

## Tests

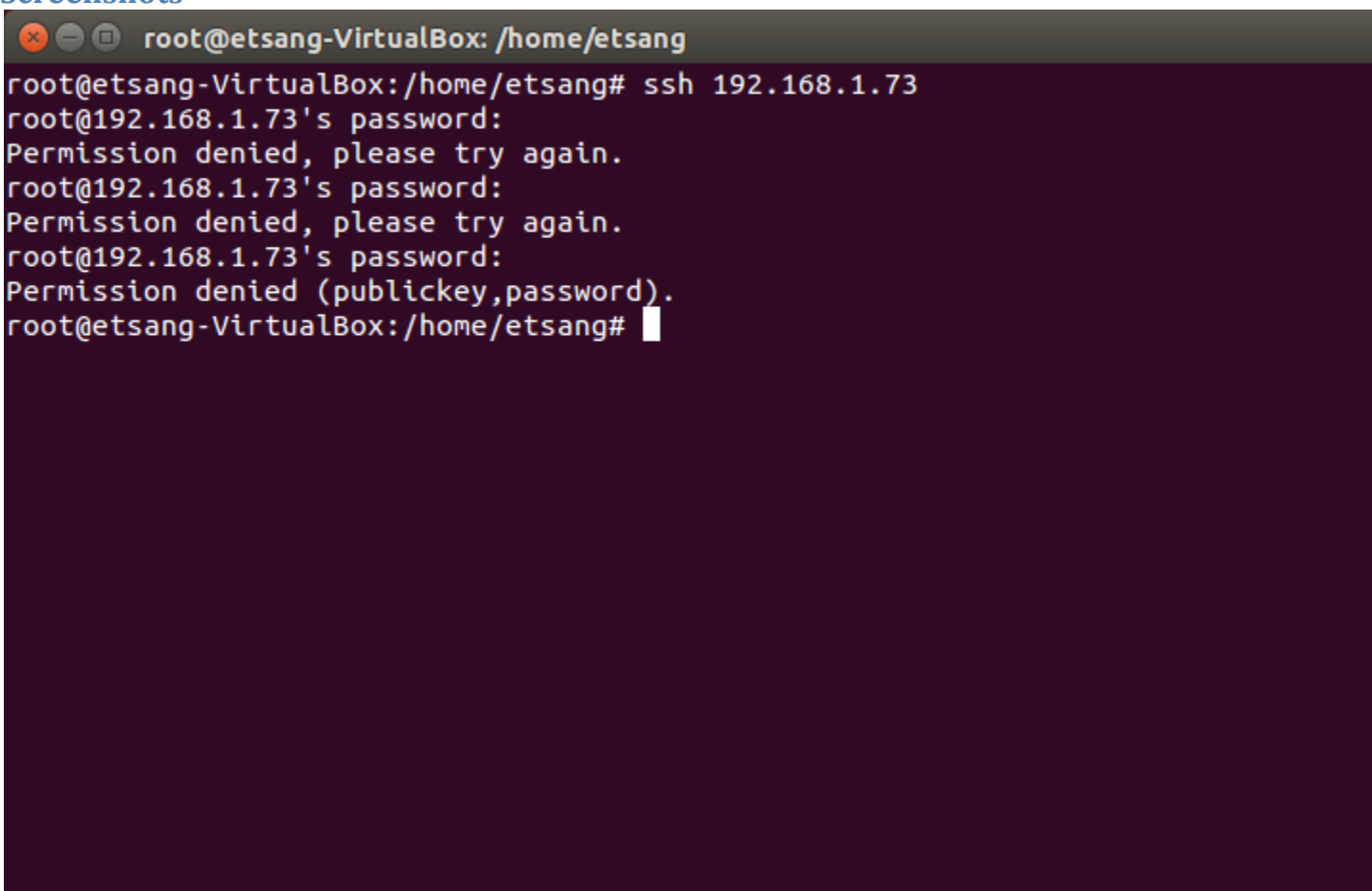
Test #	Test procedure / description	Expected Outcome	Actual Outcome & Remarks	Pass / Fail
1	<ol style="list-style-type: none"><li>on a client machine, SSH into the server machine</li><li>input an invalid password 3 or more times</li><li>check the security logs</li></ol>	<ul style="list-style-type: none"><li>entries in the security log should show that there were password failed attempts</li></ul>	As expected	Pass
2	<ol style="list-style-type: none"><li>enter "crontab -r" into a terminal</li><li>use the setjob.ch script to add the ips script as a cronjob</li><li>check the crontab file</li></ol>	<ul style="list-style-type: none"><li>the crontab file should have an entry in it for regularly running the IPS script</li></ul>	As expected	
3	<ol style="list-style-type: none"><li>enter "crontab -r" into a terminal</li><li>use the setjob.ch script to add the ips script as a cronjob</li><li>try to log in 3 or more times from a client with invalid passwords</li><li>await the ips' execution</li><li>check the database, and iptables</li></ol>	<ul style="list-style-type: none"><li>In iptables, it should have an entry to drop all packets from the client's IP address.</li><li>The database should have an entry with the client's IP address, number of failed attempts, and timestamp of the last attempt.</li></ul>	As expected	Pass
