

Linux Host Review

Walkthrough by Basil
Wattlecorp Cybersecurity Labs

System Review

We had got access of ssh from the description.
ssh user@192.168.56.182
pass - live

```
[baz@parrot]~$ ssh user@192.168.56.182
The authenticity of host '192.168.56.182 (192.168.56.182)' can't be established.
RSA key fingerprint is SHA256:bgMp3ocQB6FEI/92roY5XZfCkXmnvDc/qYKaV/LHDRs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.182' (RSA) to the list of known hosts.
user@192.168.56.182's password:
Linux debian 2.6.32-5-686 #1 SMP Sun Sep 23 09:49:36 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

It is always a good practice to check if the system has all permission set. If it has it's really easy to get to root.
sudo -s

```
user@debian:~$ sudo -s
root@debian:/home/user#
```

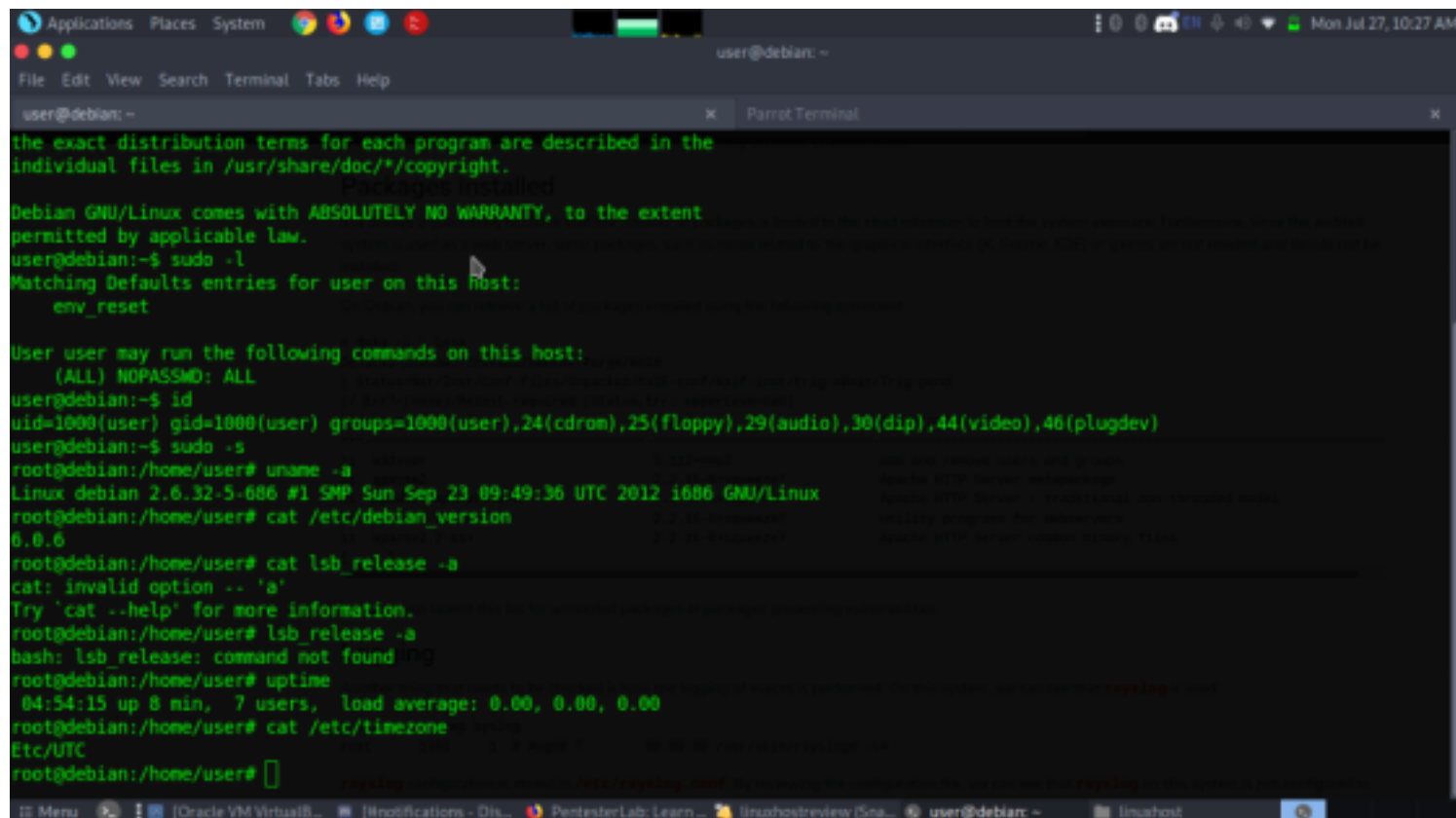
To know the system information the version use /etc/debian_version in debian

