Tests

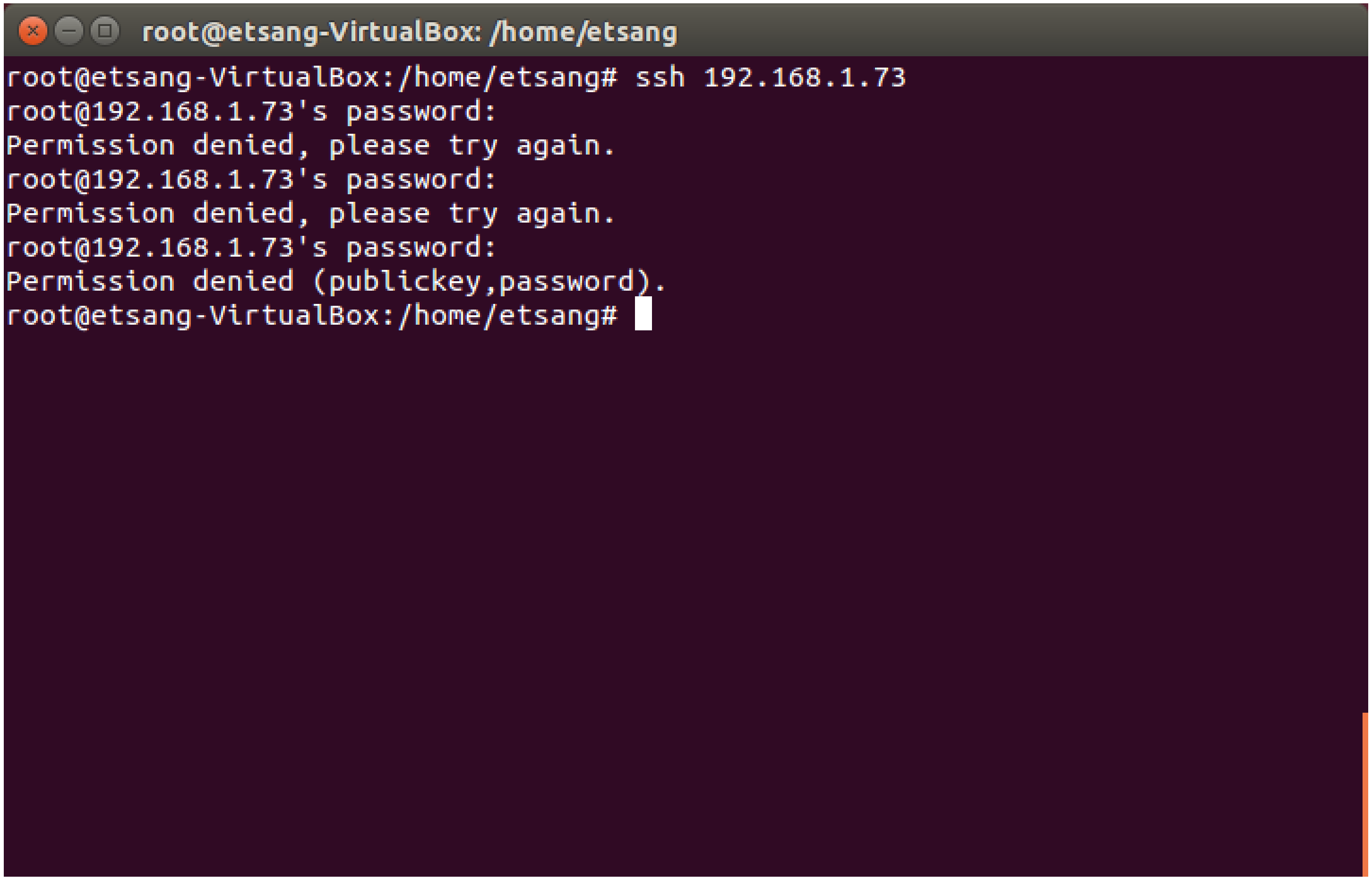
Test #	Test procedure / description	Expected Outcome	Actual Outcome & Remarks	Pass / Fail
1	1. on a client machine, SSH into the server machine 2. input an invalid password 3 or more times 3. check the security logs	• entries in the security log should show that there were password failed attempts	As expected	Pass
2	1. enter "crontab -r" into a terminal 2. use the setjob.ch script to add the ips script as a cronjob 3. check the crontab file	• the crontab file should have an entry in it for regularly running the IPS script	As expected	
3	1. enter "crontab -r" into a terminal 2. use the setjob.ch script to add the ips script as a cronjob 3. try to log in 3 or more times from a client with invalid passwords 4. await the ips' execution 5. check the database, and iptables	• In iptables, it should have an entry to drop all packets from the client's IP address. • The database should have an entry with the client's IP address, number of failed attempts, and timestamp of the last attempt.	As expected	Pass
4	1. enter "crontab -r" into a terminal 2. use the setjob.ch script to add the ips script as a cronjob 3. try to log in 3 or more times from a client with invalid passwords 4. await the ips' execution 5. attempt to connect via SSh to the server again	• the SSH client should hang as it is trying to connect to the remote host	As expected	Pass
5	1. enter "crontab -r" into a terminal 2. use the setjob.ch script to add the ips script as a cronjob 3. try to log in 3 or more times from a client with invalid passwords 4. await the ips' execution 5. wait for the user-specified time to elapse for unbanning an ip address 6. check the database, and iptables	• the database file should no longer have an entry with the client's IP address • in iptables, there should be the original rule dropping all packets from the client's IP address, but it should be preempted by a new rule that accepts all packets from that IP address.	As expected	Pass
6	1. enter "crontab -r" into a terminal 2. use the setjob.ch script to add the ips script as a cronjob 3. try to log in 3 or more times from a client with invalid passwords 4. await the ips' execution	• the SSH client should successfully connect, and prompt the user for a password	As expected	Pass