4	<ol style="list-style-type: none"><li>enter "crontab -r" into a terminal</li><li>use the setjob.ch script to add the ips script as a cronjob</li><li>try to log in 3 or more times from a client with invalid passwords</li><li>await the ips' execution</li><li>attempt to connect via SSH to the server again</li></ol>	<ul style="list-style-type: none"><li>the SSH client should hang as it is trying to connect to the remote host</li></ul>	As expected	Pass
5	<ol style="list-style-type: none"><li>enter "crontab -r" into a terminal</li><li>use the setjob.ch script to add the ips script as a cronjob</li><li>try to log in 3 or more times from a client with invalid passwords</li><li>await the ips' execution</li><li>wait for the user-specified time to elapse for unbanning an ip address</li><li>check the database, and iptables</li></ol>	<ul style="list-style-type: none"><li>the database file should no longer have an entry with the client's IP address</li><li>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.</li></ul>	As expected	Pass
6	<ol style="list-style-type: none"><li>enter "crontab -r" into a terminal</li><li>use the setjob.ch script to add the ips script as a cronjob</li><li>try to log in 3 or more times from a client with invalid passwords</li><li>await the ips' execution</li></ol>	<ul style="list-style-type: none"><li>the SSH client should successfully connect, and prompt the user for a password</li></ul>	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