```
root@debian:/home/user# cat /etc/debian_version
6.0.6
root@debian:/home/user#
```

To know the kernel version
uname -a

```
user@debian:~$ cat /etc/debian_version
6.0.6
user@debian:~$ uname -a
Linux debian 2.6.32-5-686 #1 SMP Sun Sep 23 09:49:36 UTC 2012 i686 GNU/Linux
```

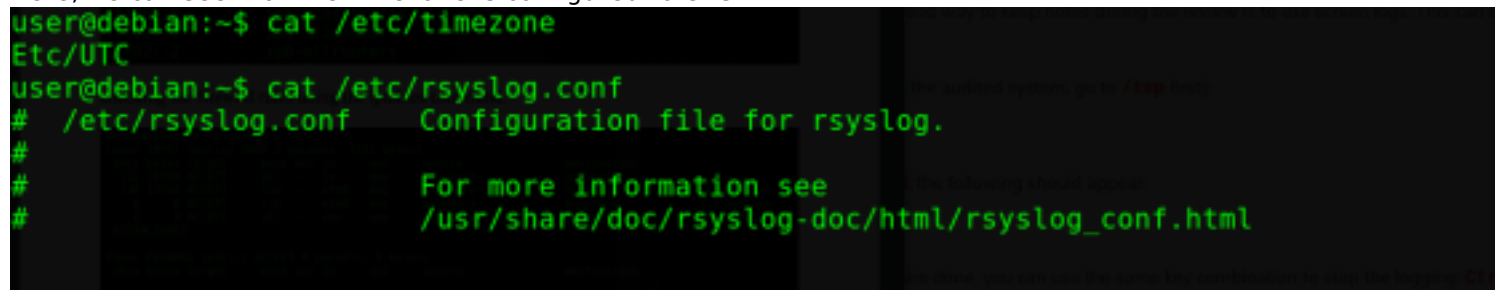
To check when the last kernel upgrade was performed
uptime



```
user@debian: ~  
File Edit View Search Terminal Tabs Help  
user@debian: ~  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
user@debian:~$ sudo -l  
Matching Defaults entries for user on this host:  
env_reset  
  