Test #	Test procedure / description	Expected Outcome	Actual Outcome & Remarks	Pass / Fail
	5. wait for the user-specified time to elapse for unbanning an ip address 6. attempt to connect via SSh to the server again			

Note

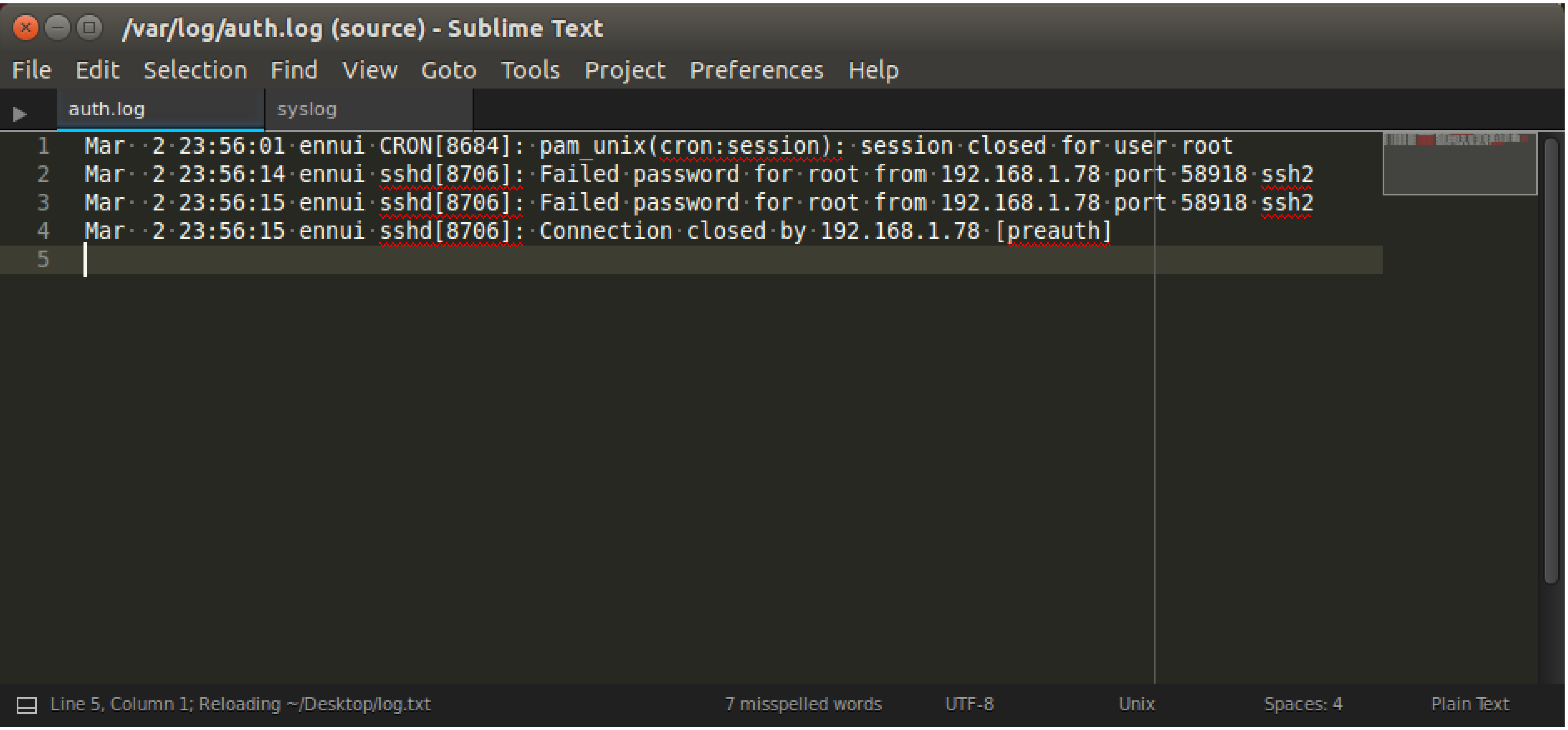
the tests here show only the IPS working when monitoring the ubuntu auth.log, however it has proven to work on Fedora 22's /var/log/messages as well as its /var/log/secure.

