

COMP 8006 - Assignment #3 Annex

Mario Enriquez

British Columbia Institute of Technology

COMP 8005, COMP 6D

Aman Abdullah

2016-03-03

Contents

Test 1 3

Test 2 4

Test 3 5

Test 3.1 Attempt to connect again 6

Test 4 7

Test 5 8

Test 6 10

Test 7 11

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 21:56:01 datacomm CROND[13677]: (root) CMD (/root/Documents/C8006_Assignment_3/execute.sh)
root@datacomm:~#

```

Figure 1 Cron logs

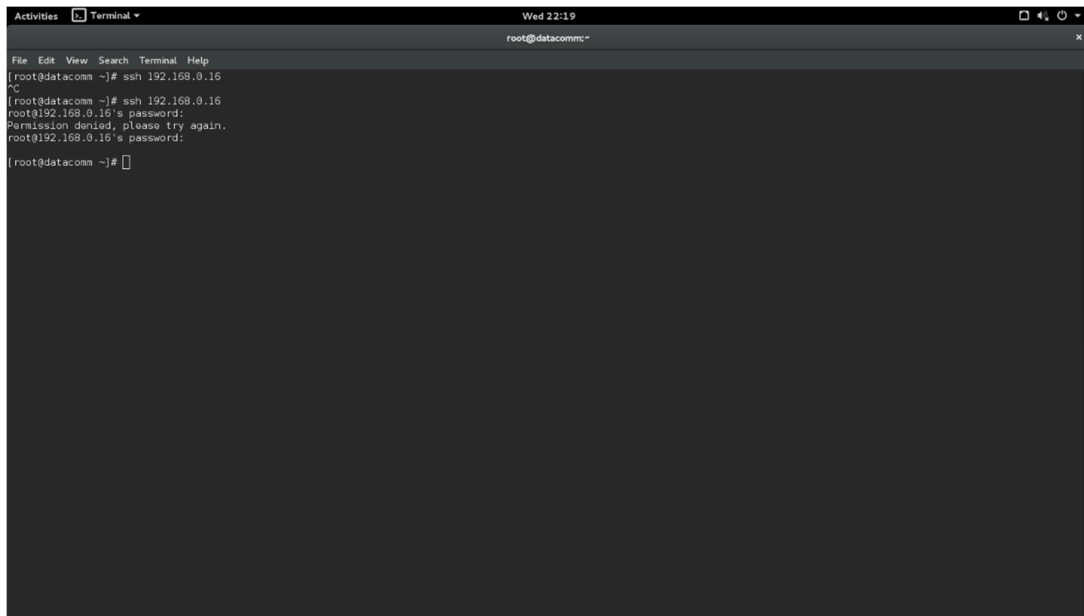
```

Log
~/Documents/C8006_Assignment_3
Save
Log
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

