FORENSICS
LAB SERIES

Lab 6: Linux OS Artifact Forensics

Material in this Lab Aligns to the Following Certification Domains/Objectives
Computer Hacking Forensic Investigator (CHFI) Objectives
7: Understanding Hard Disks and File Systems

Document Version: 2016-08-17

Contents

Introduction 3
Objective 3
Pod Topology 4
Lab Settings 5
1 Analyzing the Linux File System 6
2 Analyzing the Linux User Information 15

Introduction

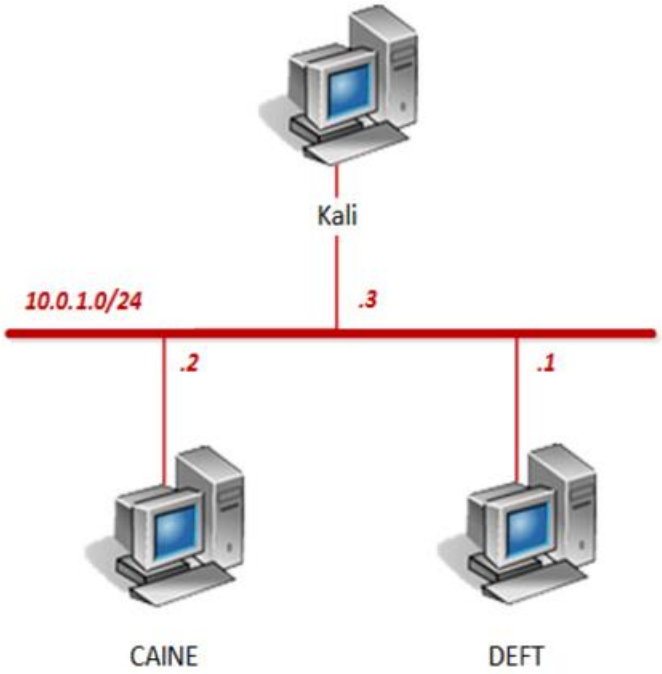
This lab will introduce the concept of performing a forensic examination of a Linux system. The examination process will pinpoint where to find pertinent information in regards to what an investigation may require.

Objective

In this lab, you will be conducting forensic practices using various tools. You will be performing the following tasks:

1. Analyzing the Linux File System
2. Analyzing the Linux User Information

Pod Topology



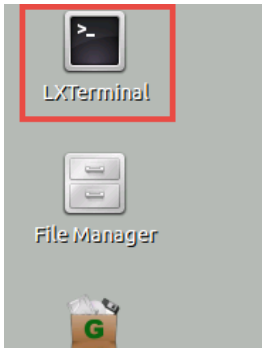
Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
DEFT	10.0.1.1	deft	password
CAINE	10.0.1.2	caine	
Kali	10.0.1.3	root	toor

1 Analyzing the Linux File System

1. Click on the **DEFT** graphic on the *topology page* to open the VM.
2. Open a new terminal by clicking on the **LXTerminal** icon located on the Desktop.



3. Using the terminal, determine the system date and time by typing the command below followed by pressing the **Enter** key.

```
date
```

```
deft-virtual-machine ~ % date
Wed Jul 13 10:12:09 CDT 2016
deft-virtual-machine ~ %
```

The data will vary when compared to the image above.

4. Identify where the time zone setting comes from by entering the command below.

```
cat /etc/timezone
```

```
deft-virtual-machine ~ % cat /etc/timezone
America/Chicago
deft-virtual-machine ~ %
```

5. Enter the *zdump* command below as an alternative way of identifying the local time.

```
Zdump /etc/localtime
```

```
deft-virtual-machine ~ % zdump /etc/localtime
/etc/localtime  Wed Jul 13 10:22:06 2016 CDT
deft-virtual-machine ~ %
```


6. Identify the operating system version. Enter the command below.

```
uname -a
```

```
deft-virtual-machine ~ % uname -a
Linux deft-virtual-machine 3.5.0-51-generic #76-Ubuntu SMP Thu May 15 21:19:10 U
TC 2014 x86_64 x86_64 x86_64 GNU/Linux
deft-virtual-machine ~ %
```

Notice that the system is a 64-bit version of *Ubuntu* with a *Kernel* version of *3.5.0-51-generic*.

7. Identify the distribution information. Enter the command below.

```
cat /etc/issue
```

```
deft-virtual-machine ~ % cat /etc/issue
Ubuntu 12.10 \n \l

deft-virtual-machine ~ %
```

8. For deeper detailing on the distribution information, issue the command below.

```
cat /etc/lsb-release
```

```
deft-virtual-machine ~ % cat /etc/lsb-release
DISTRIB_ID=DEFT
DISTRIB_RELEASE=8
DISTRIB_CODENAME=Ball in hole
DISTRIB_DESCRIPTION="DEFT Linux 8"
deft-virtual-machine ~ %
```

Notice that codename for this Deft Linux is “Ball in hole”.