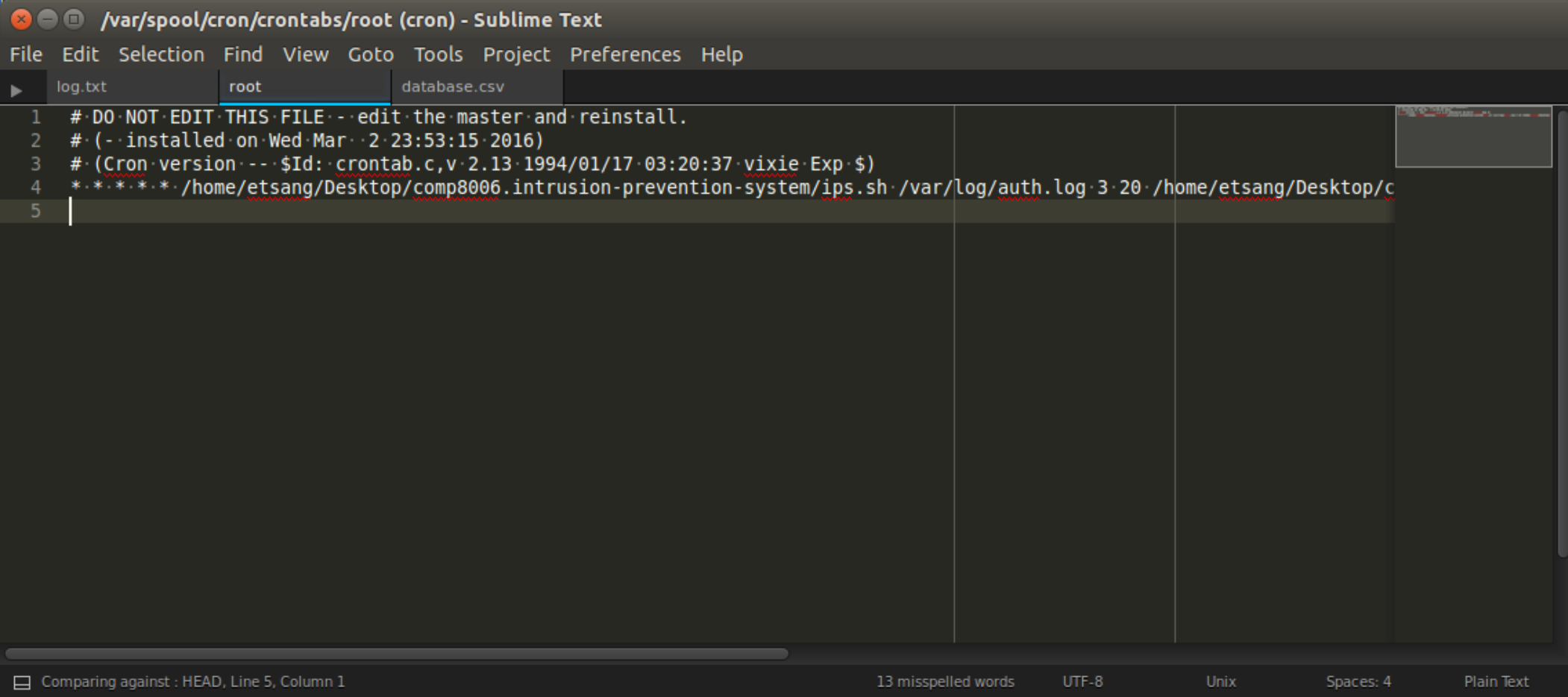
A terminal window titled 'root@etsang-VirtualBox: /home/etsang' with standard window controls. The terminal shows a user at the root@etsang-VirtualBox prompt running 'ssh 192.168.1.73'. This prompts for a password at the root@192.168.1.73's prompt. Three password attempts are shown, each resulting in 'Permission denied, please try again.' The third attempt shows 'Permission denied (publickey,password).' before returning to the root@etsang-VirtualBox prompt, where a cursor is visible.

```
root@etsang-VirtualBox: /home/etsang
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*