Screenshots



```
root@etsang-VirtualBox:/home/etsang# ssh 192.168.1.73
root@192.168.1.73's password:
Permission denied, please try again.
root@192.168.1.73's password:
Permission denied, please try again.
root@192.168.1.73's password:
Permission denied (publickey,password).
root@etsang-VirtualBox:/home/etsang#
```

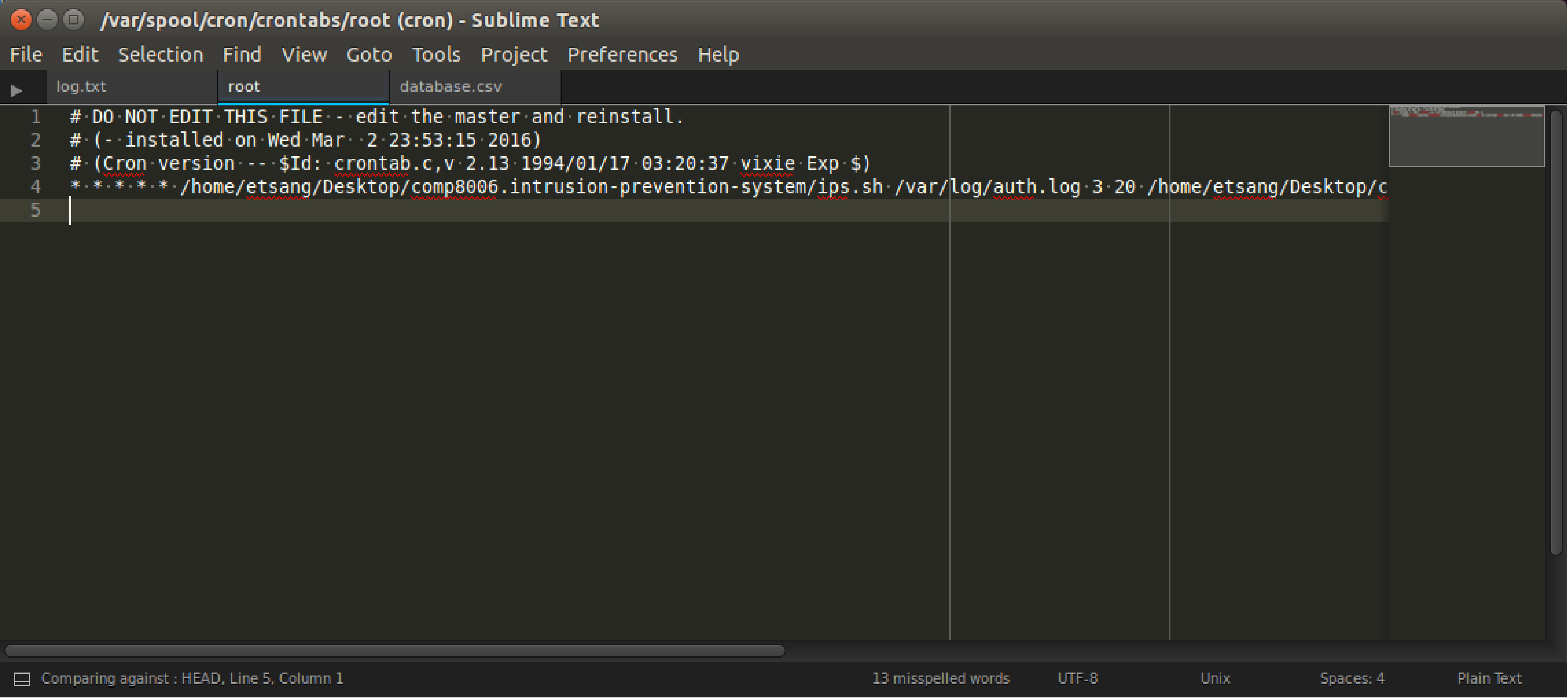
Figure 1 Test 1, client is SSHing into the server with invalid passwords 3 times



```
Mar  2 23:56:01 ennui CRON[8684]: pam_unix(cron:session): session closed for user root
Mar  2 23:56:14 ennui sshd[8706]: Failed password for root from 192.168.1.78 port 58918 ssh2
Mar  2 23:56:15 ennui sshd[8706]: Failed password for root from 192.168.1.78 port 58918 ssh2
Mar  2 23:56:15 ennui sshd[8706]: Connection closed by 192.168.1.78 [preauth]
```