9. Issue the command below to determine when the OS was installed. Use the SSH keys since they are generated on the initial install date of the system.

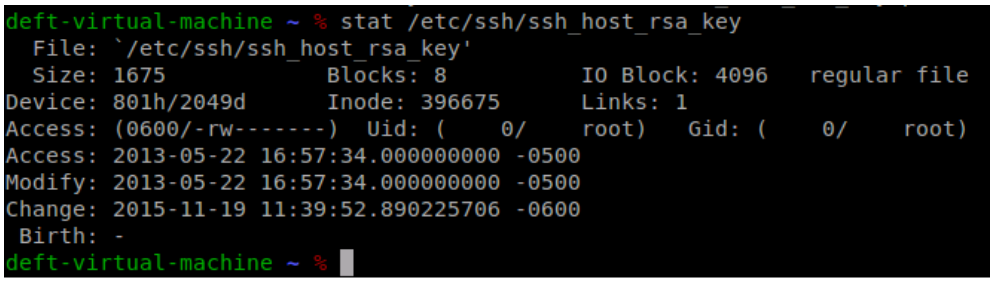
```
ls -l /etc/ssh/ssh_host*
```

```
deft-virtual-machine ~ % ls -l /etc/ssh/ssh_host*
-rw------- 1 root root  668 May 22  2013 /etc/ssh/ssh_host_dsa_key
-rw-r--r-- 1 root root  602 May 22  2013 /etc/ssh/ssh_host_dsa_key.pub
-rw------- 1 root root  227 May 22  2013 /etc/ssh/ssh_host_ecdsa_key
-rw-r--r-- 1 root root  174 May 22  2013 /etc/ssh/ssh_host_ecdsa_key.pub
-rw------- 1 root root 1675 May 22  2013 /etc/ssh/ssh_host_rsa_key
-rw-r--r-- 1 root root  394 May 22  2013 /etc/ssh/ssh_host_rsa_key.pub
deft-virtual-machine ~ %
```

Notice the date appears to be *May 22, 2013* as the initial install date.

10. Dig a little deeper by viewing the contents of the **ssh_host_rsa_key** file. Enter the command below.

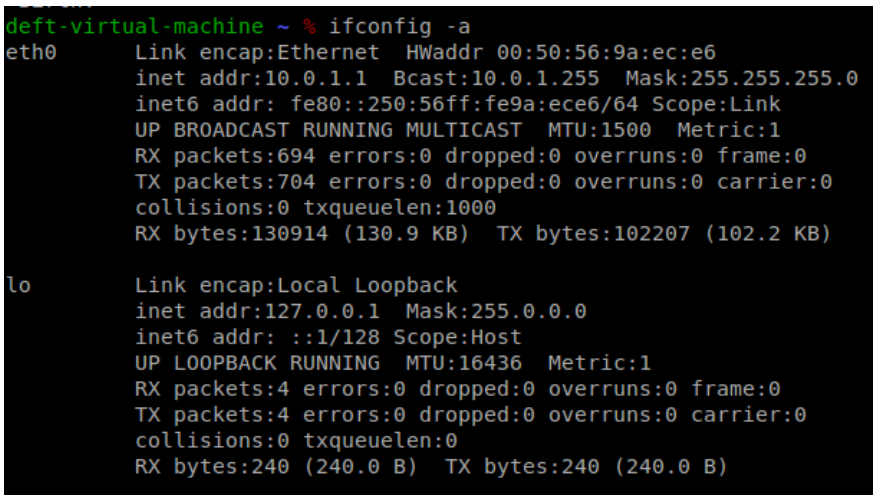
```
stat /etc/ssh/ssh_host_rsa_key
```



Notice the file has a *Modify* and *Access* date of May 22, 2013 and the same timestamp for both values.

11. Identify the network interfaces by entering the command below.

```
ifconfig -a
```



Only two network interfaces should appear.

12. Another alternative to receive information about the network interfaces can be accomplished by entering the command below.

```
ip addr
```

```
deft-virtual-machine ~ % ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 00:50:56:9a:ec:e6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.1/24 brd 10.0.1.255 scope global eth0
    inet6 fe80::250:56ff:fe9a:ece6/64 scope link
       valid_lft forever preferred_lft forever
```

13. Enter the command below to identify the computer name.

```
cat /etc/hostname
```

```
deft-virtual-machine ~ % cat /etc/hostname
deft-virtual-machine
deft-virtual-machine ~ %
```

14. Enter the command below to identify the current network connections that the *Deft Linux* system has.

```
sudo netstat -anp
```

```
deft-virtual-machine ~ % sudo netstat -anp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
749/smbd
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
1253/dnsmasq
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
2213/cupsd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
749/smbd
tcp6       0      0 :::139                  :::*                    LISTEN
749/smbd
tcp6       0      0 ::1:631                 :::*                    LISTEN
2213/cupsd
tcp6       0      0 :::445                  :::*                    LISTEN
749/smbd
```

If prompted for a password, type **`password`** and press **Enter**.