```
File Edit Selection Find View Goto Tools Project Preferences Help
auth.log syslog
1 Mar · 2 · 23:56:01 · ennui · CRON[8684] : pam_unix(cron:session) : session closed for user root
2 Mar · 2 · 23:56:14 · ennui · sshd[8706] : Failed password for root from 192.168.1.78 port 58918 ssh2
3 Mar · 2 · 23:56:15 · ennui · sshd[8706] : Failed password for root from 192.168.1.78 port 58918 ssh2
4 Mar · 2 · 23:56:15 · ennui · sshd[8706] : Connection closed by 192.168.1.78 [preauth]
5
Line 5, Column 1; Reloading ~/Desktop/log.txt 7 misspelled words UTF-8 Unix Spaces: 4 Plain Text
```

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



The image shows a Sublime Text editor window titled `/var/spool/cron/crontabs/root (cron) - Sublime Text`. The editor has a menu bar with `File`, `Edit`, `Selection`, `Find`, `View`, `Goto`, `Tools`, `Project`, `Preferences`, and `Help`. Below the menu bar, there are three tabs: `log.txt`, `root` (which is the active tab), and `database.csv`. The `root` tab contains a crontab file with the following content:

```
1 # DO NOT EDIT THIS FILE - edit the master and reinstall.
2 # ( - installed on Wed Mar 2 23:53:15 2016)
3 # (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
4 *. * * * * /home/etsang/Desktop/comp8006.intrusion-prevention-system/ips.sh /var/log/auth.log 3 20 /home/etsang/Desktop/c
5
```

The status bar at the bottom of the editor displays the following information: `Comparing against : HEAD, Line 5, Column 1`, `13 misspelled words`, `UTF-8`, `Unix`, `Spaces: 4`, and `Plain Text`.

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

```
root@ennui: /var/log
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

```
~/Desktop/comp8006.intrusion-prevention-system/database.csv (cron) - Subl
File Edit Selection Find View Goto Tools Project Preferences Help
log.txt root database.csv
1 IP ADDRESS, ATTEMPTS, LAST ATTEMPT TIME
2 192.168.1.78,3,1456991821
3
Line 3, Column 1 0 misspelled words UTF-8 Unix Spaces: 4 Plain Text
```

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
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
```

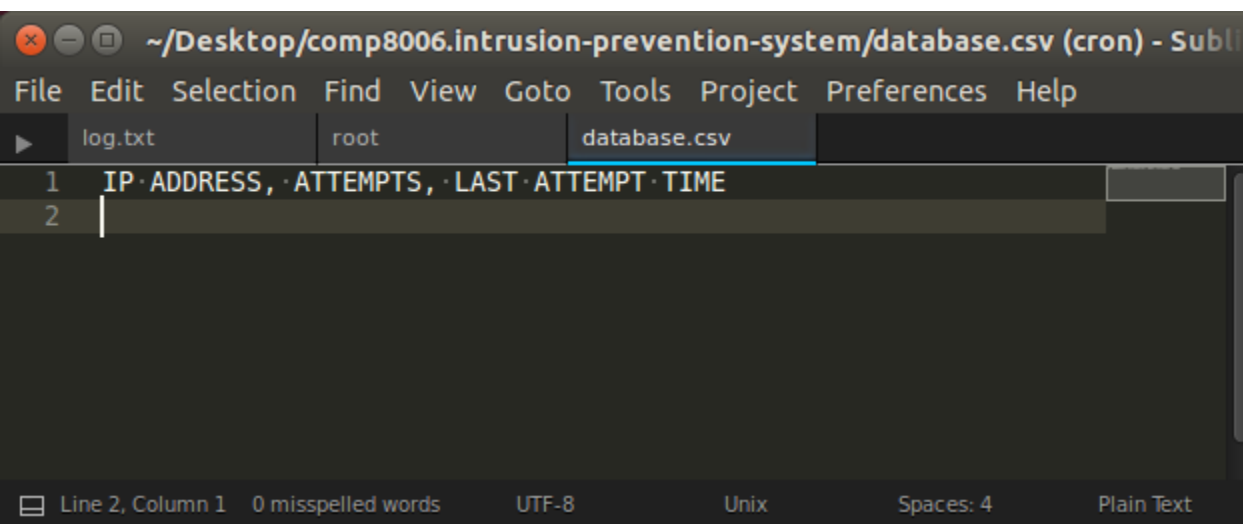
*Figure 6 Test 4, SSH client hanging while trying to connect to the server, because the server has banned its IP address*