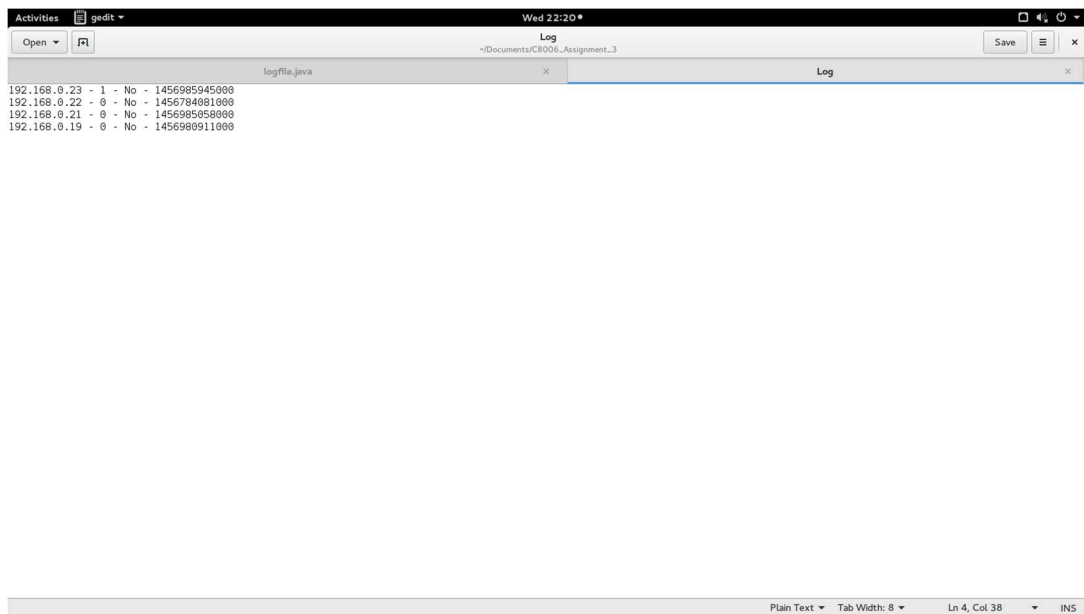
```

Plain Text ▾ Tab Width: 8 ▾ Ln 4, Col 38 ▾ INS

Figure 2 Server Logs

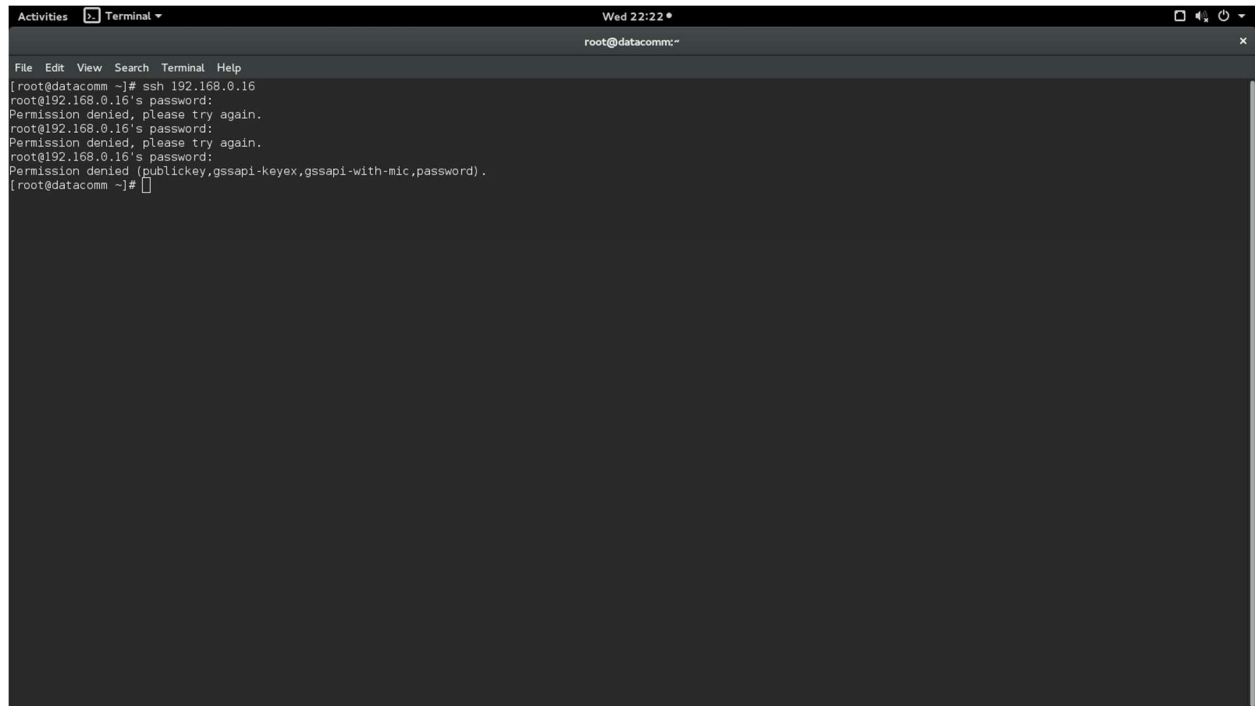
Test 2

```
Activities Terminal Wed 22:19
root@datacomm:~
File Edit View Search Terminal Help
[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