User user may run the following commands on this host:  
(ALL) NOPASSWD: ALL  
user@debian:~$ id  
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)  
user@debian:~$ sudo -s  
root@debian:/home/user# uname -a  
Linux debian 2.6.32-5-686 #1 SMP Sun Sep 23 09:49:36 UTC 2012 1686 GNU/Linux  
root@debian:/home/user# cat /etc/debian_version  
6.0.6  
root@debian:/home/user# cat lsb_release -a  
cat: invalid option -- 'a'  
Try 'cat --help' for more information.  
root@debian:/home/user# lsb_release -a  
bash: lsb_release: command not found  
root@debian:/home/user# uptime  
04:54:15 up 8 min, 7 users, load average: 0.00, 0.00, 0.00  
root@debian:/home/user# cat /etc/timezone  
Etc/UTC  
root@debian:/home/user#
```

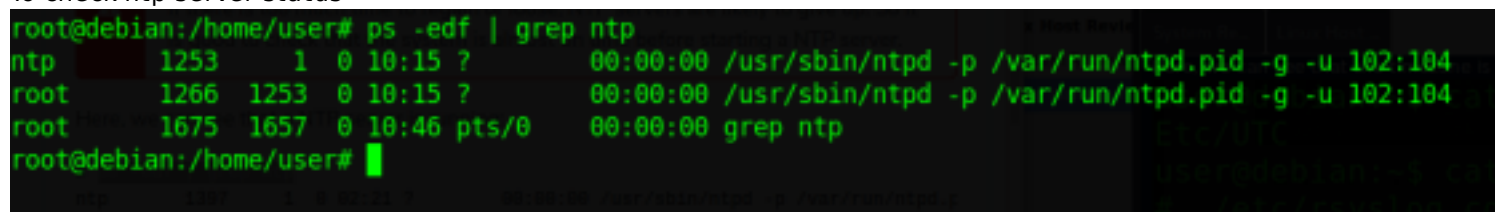
Time Management

Here, we can see that the timezone is configured to UTC:



```
user@debian:~$ cat /etc/timezone  
Etc/UTC  
user@debian:~$ cat /etc/rsyslog.conf  
# /etc/rsyslog.conf Configuration file for rsyslog.  
#  
#  
# For more information see  
# /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
```

To check ntp server status



```
root@debian:/home/user# ps -edf | grep ntp  
ntp      1253      1  0 10:15 ?        00:00:00 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 102:104  
root     1266    1253  0 10:15 ?        00:00:00 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 102:104  
root     1675    1657  0 10:46 pts/0    00:00:00 grep ntp  
root@debian:/home/user#
```

Network Review

ifconfig -a to see what network interfaces are present;

```

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:4b:41:1a
          inet addr:192.168.56.182  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4b:411a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41133 errors:0 dropped:0 overruns:0 frame:0
          TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2473096 (2.3 MiB)  TX bytes:6771 (6.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:164 errors:0 dropped:0 overruns:0 frame:0
          TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:13300 (12.9 KiB)  TX bytes:13300 (12.9 KiB)

```

route -n to get the system routes. If the system does not have the route command installed, netstat -rn can be a suitable substitute.

```

user@debian:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.56.0    0.0.0.0        255.255.255.0   U        0      0      0 eth0
user@debian:~$ iptables -L -v
iptables v1.4.8: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
user@debian:~$ ps -edf | grep syslog
root      1154      1  0 10:15 ?        00:00:00 /usr/sbin/rsyslogd -c4
user      1622    1612  0 10:25 pts/0    00:00:00 grep syslog

```

cat /etc/resolv.conf and cat /etc/hosts to know more about the DNS configuration of the system.

```

user@debian:~$ cat /etc/rsyslog.conf
# /etc/rsyslog.conf  Configuration file for rsyslog.
#
# For more information see
# /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
#
#####
#### MODULES ####
#####

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog    # provides kernel logging support (previously done by rklogd)
$ModLoad immark    # provides --MARK-- message capability

# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514

#####
#### GLOBAL DIRECTIVES ####
#####

# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

```

Firewall rules

To retrieve firewall rules by iptables

```

user@debian:~$ sudo iptables -L -v
Chain INPUT (policy DROP 2 packets, 1152 bytes)
  pkts bytes target     prot opt in     out     source            destination
   164 13300 ACCEPT     all  --  lo      any      anywhere          anywhere
    250 20608 ACCEPT     tcp  --  eth0    any      anywhere          anywhere        tcp dpt:ssh
      0      0 ACCEPT     tcp  --  eth0    any      anywhere          anywhere        tcp dpt:www
      2   1152 ACCEPT     all  --  any     any      anywhere          anywhere        state RELATED,ESTABLISHED