```
root@ennui: /var/log
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#
```

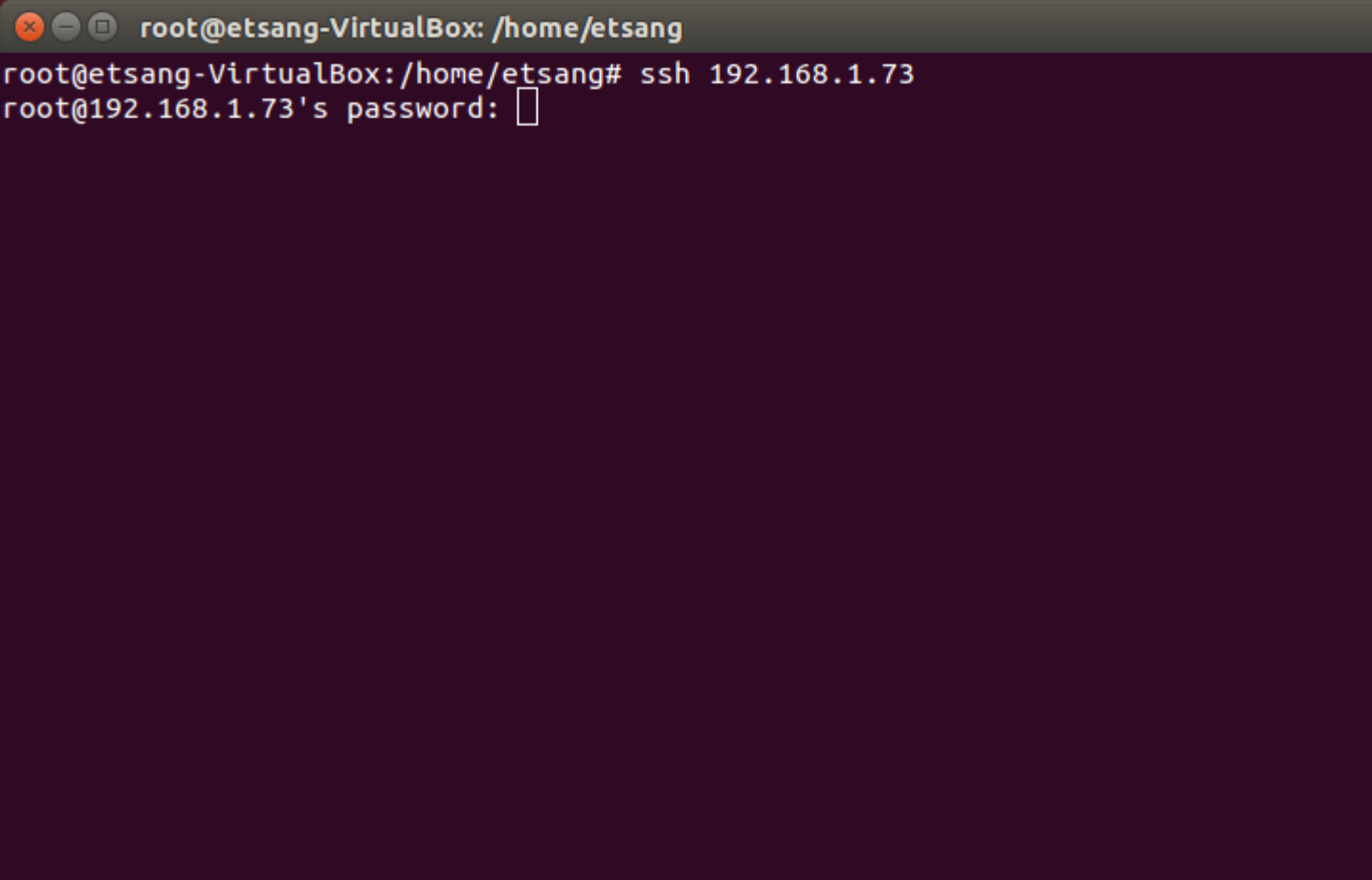
Figure 7 Test 5, the iptables drop all packets from malicious client rule has been preempted with a rule that accepts all traffic from the client



```
~/Desktop/comp8006.intrusion-prevention-system/database.csv (cron) - Subl
File Edit Selection Find View Goto Tools Project Preferences Help
log.txt root database.csv
1 IP ADDRESS, ATTEMPTS, LAST ATTEMPT TIME
2
```

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



A terminal window with a dark purple background and a grey title bar. The title bar contains three window control icons (close, maximize, and a square icon) followed by the text 'root@etsang-VirtualBox: /home/etsang'. The terminal shows a command 'ssh 192.168.1.73' being executed, followed by a password prompt 'root@192.168.1.73's password:' and a single character input.

```
root@etsang-VirtualBox: /home/etsang
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*