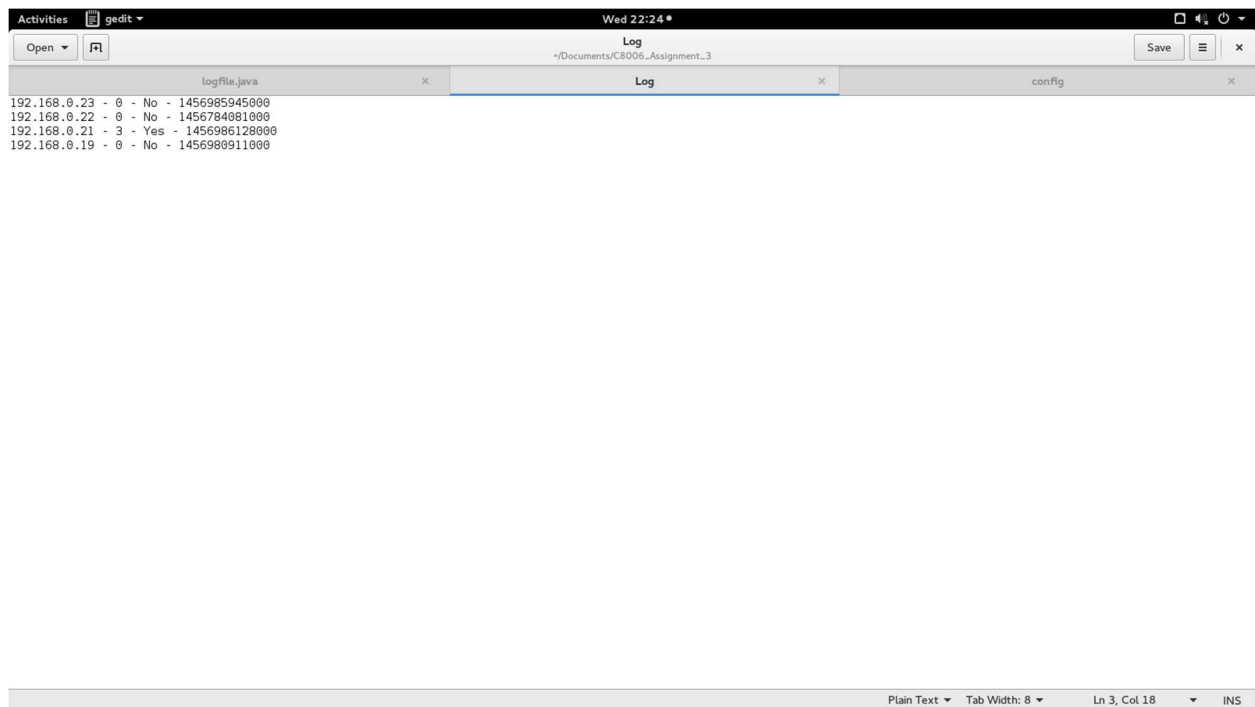
```
Activities gedit Wed 22:20
Log
~/Documents/C8006_Assignment_3
Save
logfile.java
Log
192.168.0.23 - 1 - No - 1456985945000
192.168.0.22 - 0 - No - 1456794081000
192.168.0.21 - 0 - No - 1456985058000
192.168.0.19 - 0 - No - 1456980911000
Plain Text Tab Width: 8 Ln 4, Col 38 INS
```

Figure 4 Logs from the Server

Test 3

A terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (root@datacomm ~). The terminal shows the following commands and output:

```
[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

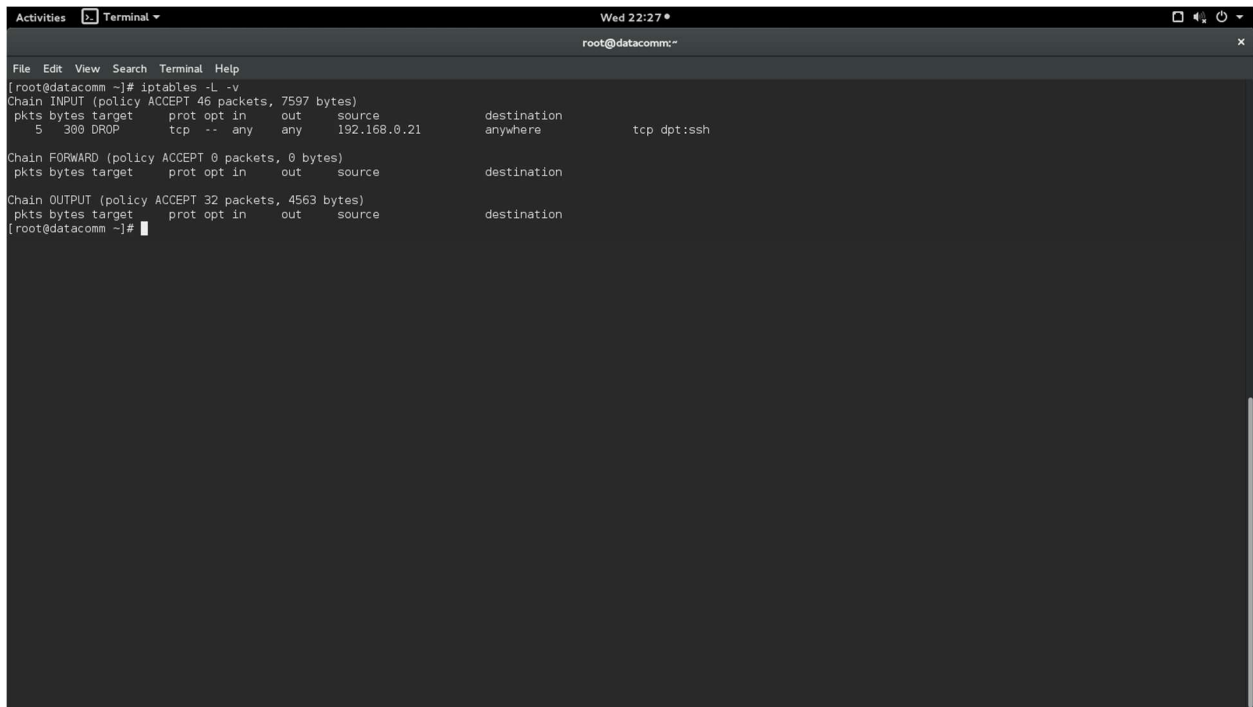
A Gedit editor window titled "gedit" with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Plain Text, Tab Width: 8, Ln 3, Col 18, INS). The editor shows a log file with the following entries:

```
logfile.java
Log
~/Documents/C8006_Assignment_3
Log
config
```

IP Address	Port	Protocol	Authentication	Result	Session ID
192.168.0.23	0	No	-	No	1456985945000
192.168.0.22	0	No	-	No	1456784081000
192.168.0.21	3	Yes	-	Yes	1456986128000
192.168.0.19	0	No	-	No	1456988911000

Figure 6 Server Log after maximum number of retries reached

Test 3.1 Attempt to connect again



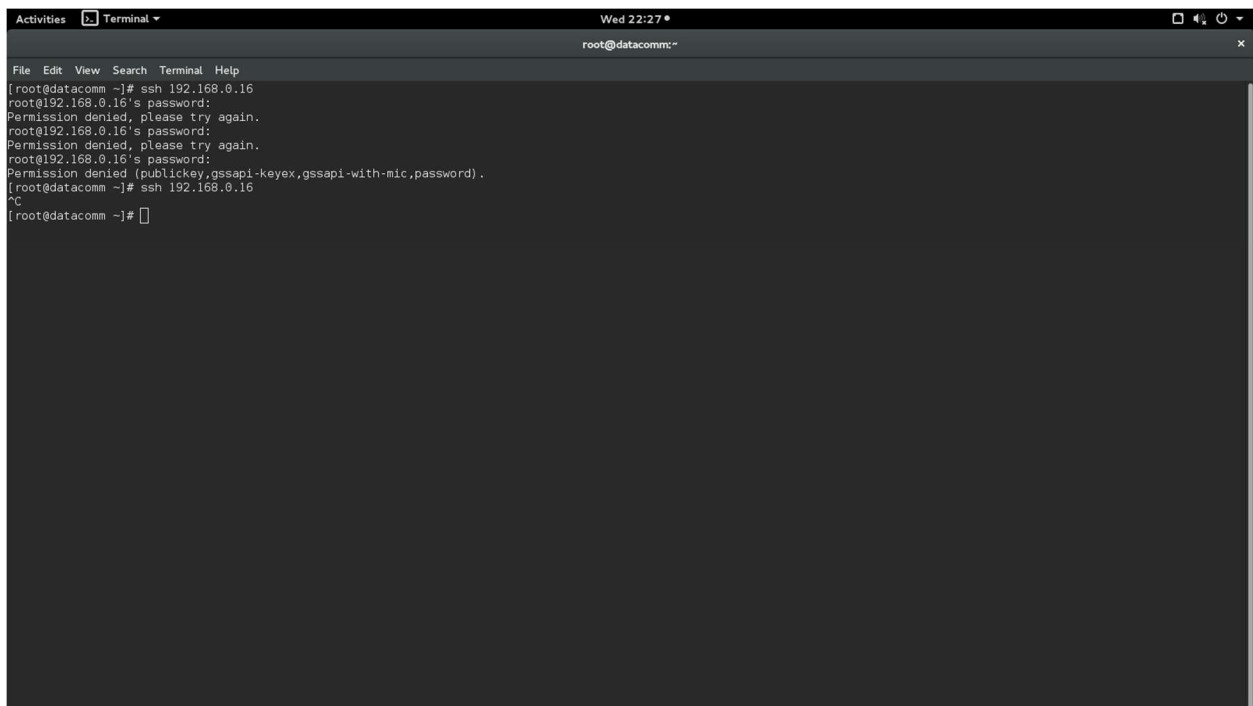
A terminal window titled "Terminal" with a subtitle "Wed 22:27" and a prompt "root@datacomm~". The terminal shows the output of the command "iptables -L -v". The output displays three chains: INPUT, FORWARD, and OUTPUT. The INPUT chain has a policy of ACCEPT and shows 46 packets and 7597 bytes accepted. The FORWARD chain has a policy of ACCEPT and shows 0 packets and 0 bytes accepted. The OUTPUT chain has a policy of ACCEPT and shows 32 packets and 4563 bytes accepted. The terminal also shows a rule for the INPUT chain that drops traffic from 192.168.0.21 to anywhere on port 22.

