



FORENSICS LAB SERIES

Lab 19: Log Analysis

Material in this Lab Aligns to the Following Certification Domains/Objectives	
GIAC Certified Forensics Examiner (GCFE) Domains	Computer Hacking Forensic Investigator (CHFI) Objectives
5: Log Analysis	16: Network Forensics, Investigating Logs, and Investigating Network Traffic

Document Version: 2016-08-17

Contents

Introduction	3
Objective	3
Pod Topology	4
Lab Settings	5
1 Examining Linux Logs	6
2 Examining Windows Event Logs	11

Introduction

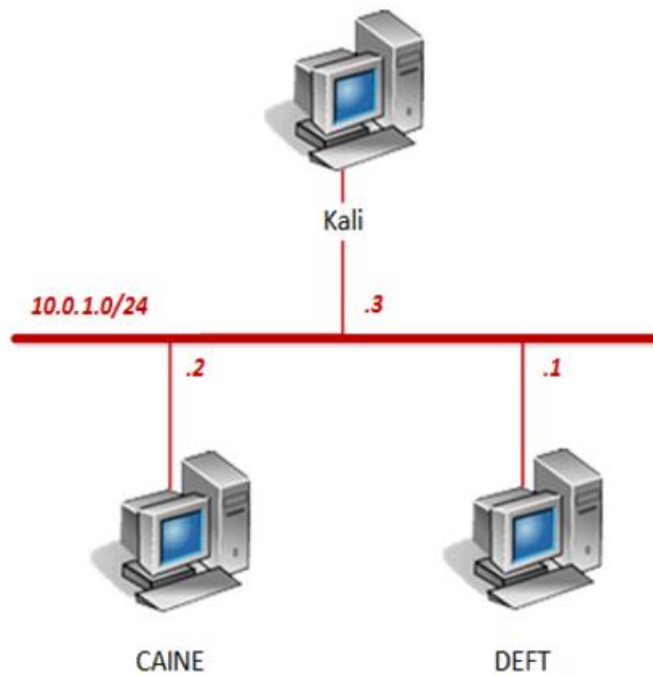
This lab will introduce how to analyze logs, which is an important skill to have in order to curate information about the actions performed by an individual on a computer. In this lab, Linux logs and Windows event logs will be explored.

Objective

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

1. Examining Linux Logs
2. Examining Windows Event Logs

Pod Topology



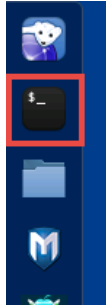
Lab Settings

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 Examining Linux Logs

1. Click on the **Kali** graphic on the *topology page* to open the VM.
2. Login using **root** as the *username* and **toor** as the *password*.
3. Open a new terminal by clicking on the **Terminal** icon located in the left tool pane.



4. Using the terminal, enter the command below to change to the **/var/log/** directory.

```
cd /var/log
```

```
root@Kali2:~# cd /var/log
root@Kali2:/var/log#
```

5. List the files in the current directory by entering the command below.

```
ls
```

```
root@Kali2:/var/log# ls
alternatives.log      debug.4.gz           lynis.log            redis
alternatives.log.1    dmesg               lynis-report.dat     samba
alternatives.log.2.gz dpkg.log            macchanger.log       speech-dispatcher
alternatives.log.3.gz dpkg.log.1          macchanger.log.1.gz stunnel4
alternatives.log.4.gz dpkg.log.2.gz       macchanger.log.2.gz syslog
apache2               dpkg.log.3.gz       macchanger.log.3.gz syslog.1
apt                  dpkg.log.4.gz       macchanger.log.4.gz syslog.2.gz
auth.log             dpkg.log.5.gz       messages             syslog.3.gz
auth.log.1           dpkg.log.6.gz       messages.1           syslog.4.gz
auth.log.2.gz        dpkg.log.7.gz       messages.2.gz        syslog.5.gz
auth.log.3.gz        dpkg.log.8.gz       messages.3.gz        syslog.6.gz
auth.log.4.gz        dradis              messages.4.gz        syslog.7.gz
bootstrap.log        exim4               mysql                user.log
btmp                 faillog             mysql.err            user.log.1
btmp.1               fontconfig.log      mysql.log            user.log.2.gz
chkrootkit           fsck                mysql.log.1.gz       user.log.3.gz
daemon.log           gdm3               mysql.log.2.gz       user.log.4.gz
daemon.log.1         inetsim             mysql.log.3.gz       vsftpd.log
daemon.log.2.gz      installer           mysql.log.4.gz       vsftpd.log.1
daemon.log.3.gz      kern.log            mysql.log.5.gz       wtmp
daemon.log.4.gz      kern.log.1          mysql.log.6.gz       wtmp.1
debug               kern.log.2.gz       mysql.log.7.gz       wvdialconf.log
debug.1              kern.log.3.gz       ntpstats             Xorg.0.log
debug.2.gz           kern.log.4.gz       openvas              Xorg.0.log.old
debug.3.gz           lastlog             postgresql            Xorg.1.log
root@Kali2:/var/log#
```