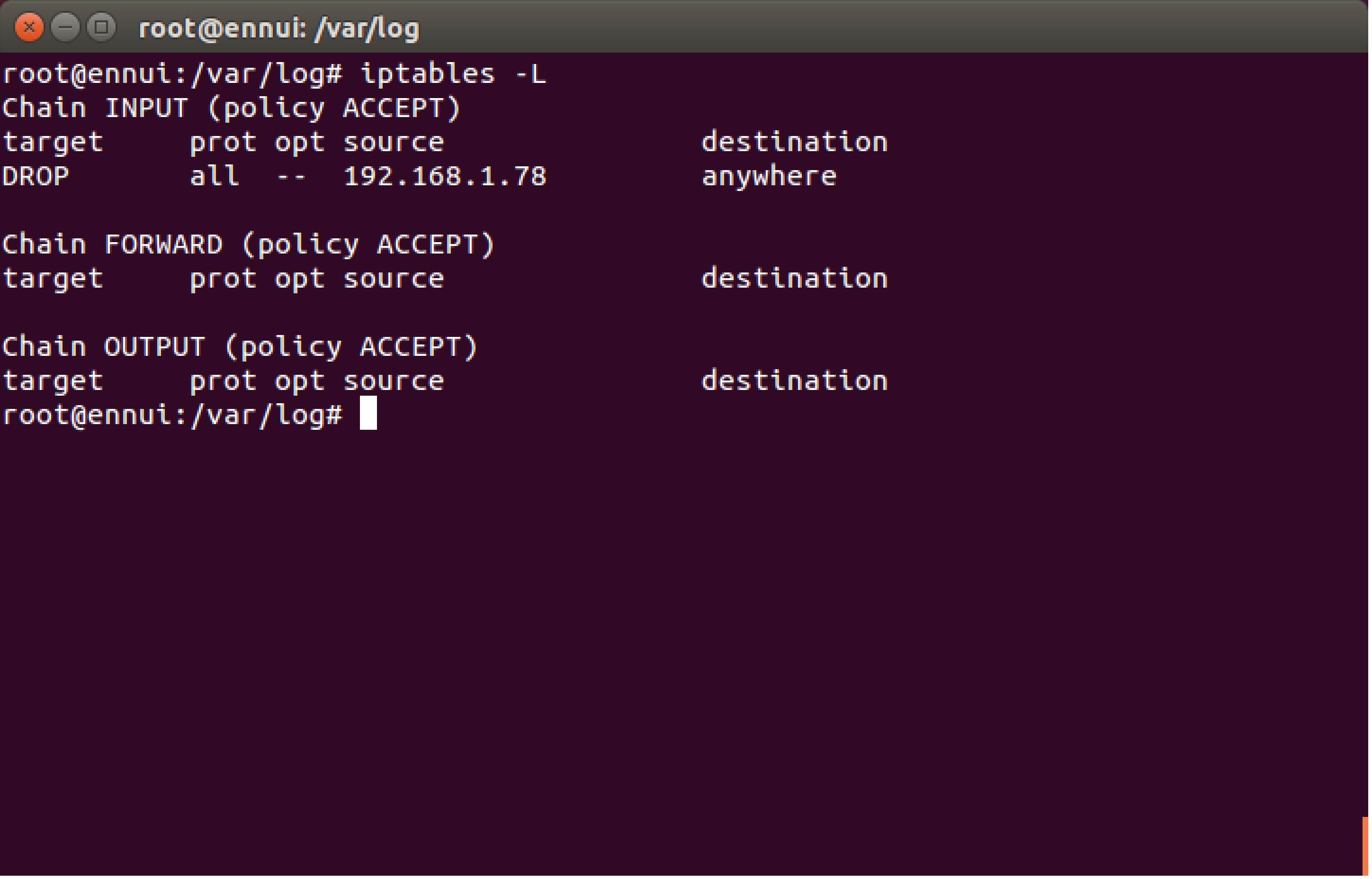
Line 5, Column 1; Reloading ~/Desktop/log.txt