15. Identify the routing information present on the system by issuing the command below.

```
netstat -rn
```

```
deft-virtual-machine ~ % netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.1.254      0.0.0.0         UG        0 0          0 eth0
10.0.1.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
deft-virtual-machine ~ %
```

16. An alternative command to show routing information can be used by entering the command below.

```
route
```

```
deft-virtual-machine ~ % route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.0.1.254      0.0.0.0         UG    0      0        0 eth0
10.0.1.0        *               255.255.255.0   U     1      0        0 eth0
deft-virtual-machine ~ %
```

17. Identify which open files are using the ports from *Task 1, Step 14*. Enter the command below.

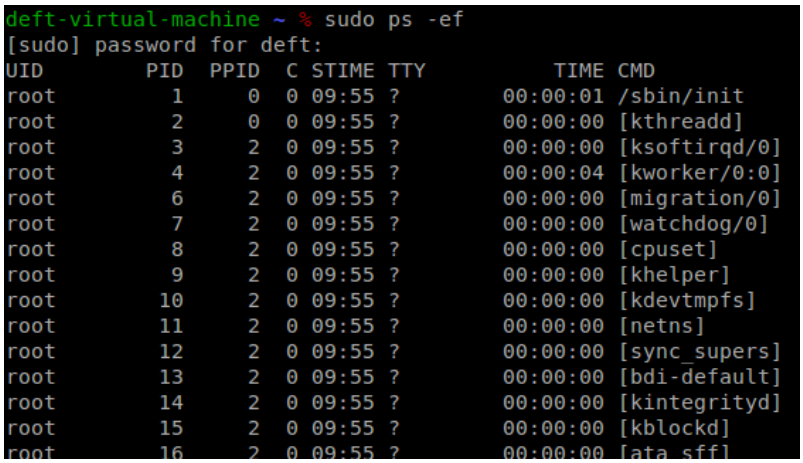
```
sudo lsof -V
```

```
deft-virtual-machine ~ % sudo lsof -V
[sudo] password for deft:
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/deft/gvfs
      Output information may be incomplete.
COMMAND    PID  TID       USER   FD      TYPE             DEVICE SIZE/OFF
NODE NAME
init         1            root  cwd       DIR               8,1     4096
   2 /
init         1            root  rtd       DIR               8,1     4096
   2 /
init         1            root  txt       REG               8,1   163144     78
6701 /sbin/init
init         1            root  mem       REG               8,1    52152     26
7056 /lib/x86_64-linux-gnu/libnss_files-2.15.so
init         1            root  mem       REG               8,1    47712     26
7060 /lib/x86_64-linux-gnu/libnss_nis-2.15.so
init         1            root  mem       REG               8,1    97272     26
7050 /lib/x86_64-linux-gnu/libnsl-2.15.so
```

If prompted for a password, type **`password`** and press **Enter**.

18. Identify which system processes are currently running. Enter the command below.

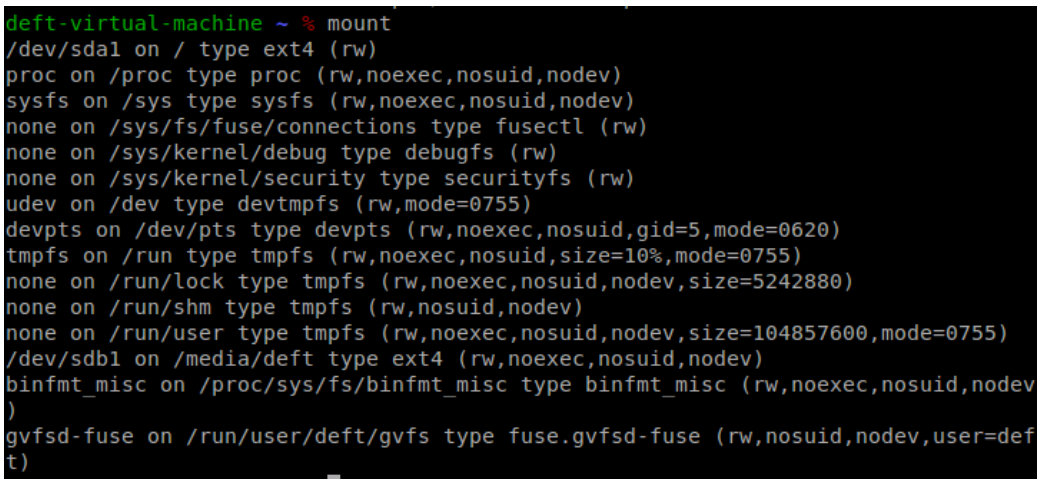
```
sudo ps -ef
```



If prompted for a password, type **password** and press **Enter**.