These are the main log files in a Linux operating system.



6. Enter the command below using the *last* command to view the contents of the *utmp* file.

```
last -f /var/run/utmp
```

```
root@Kali2:/var/log# last -f /var/run/utmp
root    pts/0      :0                Fri Aug  5 13:19    still logged in
root    :0         :0                Fri Aug  5 13:19    still logged in
reboot  system boot  4.0.0-kali1-amd64 Fri Aug  5 07:48 - 13:35  (05:47)

utmp begins Fri Aug  5 07:48:36 2016
root@Kali2:/var/log#
```

Notice the *utmp* file shows who is currently logged onto the system with a time and date stamp.

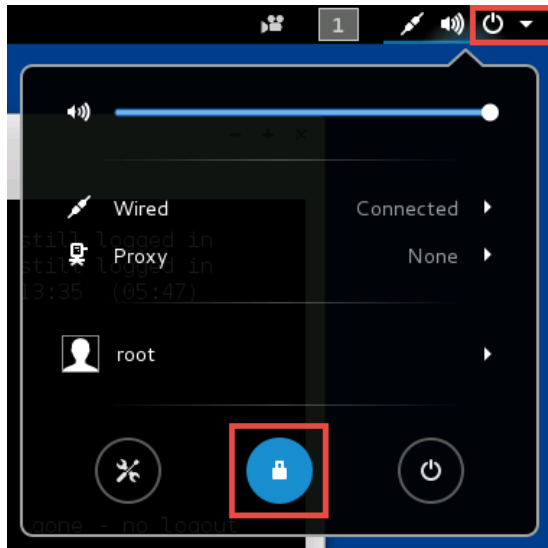
7. Enter the command below to view the contents of the *btmp* file.

```
last -f btmp
```

```
root@Kali2:/var/log# last -f btmp
btmp begins Fri Aug  5 07:48:44 2016
root@Kali2:/var/log#
```

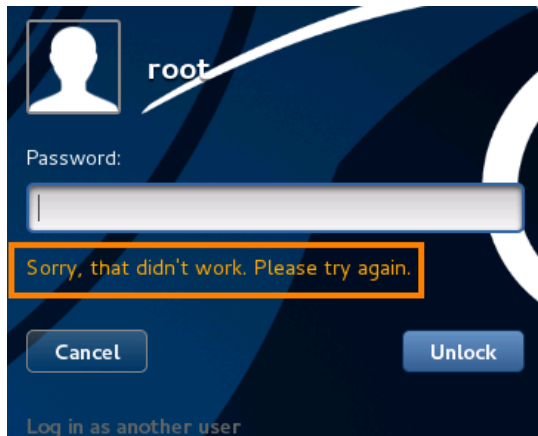
The *btmp* file records failed login attempts but notice no information is available.

8. Logout of the system by clicking on the **power** icon located in the upper-right corner, followed by clicking on the **lock** icon.



9. Once the time and date appears on the screen, press the **Enter** key to bring up the login prompt.

10. Type `root` into the *Password* field, press **Enter**.



Notice the message stating that the password was incorrect.

11. This time type `toor` into the *Password* field, press **Enter**.

12. Using the same terminal, enter the command below once more.

```
last -f btmp
```

```
root@Kali2:/var/log# last -f btmp
root      :0                :0                Fri Aug  5 13:39    gone - no logout

btmp begins Fri Aug  5 13:39:40 2016
root@Kali2:/var/log#
```

Notice now that *btmp* is able to report a failed login attempt for the *root* account.