Figure 2 Test 1, security logs show that there are failed password attempts



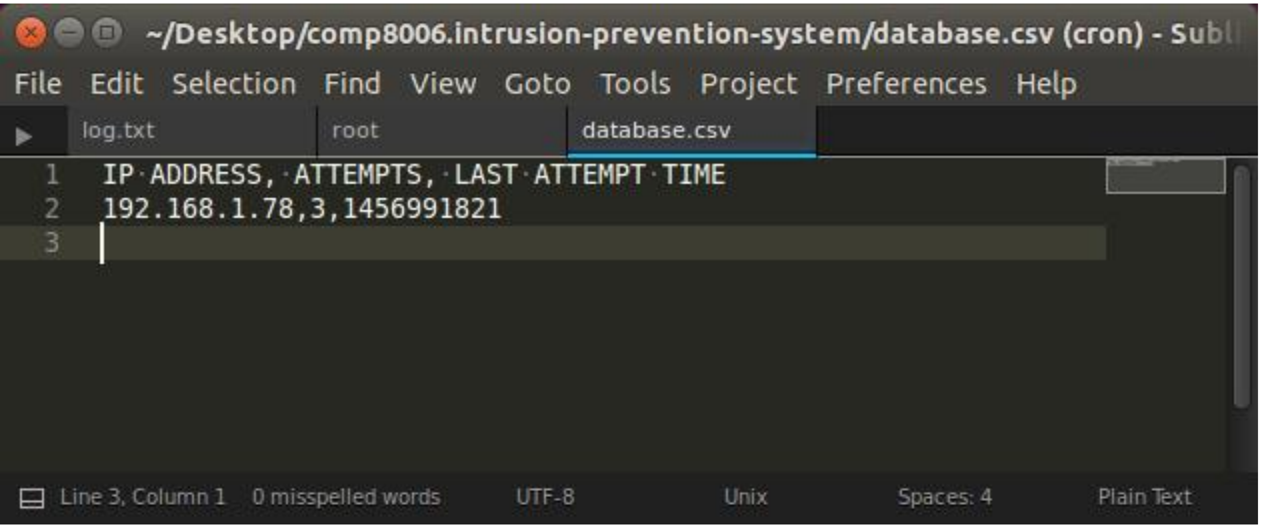
```
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (- installed on Wed Mar  2 23:53:15 2016)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
* * * * * /home/etsang/Desktop/comp8006.intrusion-prevention-system/ips.sh /var/log/auth.log 3 20 /home/etsang/Desktop/c

```

Figure 3 Test 2, the crontab file for root has an entry in it for regularly running the IPS script