19. Identify what file systems are mounted and how much space they are utilizing. Enter the command below.

```
mount
```



Notice that the hard disk partition *sda1* and another partition mounted as in media *sdb1* are mounted.

20. Another alternative to see what disks are mounted is to view the contents of the *mtab* file. Enter the command below.

```
cat /etc/mtab
```

```
deft-virtual-machine ~ % cat /etc/mtab
/dev/sda1 / ext4 rw 0 0
proc /proc proc rw,noexec,nosuid,nodev 0 0
sysfs /sys sysfs rw,noexec,nosuid,nodev 0 0
none /sys/fs/fuse/connections fusectl rw 0 0
none /sys/kernel/debug debugfs rw 0 0
none /sys/kernel/security securityfs rw 0 0
udev /dev devtmpfs rw,mode=0755 0 0
devpts /dev/pts devpts rw,noexec,nosuid,gid=5,mode=0620 0 0
tmpfs /run tmpfs rw,noexec,nosuid,size=10%,mode=0755 0 0
none /run/lock tmpfs rw,noexec,nosuid,nodev,size=5242880 0 0
none /run/shm tmpfs rw,nosuid,nodev 0 0
none /run/user tmpfs rw,noexec,nosuid,nodev,size=104857600,mode=0755 0 0
/dev/sdb1 /media/deft ext4 rw,noexec,nosuid,nodev 0 0
binfmt_misc /proc/sys/fs/binfmt_misc binfmt_misc rw,noexec,nosuid,nodev 0 0
gvfsd-fuse /run/user/deft/gvfs fuse.gvfsd-fuse rw,nosuid,nodev,user=deft 0 0
```

21. Enter the command below to view the contents of the partitions file.

```
cat /proc/partitions
```

```
deft-virtual-machine ~ % cat /proc/partitions
major minor  #blocks  name

  11        0    1048575 sr0
   8        0   20971520 sda
   8        1   18874368 sda1
   8        2          1 sda2
   8        5    2094080 sda5
   8       16   20971520 sdb
   8       17   20971486 sdb1
deft-virtual-machine ~ %
```

Notice how this command shows more drives. Reference the number *8* underneath the *major* column indicates a *SCSI HD* while the *11* indicates a *SCSI CD-ROM* device.

```
8 block    SCSI disk devices (0-15)
             0 = /dev/sda          First SCSI disk whole disk
            16 = /dev/sdb          Second SCSI disk whole disk
            32 = /dev/sdc          Third SCSI disk whole disk
               ...
           240 = /dev/sdp          Sixteenth SCSI disk whole disk

           Partitions are handled in the same way as for IDE
           disks (see major number 3) except that the limit on
           partitions is 15.
```

```
11 block   SCSI CD-ROM devices
             0 = /dev/scd0         First SCSI CD-ROM
             1 = /dev/scd1         Second SCSI CD-ROM
               ...

           The prefix /dev/sr (instead of /dev/scd) has been deprecated.
```


22. Verify the mounted disks with *fdisk*. Enter the command below.

```
sudo fdisk -l
```

```
deft-virtual-machine ~ % sudo fdisk -l
[sudo] password for deft:

Disk /dev/sda: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders, total 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0002e7f9

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048    37750783    18874368   83  Linux
/dev/sda2        37752830    41940991     2094081    5  Extended
/dev/sda5        37752832    41940991     2094080   82  Linux swap / Solaris

WARNING: GPT (GUID Partition Table) detected on '/dev/sdb'! The util fdisk doesn
't support GPT. Use GNU Parted.


Disk /dev/sdb: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders, total 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1    41943039    20971519+  ee  GPT
deft-virtual-machine ~ %
```

If prompted for a password, type **`password`** and press **Enter**.