13. Enter the command below to view the contents of the *wtmp* file.

```
last -f wtmp
```

```
root@Kali2:/var/log# last -f wtmp
root      pts/0                :0                Fri Aug  5 13:19    still logged in
root      :0                :0                Fri Aug  5 13:19    still logged in
(unknown) :0                :0                Fri Aug  5 07:49 - 13:19    (05:30)
reboot    system boot      4.0.0-kali1-amd64 Fri Aug  5 07:48 - 13:48    (05:59)
root      pts/0                :0                Thu Aug  4 14:09 - 18:20    (04:10)
root      :0                :0                Thu Aug  4 14:02 - 18:20    (04:18)

wtmp begins Thu Aug  4 14:02:07 2016
root@Kali2:/var/log#
```

The *wtmp* file is a historical record of the *utmp* file.

14. Enter the command below to see if any user logged in remotely over the network.

```
lastlog
```

```
root@Kali2:/var/log# lastlog
Username      Port      From      Latest
root          *Never   logged in**
daemon        *Never   logged in**
bin           *Never   logged in**
sys           *Never   logged in**
sync          *Never   logged in**
games         *Never   logged in**
man           *Never   logged in**
lp            *Never   logged in**
mail          *Never   logged in**
news          *Never   logged in**
uucp          *Never   logged in**
proxy         *Never   logged in**
www-data      *Never   logged in**
```

After briefly analyzing through the list, notice no user logged in remotely.

15. The *auth.log* is a log file that shows authorization information including user's logins and the services the operating system used. Enter the command below to view the contents of the **auth.log** file.

```
less auth.log
```

```
Aug  4 14:09:01 Kali2 CRON[1856]: pam_unix(cron:session): session opened for use
r root by (uid=0)
Aug  4 14:09:02 Kali2 CRON[1856]: pam_unix(cron:session): session closed for use
r root
Aug  4 14:17:01 Kali2 CRON[2003]: pam_unix(cron:session): session opened for use
r root by (uid=0)
Aug  4 14:17:01 Kali2 CRON[2003]: pam_unix(cron:session): session closed for use
r root
Aug  4 14:39:01 Kali2 CRON[2035]: pam_unix(cron:session): session opened for use
r root by (uid=0)
Aug  4 14:39:02 Kali2 CRON[2035]: pam_unix(cron:session): session closed for use
r root
Aug  4 15:09:01 Kali2 CRON[2095]: pam_unix(cron:session): session opened for use
r root by (uid=0)
Aug  4 15:09:01 Kali2 CRON[2095]: pam_unix(cron:session): session closed for use
r root
Aug  4 15:17:01 Kali2 CRON[2120]: pam_unix(cron:session): session opened for use
:
```

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.

16. Another log that may be useful to examine is the *dpkg* log, which shows what software was installed. It is snapshotted during each reboot of the system. Enter the command below to view the contents of the archived **dpkg.log.1** file.

```
less dpkg.log.1
```

```
2016-05-20 10:19:15 status unpacked vsftpd:amd64 3.0.2-17
2016-05-20 10:19:15 trigproc man-db:amd64 2.7.0.2-5 <none>
2016-05-20 10:19:15 status half-configured man-db:amd64 2.7.0.2-5
2016-05-20 10:19:17 status installed man-db:amd64 2.7.0.2-5
2016-05-20 10:19:17 trigproc systemd:amd64 215-17+deb8u1 <none>
2016-05-20 10:19:17 status half-configured systemd:amd64 215-17+deb8u1
2016-05-20 10:19:18 status installed systemd:amd64 215-17+deb8u1
2016-05-20 10:19:18 startup packages configure
2016-05-20 10:19:18 configure dialog:amd64 1.2-20140911-1 <none>
2016-05-20 10:19:18 status unpacked dialog:amd64 1.2-20140911-1
2016-05-20 10:19:18 status half-configured dialog:amd64 1.2-20140911-1
2016-05-20 10:19:18 status installed dialog:amd64 1.2-20140911-1
2016-05-20 10:19:18 configure vsftpd:amd64 3.0.2-17 <none>
2016-05-20 10:19:18 status unpacked vsftpd:amd64 3.0.2-17
2016-05-20 10:19:18 status unpacked vsftpd:amd64 3.0.2-17
2016-05-20 10:19:18 status unpacked vsftpd:amd64 3.0.2-17
2016-05-20 10:19:18 status triggers-pending systemd:amd64 215-17+deb8u1
2016-05-20 10:19:18 status unpacked vsftpd:amd64 3.0.2-17
2016-05-20 10:19:18 status unpacked vsftpd:amd64 3.0.2-17
2016-05-20 10:19:18 status unpacked vsftpd:amd64 3.0.2-17
dpkg.log.1
```

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.