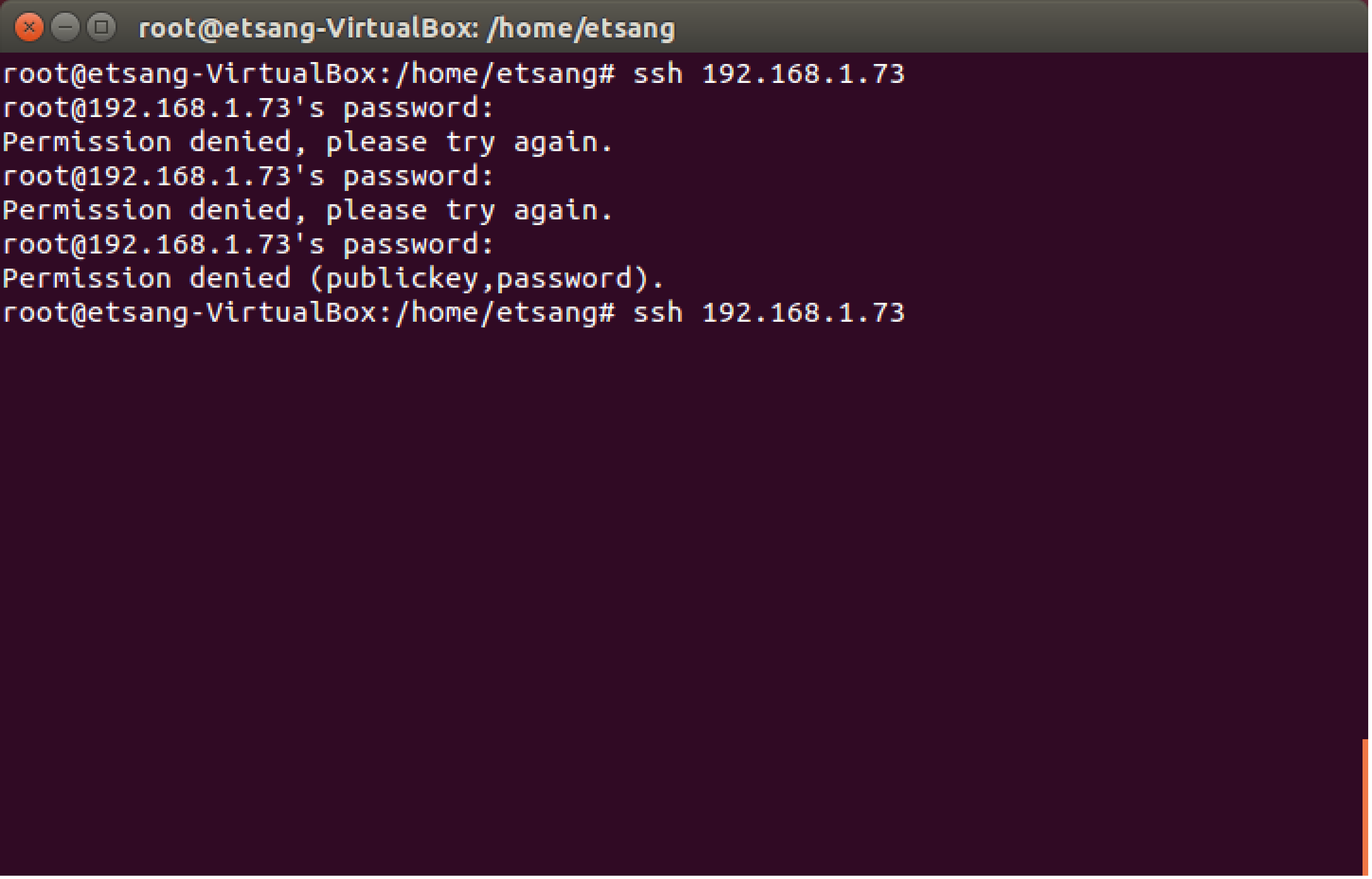
```
root@ennui:/var/log# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.1.78         anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ennui:/var/log# 
```

Figure 4 Test 3, iptables shows that a new rule was appended to it, banning all traffic from the client IP address