23. The fstab file can be viewed for physical and logical disk partitions available on the system for both mounted and unmounted. Enter the command below.

```
cat /etc/fstab
```

```
deft-virtual-machine ~ % cat /etc/fstab
/dev/fd0 /media/floppy0 vfat noauto 0 0
UUID=759ce1da-9adb-4563-a87a-01eeb58bd24a swap swap sw 0 0
UUID=6a8aa896-2633-4134-9a04-da5b825504e3 /media/deft ext4 user,rw 0 0
UUID=722da13a-a275-43f7-bd42-26860e5b6803 / ext4 defaults 0 1
deft-virtual-machine ~ %
```


24. Given a scenario, sometimes a user or malware can load small pieces of code into the Kernel of the operating system. Identify what is loaded on the system by entering the command below.

```
lsmod
```

```
deft-virtual-machine ~ % lsmod
Module                  Size  Used by
vsock                  52876  0
acpiphp                24025  0
ib_iser                37866  0
rdma_cm                43022  1 ib_iser
ib_cm                  42682  1 rdma_cm
iw_cm                  18583  1 rdma_cm
ib_sa                  29096  2 rdma_cm,ib_cm
ib_mad                 47134  2 ib_cm,ib_sa
ib_core                82363  6 ib_iser,rdma_cm,ib_cm,iw_cm,ib_sa,ib_mad
ib_addr                14110  1 rdma_cm
iscsi_tcp              18334  0
libiscsi_tcp           25147  1 iscsi_tcp
libiscsi               57110  3 ib_iser,iscsi_tcp,libiscsi_tcp
scsi_transport_iscsi    59269  4 ib_iser,iscsi_tcp,libiscsi
coretemp               13401  0
bnep                   18141  2
rfcomm                 46620  0
ghash_clmulni_intel    13221  0
bluetooth             209438  10 bnep,rfcomm
aesni_intel            51038  0
cryptd                 20404  2 ghash_clmulni_intel,aesni_intel
```

25. Leave the terminal open to continue with the next task.

2 Analyzing the Linux User Information

1. Using the terminal, enter the command below to identify who is currently logged into the system.

```
w
```

```
deft-virtual-machine ~ % w
 14:21:08 up  4:25,  2 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
deft     tty7     :0               09:55    4:25m  3.46s  0.11s /usr/bin/lxsession -s
deft     pts/0    :0.0             13:19    4.00s  0.05s  0.00s w
deft-virtual-machine ~ %
```

Notice that the user “deft” is logged in.

2. Identify who last logged into the system by issuing the command below.

```
last
```

```
deft-virtual-machine ~ % last
deft     pts/0        :0.0             Wed Jul 13 13:19   still logged in
deft     pts/0        :0.0             Wed Jul 13 13:17 - 13:19  (00:02)
deft     pts/0        :0.0             Wed Jul 13 11:16 - 13:17  (02:00)
deft     pts/0        :0.0             Wed Jul 13 10:11 - 11:16  (01:04)
reboot   system boot  3.5.0-51-generic Wed Jul 13 09:55 - 14:23  (04:27)

wtmp begins Tue Jul 12 18:50:25 2016
deft-virtual-machine ~ %
```

The information outputted from the *last* command comes from the */var/log/wtmp* file.

3. Identify the failed attempt logins on the system. Enter the command below.

```
sudo lastb
```

```
deft-virtual-machine ~ % sudo lastb
[sudo] password for deft:

btmp begins Tue Jul 12 18:09:59 2016
deft-virtual-machine ~ %
```

If prompted for a password, type **`password`** and press **Enter**.

Notice no failed logins appear. The information outputted from the *lastb* command comes from the */var/log/btmp* file.

4. Verify if the *btmp* file is empty by entering the command below.

```
file /var/log/btmp.1
```

```
deft-virtual-machine ~ % file /var/log/btmp.1
/var/log/btmp.1: empty
```

5. On a Linux system, system accounts and user accounts are held in a file named *passwd*. View the contents of this file by entering the command below.

```
cat /etc/passwd | less
```

```
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
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false
ntp:x:104:109::/home/ntp:/bin/false
whoopsie:x:105:110::/nonexistent:/bin/false
lightdm:x:106:115:Light Display Manager:/var/lib/lightdm:/bin/false
haldaemon:x:107:117:Hardware abstraction layer,,,:/var/run/hald:/bin/false
postgres:x:108:119:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
postfix:x:109:121::/var/spool/postfix:/bin/false
:
```

With the *less* command, use the **Enter** key to skip to the next line item of the list or use the **spacebar** to skip by page. Notice that the *deft* account has a unique ID of *1000* and a group ID of *1000* with a home directory of */home/deft* and default shell of *bash*. When finished analyzing the file, press the **q** character to quit.

6. Make the *deft* user account properties more readable by entering the command below.

```
id deft
```

```
deft-virtual-machine ~ % id deft
uid=1000(deft) gid=1000(deft) groups=1000(deft),4(adm),24(cdrom),27(sudo),30(dip),46(pl
ugdev),106(lpadmin),124(sambashare)
deft-virtual-machine ~ %
```

Notice additional information is given such that the *deft* user account has *sudo* and *sambashare* rights.

