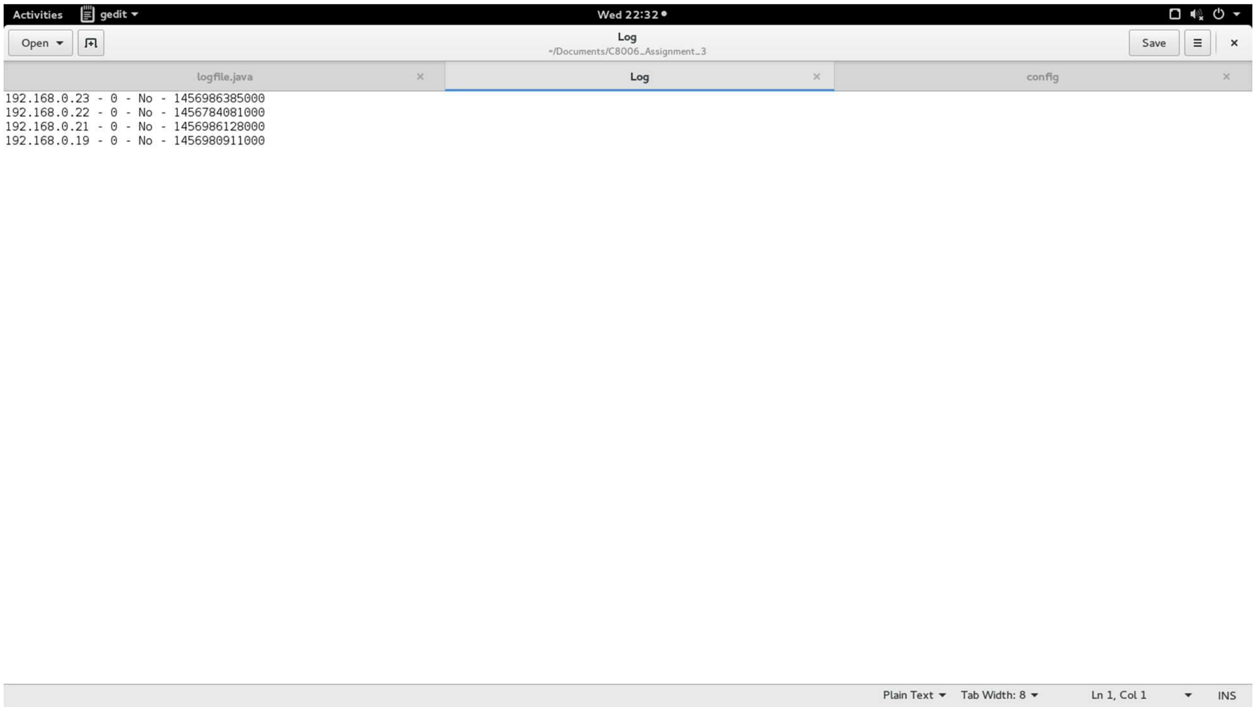
Figure 10 Log file after 4 minutes, removes unsuccessful attempts

Test 5



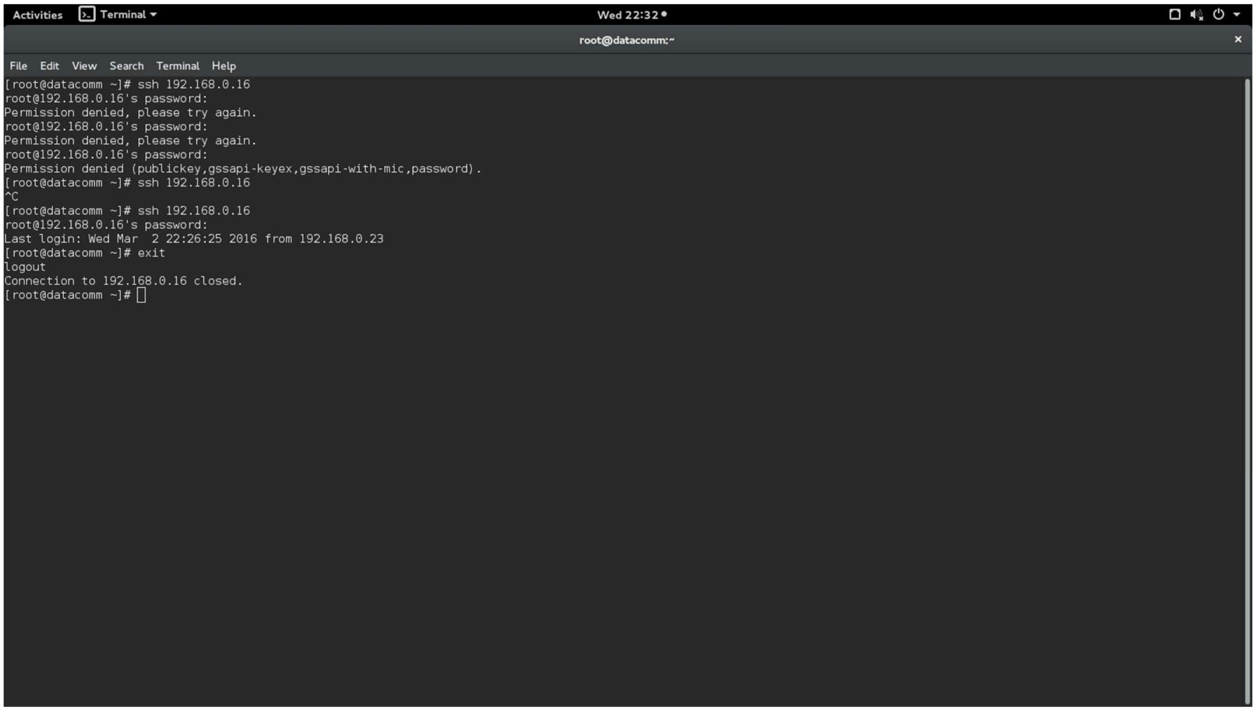
```
192.168.0.23 - 0 - No - 1456985945000
192.168.0.22 - 0 - No - 1456784081000
192.168.0.21 - 3 - Yes - 1456986128000
192.168.0.19 - 0 - No - 1456980911000
```