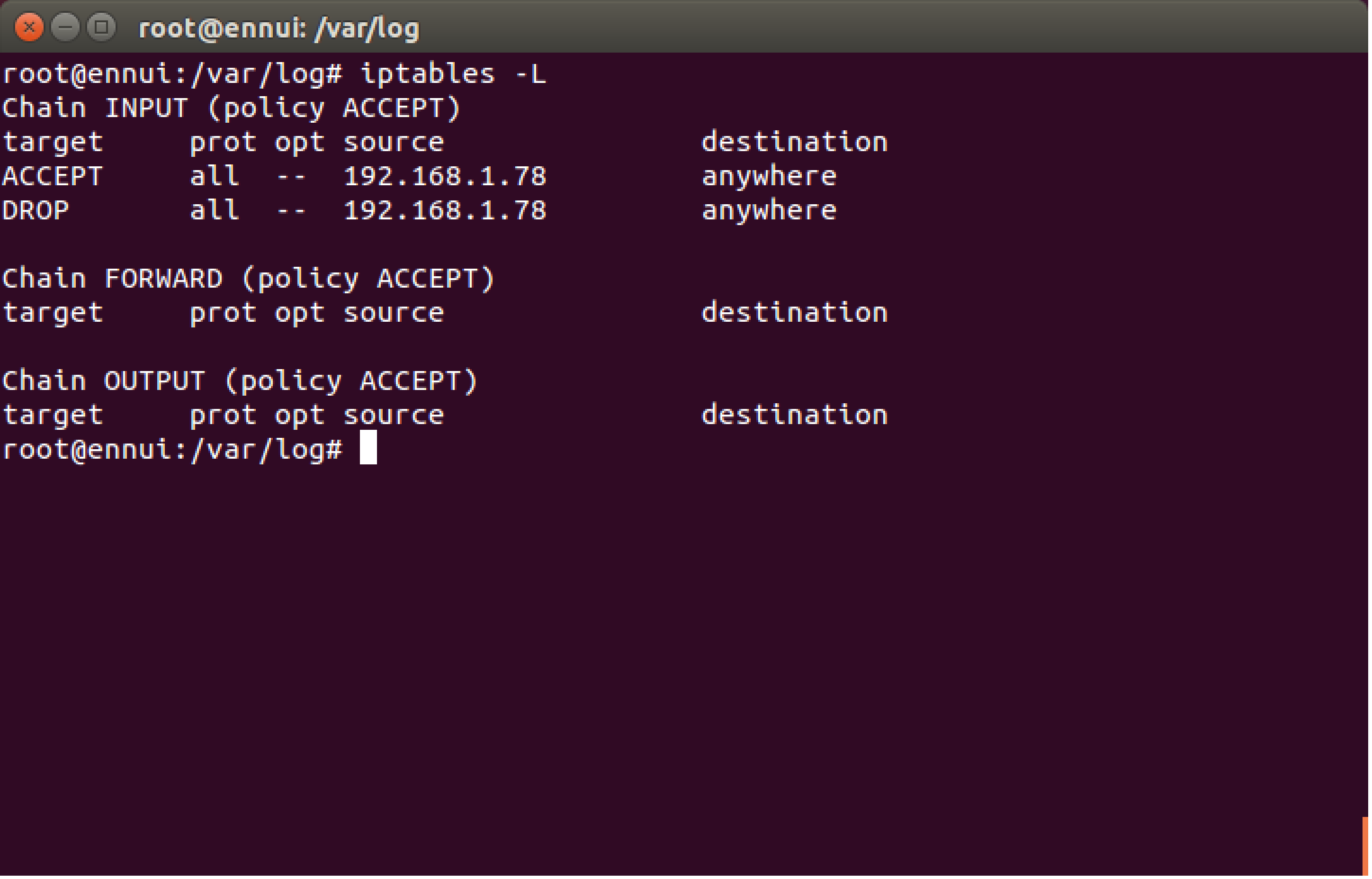
```
IP ADDRESS, ATTEMPTS, LAST ATTEMPT TIME
192.168.1.78,3,1456991821

```

Figure 5 Test 3, the database file shows the IP address of the client that failed to log in, how many password attempts there were, and a timestamp of their last attempt



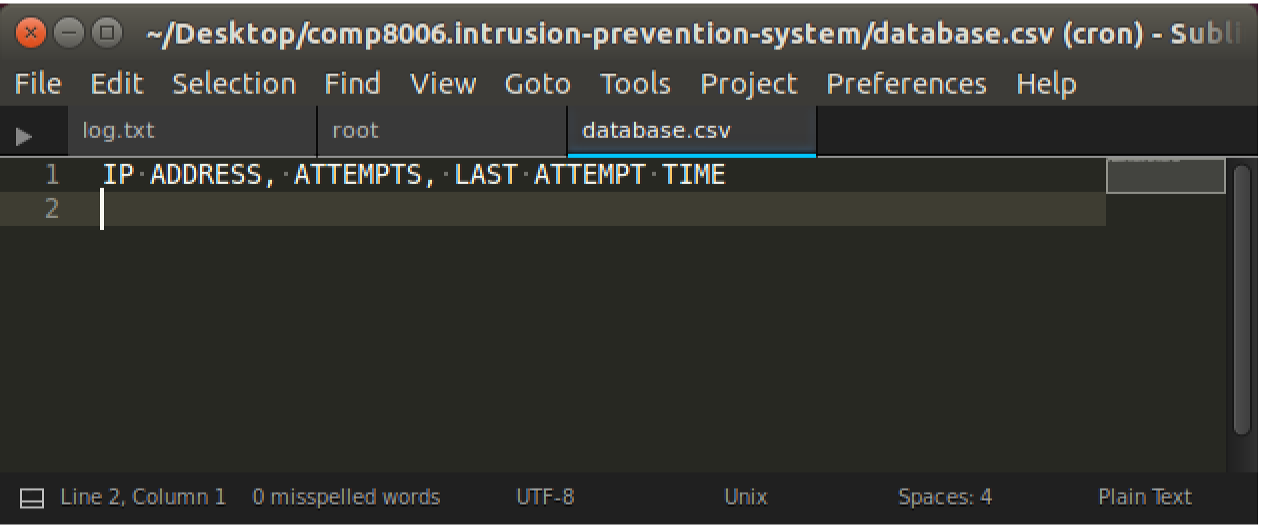
```
root@etsang-VirtualBox:/home/etsang# ssh 192.168.1.73
root@192.168.1.73's password:
Permission denied, please try again.
root@192.168.1.73's password:
Permission denied, please try again.
root@192.168.1.73's password:
Permission denied (publickey,password).
root@etsang-VirtualBox:/home/etsang# ssh 192.168.1.73
```

Figure 6 Test 4, SSH client hanging while trying to connect to the server, because the server has banned its IP address