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

Chain OUTPUT (policy ACCEPT 306 packets, 30741 bytes)
  pkts bytes target     prot opt in     out     source            destination
user@debian:~$

```

Sensitive Files

It is important to check permission on sensitive files. As a general rule, you want to check:

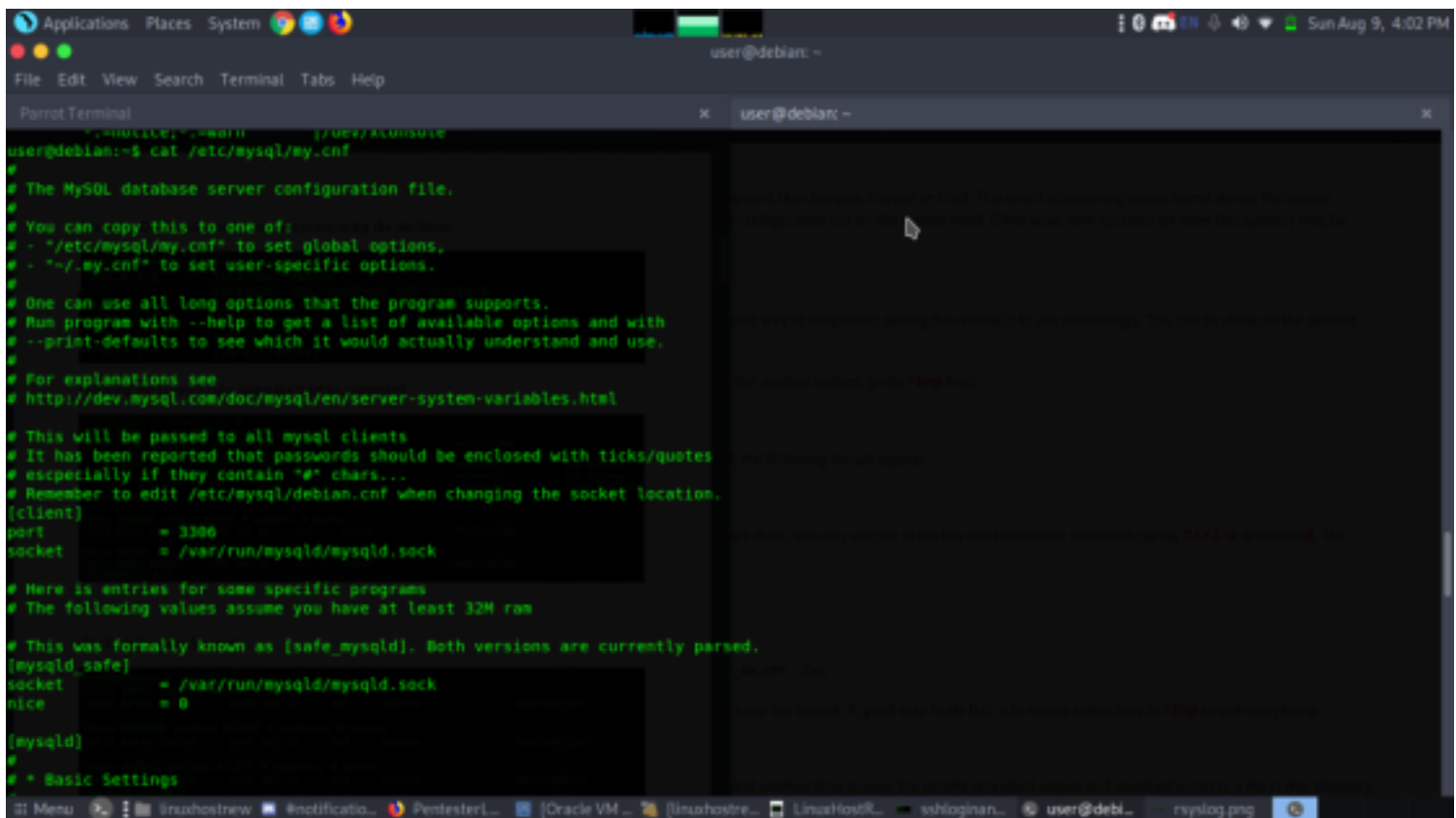
- that files containing sensitive information (password, private keys) can't be read by any user; cat /etc/passwd