2 Examining Windows Event Logs

1. Click on the **CAINE** graphic on the *topology page* to open the VM.
2. Open a new terminal by clicking on the **Mate Terminal** icon located on the bottom tool pane.



3. Using the terminal, navigate to `/home/caine/Downloads/Parse-Evtx-1.1.1` by entering the command below.

```
cd Downloads/Parse-Evtx-1.1.1
```

```
caine@Caine01:~$ cd Downloads/Parse-Evtx-1.1.1
caine@Caine01:~/Downloads/Parse-Evtx-1.1.1$
```

4. Enter the command below to list the files in the current directory.

```
ls
```

```
caine@Caine01:~/Downloads/Parse-Evtx-1.1.1$ ls
blib          lib          MANIFEST     MYMETA.yml   scripts
CHANGELOG.txt Makefile     META.yml     pm_to_blib
GPL-2.0.txt   Makefile.PL MYMETA.json  README.txt
caine@Caine01:~/Downloads/Parse-Evtx-1.1.1$
```

5. Navigate to the **scripts/** folder by entering the command below.

```
cd scripts
```

```
caine@Caine01:~/Downloads/Parse-Evtx-1.1.1$ cd scripts
caine@Caine01:~/Downloads/Parse-Evtx-1.1.1/scripts$
```



6. Using the *evtxdump.pl* Perl script, view the contents of the **Application.evtx** log by entering the command below.

```
./evtxdump.pl /home/caine/Downloads/Application.evtx | less
```

```
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
<Events>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Name="Microsoft-Windows-User Profiles Service" Guid="{89B1E9F0-5AFF-44
A6-9B44-0A07A7CE5845}" />
<EventID>1532</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords>
<TimeCreated SystemTime="2010-11-21T03:58:31.1243Z" />
<EventRecordID>1</EventRecordID>
<Correlation />
<Execution ProcessID="928" ThreadID="996" />
<Channel>Application</Channel>
<Computer>37L4247F27-25</Computer>
<Security UserID="S-1-5-18" /></System>
<EventData></EventData></Event>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Name="Microsoft-Windows-EventSystem" Guid="{899daace-4868-4295-afcd-9e
:"
```

The *Perl* script helps translate the original file format of the *Application.evtx* file, which is in *XML* format into human readable *ASCII* format. Briefly analyze the log file for installed software or problems with software.

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.



7. View the contents of the **System.evtx** log file by entering the command below.

```
./evtxdump.pl /home/caine/Downloads/System.evtx | less
```

```
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
<Events>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Name="EventLog" />
<EventID Qualifiers="32768">6011</EventID>
<Level>4</Level>
<Task>0</Task>
<Keywords>0x0080000000000000</Keywords>
<TimeCreated SystemTime="2015-03-25T10:15:46.0Z" />
<EventRecordID>1</EventRecordID>
<Channel>System</Channel>
<Computer>37L4247F27-25</Computer>
<Security /></System>
<EventData>
<Data>[0] 37L4247F27-25
[1] WIN-D9RGPJQ68G8</Data>
<Binary></Binary></EventData></Event>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Name="EventLog" />
<EventID Qualifiers="32768">6009</EventID>
<Level>4</Level>
:
```

The *System.evtx* log file shows events to Windows and Window services.

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.



8. View the contents of the **Security.evtx** log file by entering the command below.

```
./evtxdump.pl /home/caine/Downloads/Security.evtx | less
```

```
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
<Events>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A
5BA-3E3B0328C30D}" />
<EventID>4608</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12288</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2015-03-25T10:15:35.2488Z" />
<EventRecordID>1</EventRecordID>
<Correlation />
<Execution ProcessID="464" ThreadID="468" />
<Channel>Security</Channel>
<Computer>37L4247F27-25</Computer>
<Security /></System>
<EventData></EventData></Event>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A
:
```

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.

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