7. Identify the properties of the *root* account by entering the command below.

```
id root
```

```
deft-virtual-machine ~ % id root
uid=0(root) gid=0(root) groups=0(root)
deft-virtual-machine ~ %
```

Notice that the *root* user has a unique ID of *0* and a group ID of *0*.

8. On a Linux system, passwords are typically stored in the *shadow* file. Enter the command below to observe the contents of the file.

```
sudo cat /etc/shadow | less
```

```
root:!:16758:0:99999:7:::
daemon:*:15630:0:99999:7:::
bin:*:15630:0:99999:7:::
sys:*:15630:0:99999:7:::
sync:*:15630:0:99999:7:::
games:*:15630:0:99999:7:::
man:*:15630:0:99999:7:::
lp:*:15630:0:99999:7:::
mail:*:15630:0:99999:7:::
news:*:15630:0:99999:7:::
uucp:*:15630:0:99999:7:::
proxy:*:15630:0:99999:7:::
www-data:*:15630:0:99999:7:::
backup:*:15630:0:99999:7:::
list:*:15630:0:99999:7:::
irc:*:15630:0:99999:7:::
gnats:*:15630:0:99999:7:::
nobody:*:15630:0:99999:7:::
libuuid:!:15630:0:99999:7:::
syslog:*:15630:0:99999:7:::
messagebus:*:15630:0:99999:7:::
usbmux:*:15630:0:99999:7:::
ntp:*:15630:0:99999:7:::
whoopsie:*:15630:0:99999:7:::
lightdm:*:15630:0:99999:7:::
haldaemon:*:15842:0:99999:7:::
postgres:*:15845:0:99999:7:::
postfix:*:15847:0:99999:7:::
:
```


If prompted for a password, type **password** and press **Enter**.

```
deft:$6$APbTaP4P$ClkTKayAL.ICTFKlxJGRZuE.VbWVEmkvXXvk6kLxrmUS/H886zv429SkzwhNs3OlpkCgYC
MlCm9UXBH9JU/rH1:16758:0:99999:7:::
```

With the *less* command, use the **Enter** key to skip to the next line item of the list or use the **spacebar** to skip by page. Notice that the *deft* account has a password that's encrypted. Note that with a "*!*" or "***" are blank passwords. When finished analyzing the file, press the **q** character to quit.

9. Verify that you are currently in the */home/deft* directory by issuing the command below.

```
pwd
```

```
deft-virtual-machine ~ % pwd
/home/deft
deft-virtual-machine ~ %
```

10. Investigate *deft's* home directory, identifying the files and hidden files by entering the command below.

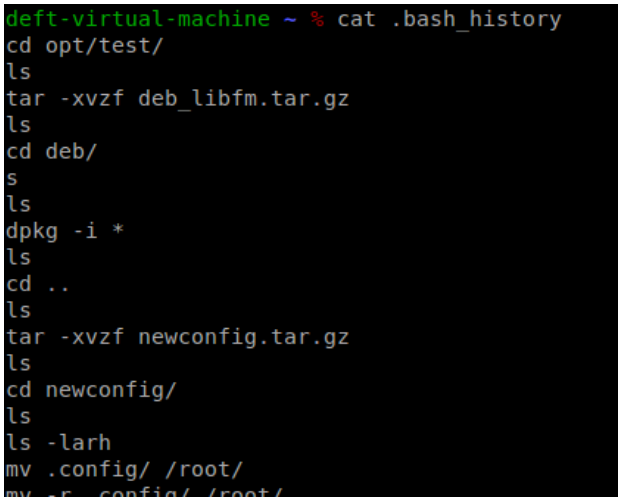
```
ls -a
```

```
deft-virtual-machine ~ % ls -a
.               Documents             .local          .pulse
..              Downloads             .macromedia     .pulse-cookie
.adobe          evidence              .mountmanager   .ssh
.android        .gconf                .mozilla        Templates
.ant            .gksu.lock            .mtpaint        .thumbnails
.bash_history   .gnome                Music           Videos
.bashrc         .gstreamer-0.10       NewFolder       .vim
.cache          .gtk-bookmarks        pdfcrack-01.5   .viminfo
.config         .icons                .pip            .Xauthority
.dbus           .java                 .pki            .xscreensaver
Desktop         .lesshst              .profile        .xsession-errors
.dmrc           .libnet-openssh-perl  Public          .xsession-errors.old
deft-virtual-machine ~ %
```

Note that files with a period in front of their names are hidden files.