Figure 11 Log file after banning an Ip



```
192.168.0.23 - 0 - No - 1456986385000
192.168.0.22 - 0 - No - 1456784081000
192.168.0.21 - 0 - No - 1456986128000
192.168.0.19 - 0 - No - 1456980911000
```

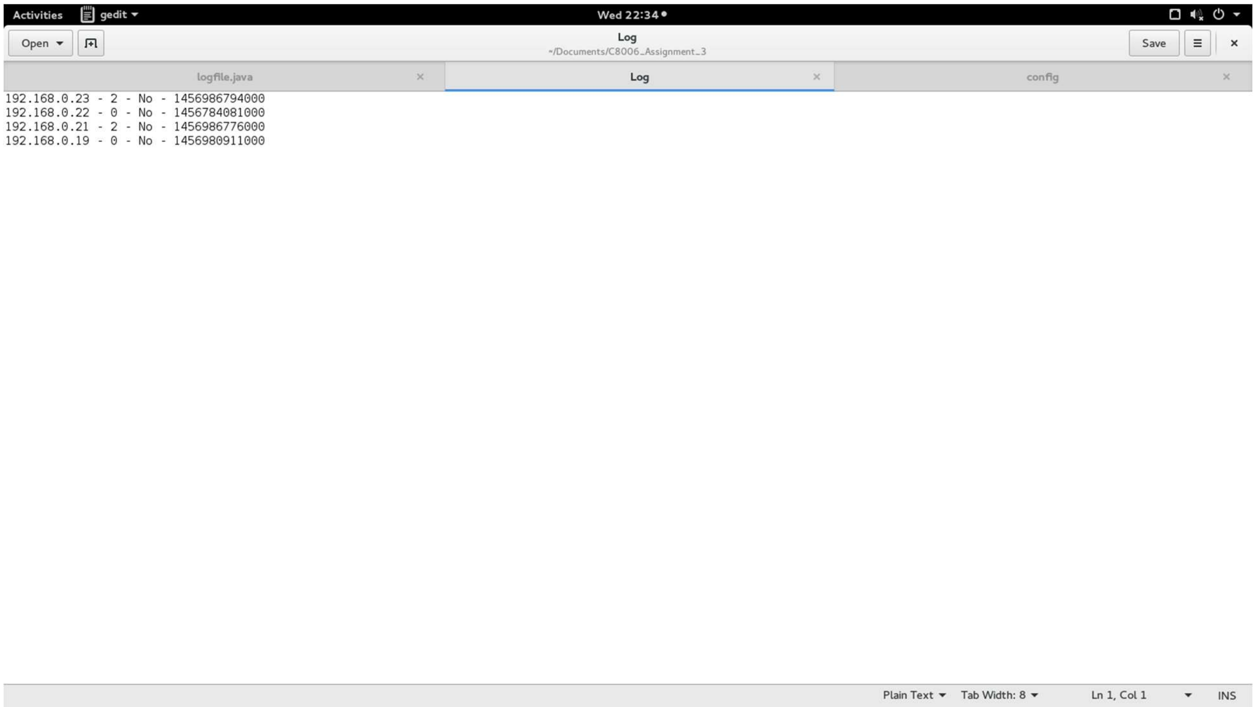
Figure 12 Log file after 8 minutes



```
[root@datacomm ~]# ssh 192.168.0.16
root@192.168.0.16's password:
Permission denied, please try again.
root@192.168.0.16's password:
Permission denied, please try again.
root@192.168.0.16's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@datacomm ~]# ssh 192.168.0.16
^C
[root@datacomm ~]# ssh 192.168.0.16
root@192.168.0.16's password:
Last login: Wed Mar  2 22:26:25 2016 from 192.168.0.23
[root@datacomm ~]# exit
logout
Connection to 192.168.0.16 closed.
[root@datacomm ~]# 
```

Figure 13 User is unbanned and can attempt to login again

Test 6



```
192.168.0.23 - 2 - No - 1456986794000
192.168.0.22 - 0 - No - 1456784081000
192.168.0.21 - 2 - No - 1456986776000
192.168.0.19 - 0 - No - 1456980911000
```

Figure 14 Log updates successfully only with the latest dates

Test 7