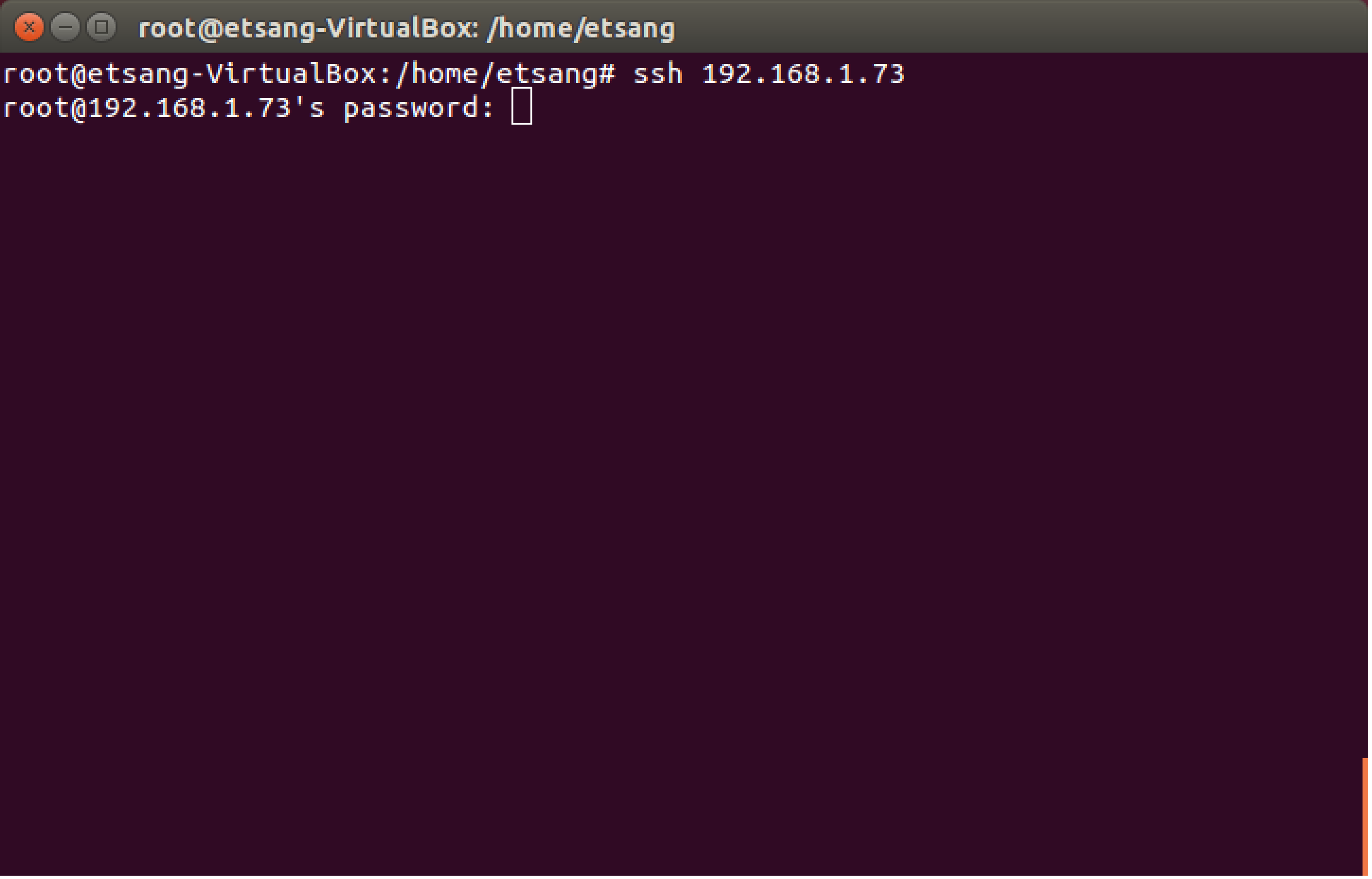
```
root@ennui:/var/log# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  192.168.1.78         anywhere
DROP       all  --  192.168.1.78         anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@ennui:/var/log# 
```

Figure 7 Test 5, the iptables drop all packets from malicious client rule has been preempted with a rule that accepts all traffic from the client



```
IP ADDRESS, ATTEMPTS, LAST ATTEMPT TIME

```

Figure 8 Test 5, there is no more entry for banning the previously banned client because the ban time has elapsed



```
root@etsang-VirtualBox:/home/etsang# ssh 192.168.1.73
root@192.168.1.73's password: 
```

Figure 9 Test 6, the SSH client can now connect to the server after being unbanned