11. Observe the command history by entering the command below.

```
cat .bash_history
```



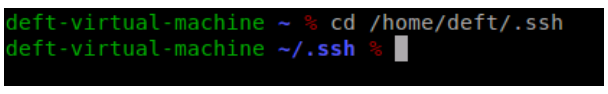
The data will vary when compared to the image above.

12. An alternative way of viewing the bash history is to use the *history* command. Enter the command below.

```
history
```

13. Navigate to the *ssh* directory by issuing the command below.

```
cd /home/deft/.ssh
```



14. Enter the command below to identify what files are present.

```
ls
```

```
deft-virtual-machine ~/.ssh % ls
known_hosts
```

15. View the *SSH* information inside the **known_hosts** file. Enter the command below.

```
cat known_hosts
```

```
deft-virtual-machine ~/.ssh % cat known_hosts
|1|ZySyHcw20VJzeegL15/C2M0QbDw=|YfCgO5zgT1OT8Fq2HBwTabeZiig= ecdsa-sha2-nistp256 AAAAE2
VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEccjUPOlCsIrGpsT45zk91YzeUDbgsW2eLt8Vukf
IGX38mNrDyDvzaufsDsw5aNYSn6H5bdhnWA1AaVlSSZddg=
|1|87cA2m+pNSgWQ6g2X+QjOW/08sU=|BGKtBwexr1kkrZTeYzbAOA/bNYI= ecdsa-sha2-nistp256 AAAAE2
VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAvWE8XFKvwtHYQ6qZvQP0aoz7/GMNF2tIKA5CjUM
5JEpbcZH18vcjd7xpUsqS9tCK7KQdibiTS8oCh6Ey+7qzg=
|1|YlEaIXgpvQyHQV9Gn0SJjf1I9wg=|l4TDZUbpGMyU+Yk0Lil2lL4xpfo= ecdsa-sha2-nistp256 AAAAE2
VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAvWE8XFKvwtHYQ6qZvQP0aoz7/GMNF2tIKA5CjUM
5JEpbcZH18vcjd7xpUsqS9tCK7KQdibiTS8oCh6Ey+7qzg=
deft-virtual-machine ~/.ssh %
```

These are the local *SSH* keys for known connections.

16. Identify if there are any other accounts on the system that possess *sudo* rights. Enter the command below.

```
sudo cat /etc/sudoers
```

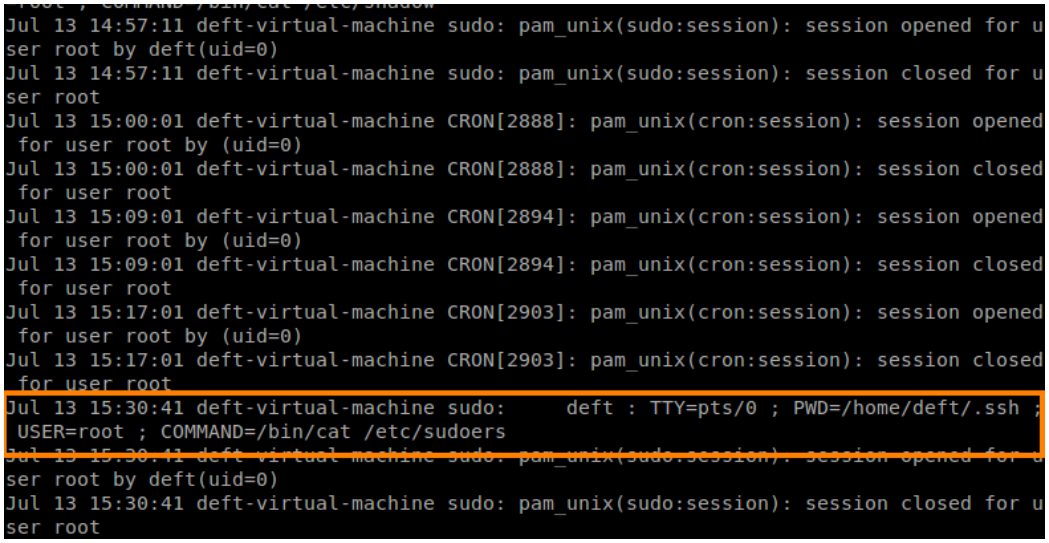
```
# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

If prompted for a password, type **`password`** and press **Enter**.

Notice that anyone on the system can have sudo rights.

17. View the *sudoers* history by issuing the command below.

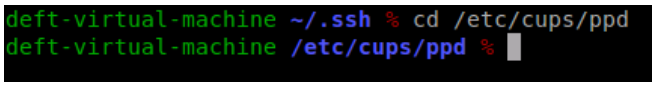
```
cat /var/log/auth.log
```



Viewing this file helps identify when *sudo* was invoked and by whom. Notice towards the bottom, it can be seen that deft asked for *sudo* rights when then "*sudo cat /etc/sudoers*" was entered.

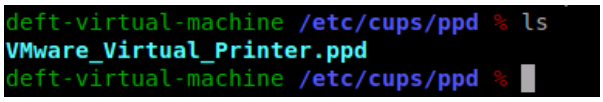
18. Change to the /etc/cups/ppd directory by entering the command below.