```

user@debian:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false
ntp:x:102:104::/home/ntp:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:Debian Live user,,,:/home/user:/bin/bash
user@debian:~$ cat /etc/sudoers

```

- etc/mysql/my.cnf containing debian-sys-maint's password;
- SSL private keys used by Apache



```
user@debian:~$ cat /etc/mysql/my.cnf
# The MySQL database server configuration file.
#
# You can copy this to one of:
# - "/etc/mysql/my.cnf" to set global options,
# - "~/.my.cnf" to set user-specific options.
#
# One can use all long options that the program supports.
# Run program with --help to get a list of available options and with
# --print-defaults to see which it would actually understand and use.
#
# For explanations see
# http://dev.mysql.com/doc/mysql/en/server-system-variables.html
#
# This will be passed to all mysql clients
# It has been reported that passwords should be enclosed with ticks/quotes
# especially if they contain " " chars...
# Remember to edit /etc/mysql/debian.cnf when changing the socket location.
[client]
port                = 3306
socket              = /var/run/mysqld/mysqld.sock

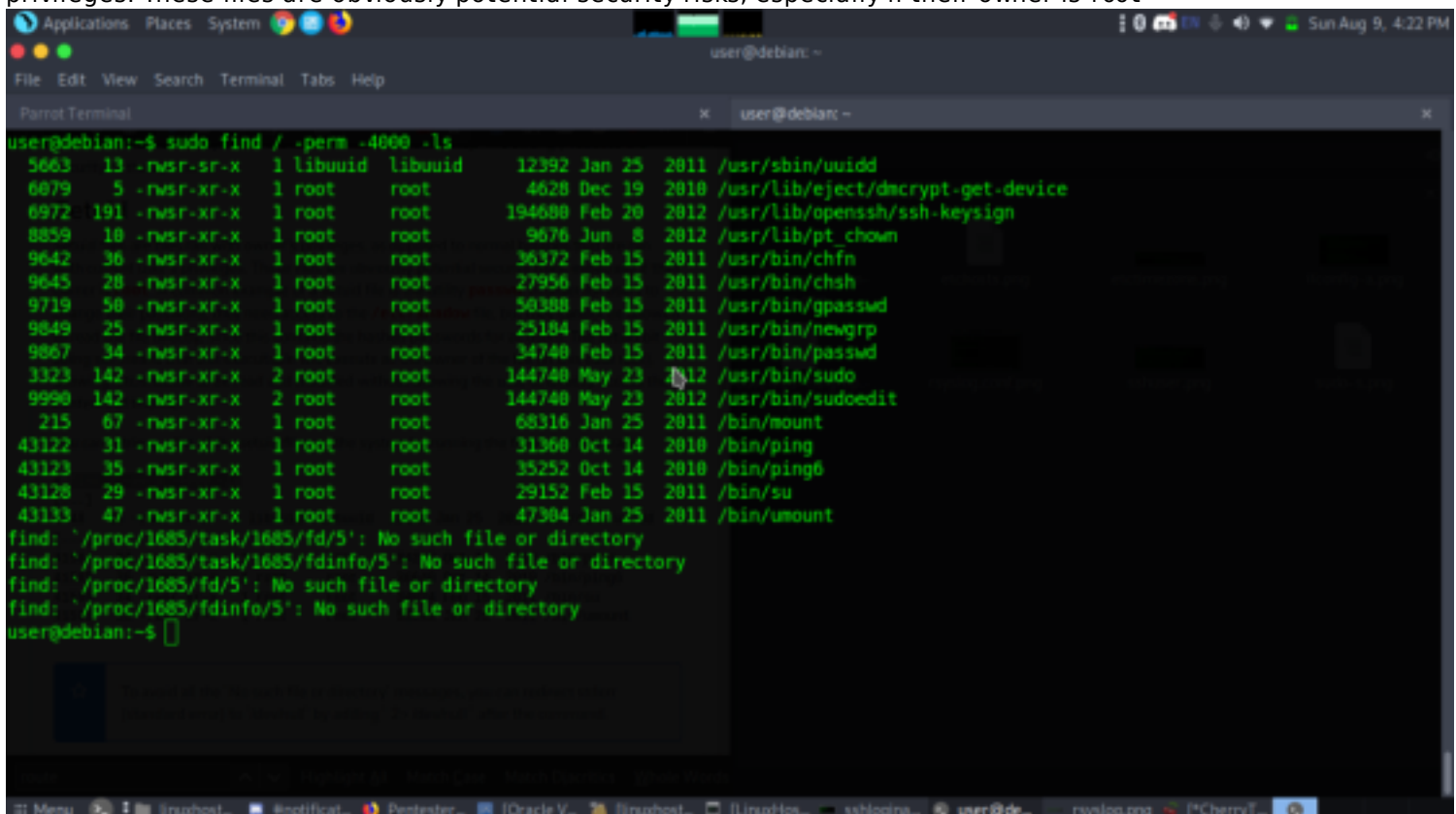
# Here is entries for some specific programs
# The following values assume you have at least 32M ram