```
[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



A terminal window titled "Terminal" with a subtitle "Wed 22:27" and a prompt "root@datacomm~". The terminal shows the output of the command "ssh 192.168.0.16". The output displays three failed login attempts for the user "root" on host "192.168.0.16". The first two attempts are for password authentication, and the third is for publickey authentication. The terminal also shows the command "ssh 192.168.0.16" being entered again.

```
[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

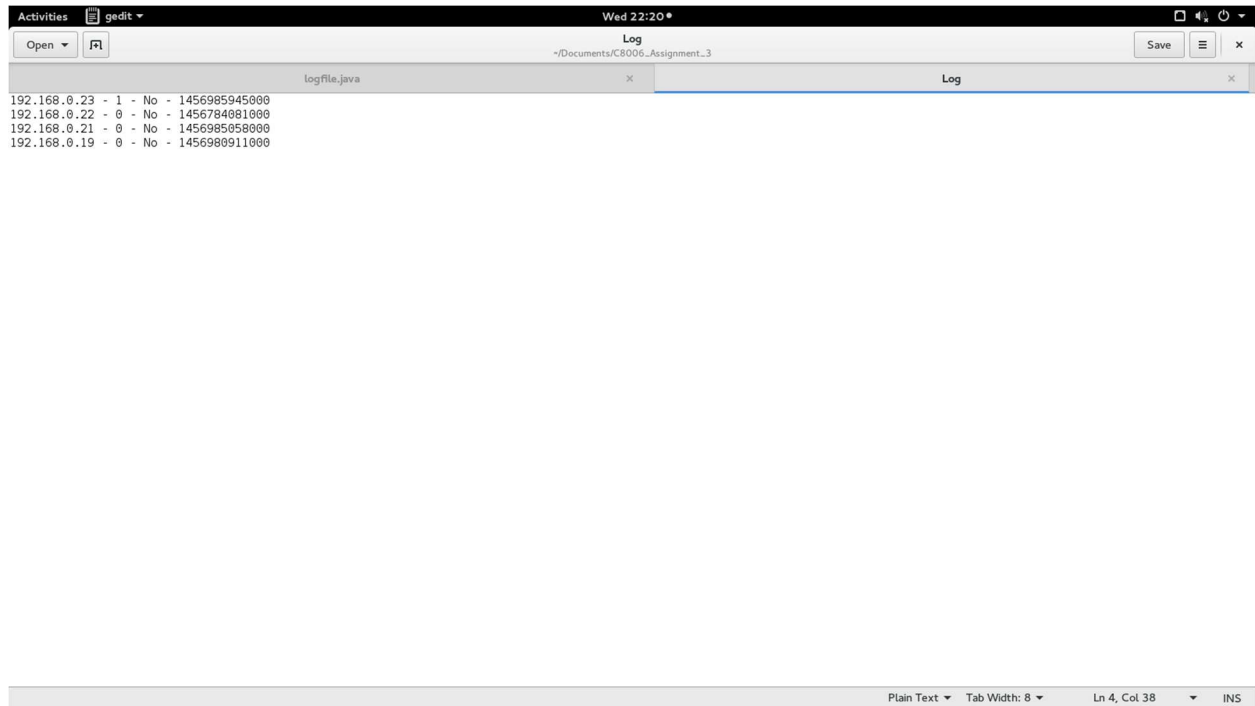
Test 4

Figure 9 Log file after unsuccessful attempt

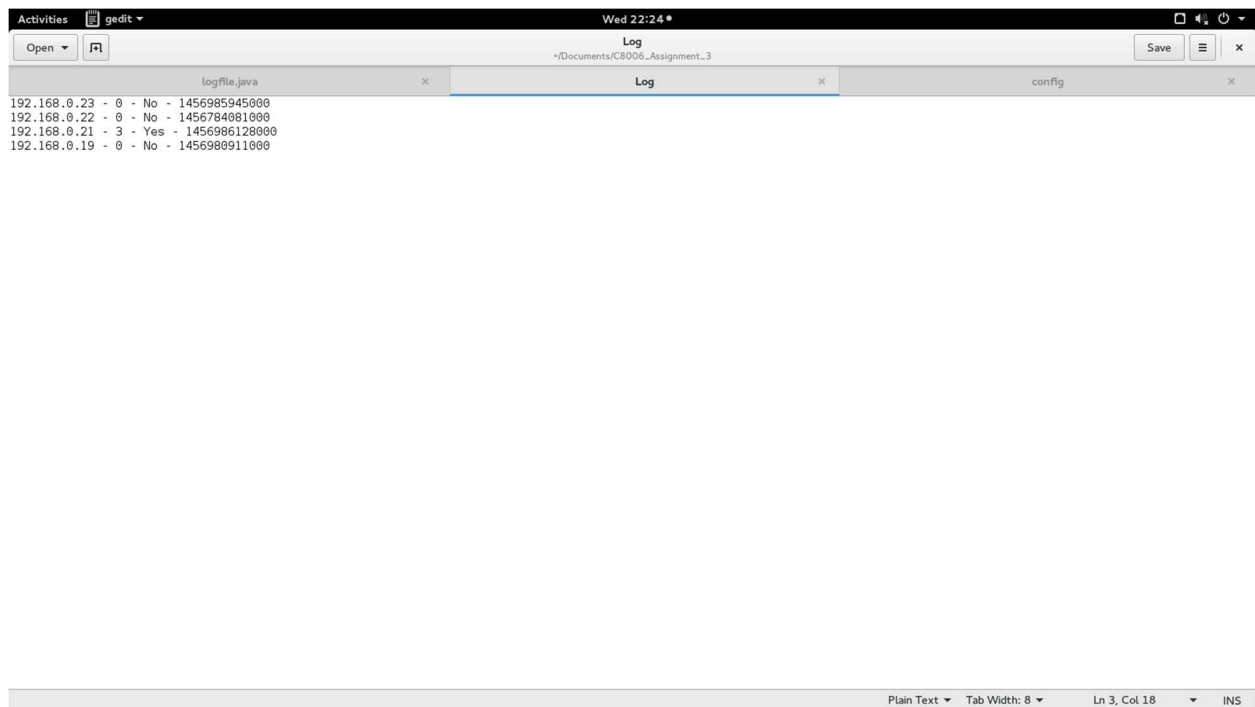
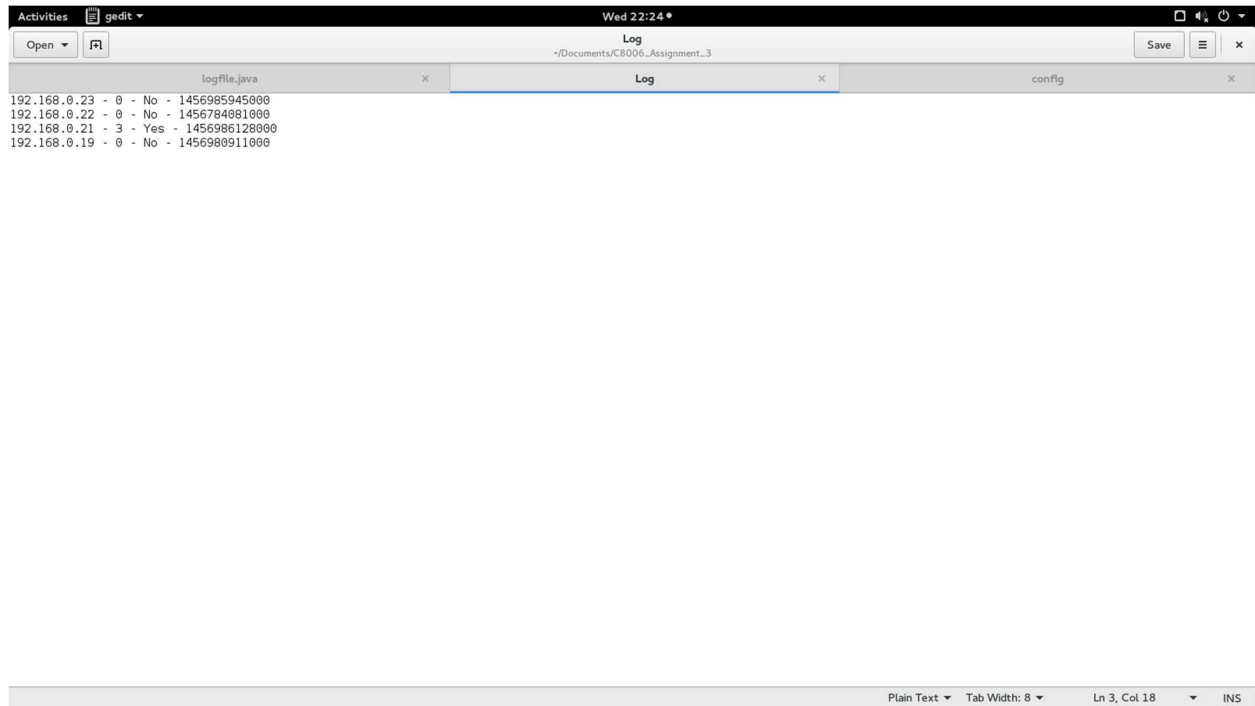


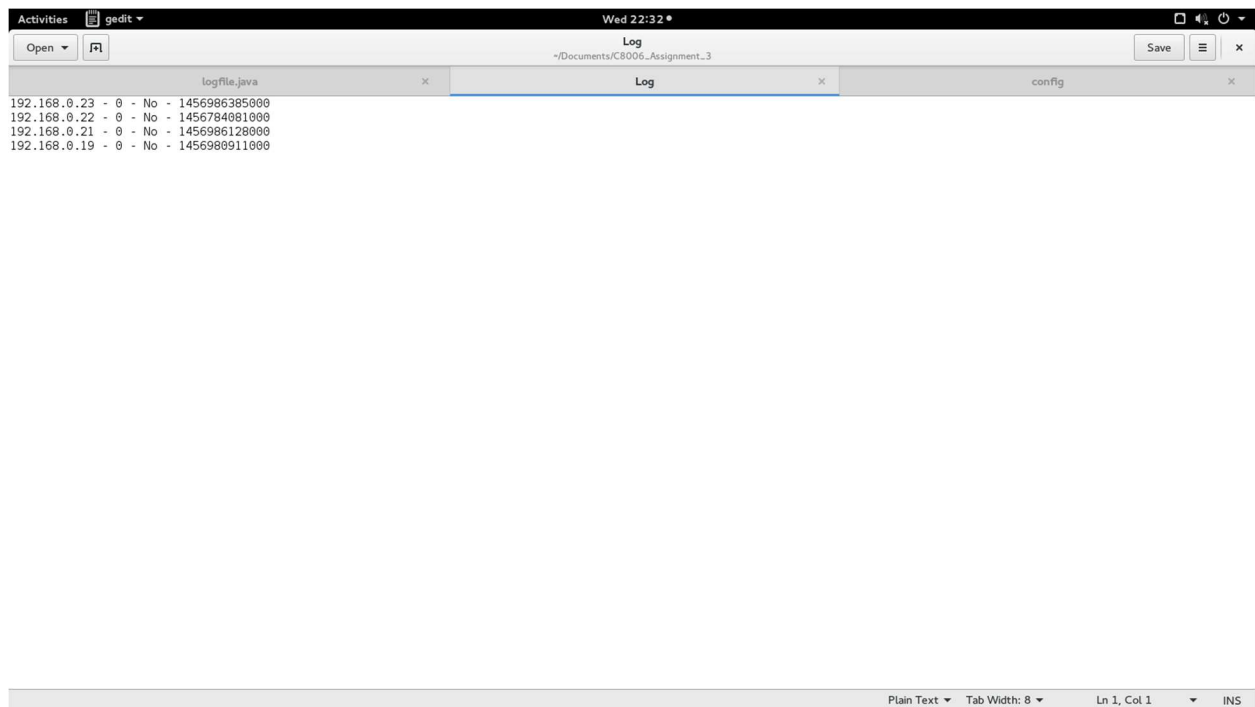
Figure 10 Log file after 4 minutes, removes unsuccessful attempts

Test 5

The screenshot shows a gedit editor window titled "Wed 22:24". The window has three tabs: "logfile.java", "Log", and "config". The "Log" tab is active and displays the following text:

```
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
```

The status bar at the bottom indicates "Plain Text", "Tab Width: 8", "Ln 3, Col 18", and "INS".

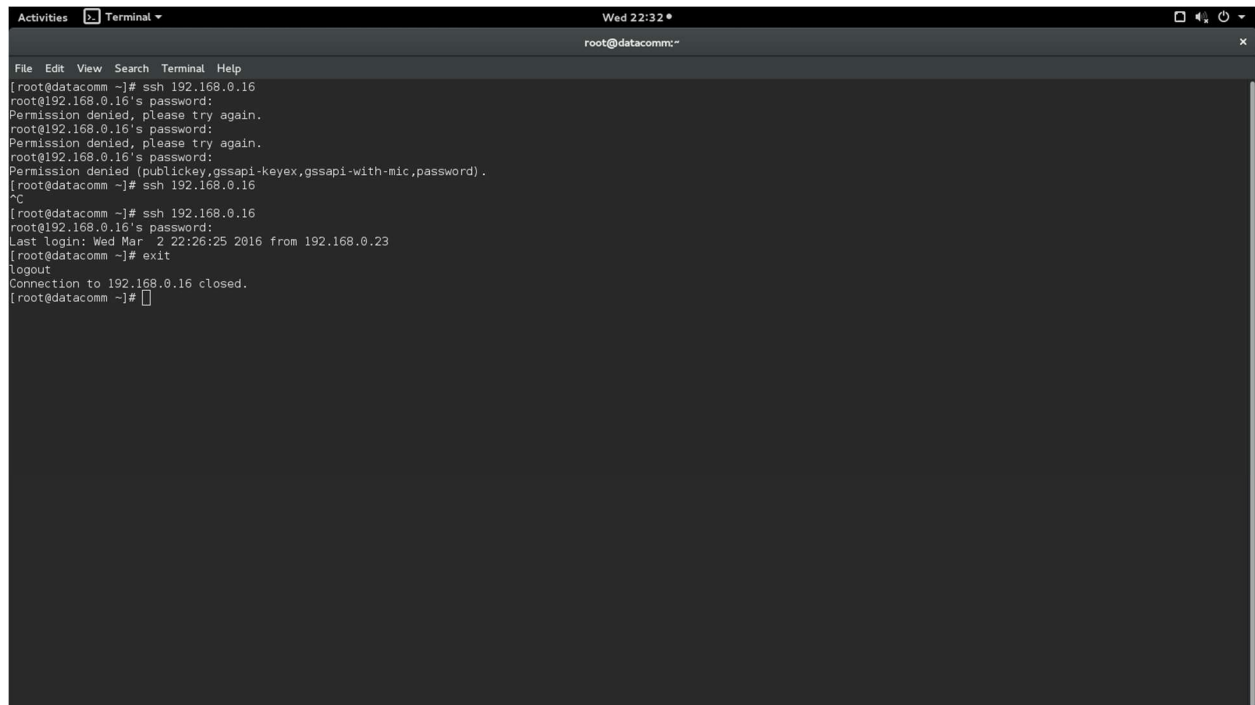
Figure 11 Log file after banning an Ip

The screenshot shows a gedit editor window titled "Wed 22:32". The window has three tabs: "logfile.java", "Log", and "config". The "Log" tab is active and displays the following text:

```
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
```

The status bar at the bottom indicates "Plain Text", "Tab Width: 8", "Ln 1, Col 1", and "INS".

Figure 12 Log file after 8 minutes



A terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Help) and a status bar (Wed 22:32, root@datacomm:~). The terminal shows a series of SSH login attempts from root@datacomm to 192.168.0.16. The first three attempts fail with "Permission denied" messages. The fourth attempt is successful, showing "Last login: Wed Mar 2 22:26:25 2016 from 192.168.0.23". The user then enters "exit" and the connection is closed.

```
File Edit View Search Terminal Help
[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

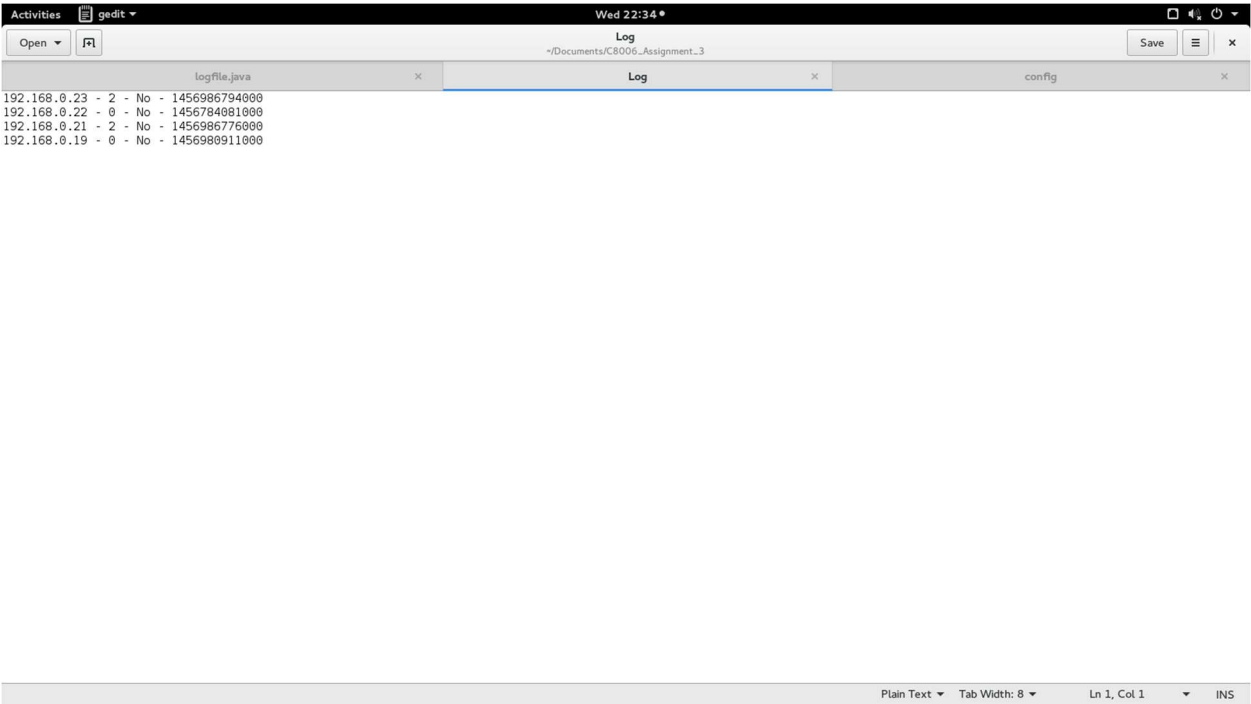


Figure 14 Log updates successfully only with the latest dates

[Test 7](#)