```
cd /etc/cups/ppd
```



19. Identify whether the user had any printers by entering the command below.

```
ls
```



Notice that only a virtual printer appears.

20. Identify whether the user plug in any external *USB* devices. Enter the command below.

```
cat /var/log/kern.log | less
```

With the *less* command, use the **Enter** key to skip to the next line item of the list or use the **spacebar** to skip by page. When finished analyzing the file, press the **q** character to quit.

21. Scrolling through can be difficult when trying to locate something specific in a given file. Enter the command below to look specifically for the term "*usb*".

```
cat /var/log/kern.log | grep -i usb
```

```
deft-virtual-machine /etc/cups/ppd % cat /var/log/kern.log | grep -i usb
Jul 13 09:55:54 deft-virtual-machine kernel: [    0.452029] ACPI: bus type usb register
ed
Jul 13 09:55:54 deft-virtual-machine kernel: [    0.452042] usbcore: registered new int
erface driver usbfs
Jul 13 09:55:54 deft-virtual-machine kernel: [    0.452048] usbcore: registered new int
erface driver hub
Jul 13 09:55:54 deft-virtual-machine kernel: [    0.452066] usbcore: registered new dev
ice driver usb
Jul 13 09:55:54 deft-virtual-machine kernel: [    1.095452] ehci_hcd: USB 2.0 'Enhanced
' Host Controller (EHCI) Driver
Jul 13 09:55:54 deft-virtual-machine kernel: [    1.095464] ohci_hcd: USB 1.1 'Open' Ho
st Controller (OHCI) Driver
Jul 13 09:55:54 deft-virtual-machine kernel: [    1.095475] uhci_hcd: USB Universal Hos
t Controller Interface driver
Jul 13 09:55:54 deft-virtual-machine kernel: [    1.095501] usbcore: registered new int
erface driver libusual
deft-virtual-machine /etc/cups/ppd %
```

Anything with the term "usb" will be displayed in a red font. Notice no removable device was attached to this system.

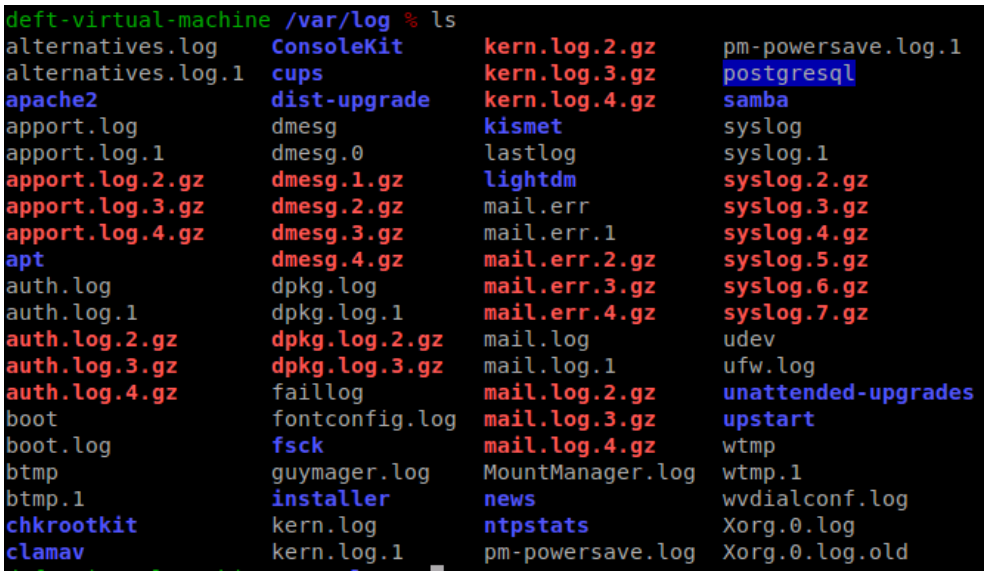
22. Navigate to the /var/log directory. Enter the command below.

```
cd /var/log
```

```
deft-virtual-machine /etc/cups/ppd % cd /var/log
deft-virtual-machine /var/log %
```


23. A bulk of information can be found in the logs. Enter the command below and take notice of the various log files presented.

```
ls
```



Log analysis will be taught more in depth in *Lab 19* of the *NDG Forensics* lab series.

24. Close all **PC Viewers** and end the reservation to complete the lab.