# This was formerly known as [safe_mysqld]. Both versions are currently parsed.
[mysqld_safe]
socket              = /var/run/mysqld/mysqld.sock
nice                = 0

[mysqld]
#
# * Basic Settings
#
```

Setuid

Setuid files are files ran with owner's privileges, as opposed to normal binaries that are run with current user's privileges. These files are obviously potential security risks, especially if their owner is root



```
user@debian:~$ sudo find / -perm -4000 -ls
5663  13 -rwsr-sr-x  1 libuuid  libuuid      12392 Jan 25  2011 /usr/sbin/uuidd
6079   5 -rwsr-xr-x  1 root    root        4628 Dec 19  2010 /usr/lib/eject/dmccrypt-get-device
6972 191 -rwsr-xr-x  1 root    root       194688 Feb 20  2012 /usr/lib/openssh/ssh-keysign
8859  18 -rwsr-xr-x  1 root    root        9676 Jun  8  2012 /usr/lib/pt_chown
9642  36 -rwsr-xr-x  1 root    root       36372 Feb 15  2011 /usr/bin/chfn
9645  28 -rwsr-xr-x  1 root    root       27956 Feb 15  2011 /usr/bin/chsh
9719  58 -rwsr-xr-x  1 root    root       50388 Feb 15  2011 /usr/bin/gpasswd
9849  25 -rwsr-xr-x  1 root    root       25184 Feb 15  2011 /usr/bin/newgrp
9867  34 -rwsr-xr-x  1 root    root       34748 Feb 15  2011 /usr/bin/passwd
3323 142 -rwsr-xr-x  2 root    root      144740 May 23  2012 /usr/bin/sudo
9990 142 -rwsr-xr-x  2 root    root      144740 May 23  2012 /usr/bin/sudoedit
  215  67 -rwsr-xr-x  1 root    root       68316 Jan 25  2011 /bin/mount
43122 31 -rwsr-xr-x  1 root    root       31360 Oct 14  2010 /bin/ping
43123 35 -rwsr-xr-x  1 root    root       35252 Oct 14  2010 /bin/ping6
43128 29 -rwsr-xr-x  1 root    root       29152 Feb 15  2011 /bin/su
43133 47 -rwsr-xr-x  1 root    root       47304 Jan 25  2011 /bin/umount
find: '/proc/1685/task/1685/fd/5': No such file or directory
find: '/proc/1685/task/1685/fdinfo/5': No such file or directory
find: '/proc/1685/fd/5': No such file or directory
find: '/proc/1685/fdinfo/5': No such file or directory
user@debian:~$
```

Using find, you can retrieve a list of files that are readable and write-able by any users using the following command:

