**3906ICT/7906ICT Digital Forensics**

**Tutorial 2.1 – Linux Forensic Artifacts**

The aim of this tutorial is to give you some experience with identifying and examining Linux based forensic artefacts. And working with the Linux operating system. There is some expectation that you have some experience using Linux. We will cover some of the topics raised in the Lecture, but there are many more Linux based forensic artefacts that you are open to explore.

Please note that this tutorial is not a step by step guide. The expectations are that if you are not sure of how to do something, you should find out via internet search or by asking your tutor.

# Preliminaries

There are two options for doing the practical component of this tutorial. You can do this tutorial by logging into the Griffith Cyber Range which is an Internet isolated set of virtual machines that has been set up on the Griffith network. The other is to download and install the software on your local PC.

## Set Up Option 1 – Griffith Cyber Range

If you are not on a Griffith University campus need to VPN into the Griffith Network. Details of how to VPN into the Griffith Network can be found here: https://intranet.secure.griffith.edu.au/computing/remote-access/virtual-private-network. Go to the bottom of the page and find the instructions for your device.

Once you have set up your VPN to the Griffith network, you can use your browser to go to the following page: https://cyber.ict.griffith.edu.au/

The credentials for the Griffith Cyber Range Server are:

**Username: sXXXXXXX**

**Password: changeme**

sXXXXXXX is your Griffith username. When you log in for the first time change your password (which you will need to remember). To do this go to your username menu on the top right corner of the web page and select the Settings item. The Settings page will allow you to reset your password. Once you have reset the password, use your new password for subsequent logins. For this tutorial we will be using the Scenic virtual machine. Click on the Scenic link and you will be connected to a virtual machine running an Ubuntu server Linux distribution.

When you have finished your tutorial simply close the browser tab with the connection to the virtual machine. Or press Shift-Ctrl-Alt to access the web menu and disconnect from the Griffith Cyber Range.

## Set Up Option 2 – Install on your local PC

The other option is to install the Scenic virtual machine on your local PC. Links to the virtual machine OVA file for download are found on the Learning@Griffith web site. **Note:** The Scenic workstation is a 4GB download. You will need to install VirtualBox and select File->Import Appliance to install the Scenic Virtual machine. Start the Virtual Machine and log in.

The login credentials for the Scenic Virtual Machine are:

**Username: user**

**Password: password**

# Linux System

Linux systems have a lot of information about the operating system that they run. Unfortunately, unlike Windows operating systems, Linux systems do not always have a graphical user interface and instead are access through a command line interface. It is useful to be familiar with the commands that you will use to find basic system information.

1. What version of Linux is running on this virtual machine?
2. How can you find this out without looking at the login screen?
3. What is the host name of the virtual machine?
4. How can you find this out without looking at the login screen or prompt?
5. How many network interfaces does the machine have?
6. What is the IP address for this machine?
7. How much disk space has been used and how much free space is available on each disk partition?

**Answer**

**Version**

Version of Linux: Ubuntu 11.10 (GNU/Linux 3.0.0-12-generic-pae i686)

user@scenic:~$ uname -a

Linux scenic 3.0.0-12-generic-pae #20-Ubuntu SMP Fri Oct 7 16:37:17 UTC 2011 i686 i686 i386 GNU/Linux

Other Commands:

lsb -a

cat /proc/version

**Hostname**

Hostname: “scenic”

Other Commands:

hostname

**IP Address**:

Eth0: 172.25.36.3/24

Eth1: 192.168.246.2/24

Command: ip a

**Disk Space**

user@scenic:~$ df -h

Filesystem Size Used Avail Use% Mounted on

/dev/mapper/scenic-root

2.7G 2.1G 466M 83% /

udev 494M 4.0K 494M 1% /dev

tmpfs 201M 256K 201M 1% /run

none 5.0M 0 5.0M 0% /run/lock

none 501M 0 501M 0% /run/shm

/dev/sda1 228M 23M 193M 11% /boot

# Users

Linux systems have traditionally been servers that allow multiple users. It is useful to be able to find information on the types of users allowed on the system.

1. How do you run a command with elevated privileges?
2. Which users can log in to the system?

**Elevated Priveledges:**

Sudo <command>

**Users that can login**

Root

User

Carrot

Vimes

user@scenic:~$ sudo cat /etc/shadow

root:$6$Q.5shfrW$oiq.lAlJCbYzd1ZxZPlZMsXytY3o.f3t96xJB8IYawoxohddwl4EPGI9z7rgKsuKyYlEHSVFlSFbmgmkQWiF3/:18826:0:99999:7:::

daemon:\*:16965:0:99999:7:::

bin:\*:16965:0:99999:7:::

sys:\*:16965:0:99999:7:::

sync:\*:16965:0:99999:7:::

games:\*:16965:0:99999:7:::

man:\*:16965:0:99999:7:::

lp:\*:16965:0:99999:7:::

mail:\*:16965:0:99999:7:::

news:\*:16965:0:99999:7:::

uucp:\*:16965:0:99999:7:::

proxy:\*:16965:0:99999:7:::

www-data:\*:16965:0:99999:7:::

backup:\*:16965:0:99999:7:::

list:\*:16965:0:99999:7:::

irc:\*:16965:0:99999:7:::

gnats:\*:16965:0:99999:7:::

nobody:\*:16965:0:99999:7:::

libuuid:!:16965:0:99999:7:::

syslog:\*:16965:0:99999:7:::

messagebus:\*:16965:0:99999:7:::

landscape:\*:16965:0:99999:7:::

sshd:\*:16965:0:99999:7:::

user:$6$cMEgevD/$GuO/OWa6AMkyf/CqIOFomAYOdDDCyDIPQmxz/i83nqWz1U67y4cdd8kFsyu3A5w7cO8C0GIvpzK3lSNSzDx231:18093:0:99999:7:::

mysql:!:16965:0:99999:7:::

varnish:!:16965::::::

Carrot:$6$plEPzyxW$ZthFFgpQ0OVfhClNNVQ6L4Rncmlvh3.4/eUBI7eR77viHw9bsv4tKGEkIf0ZdExPh4.cNq4bDJ4cGqZ7WvhMW.:16965:0:99999:7:::

Vimes:$6$YD150zgn$vvliXJ4EaOLWQRcLODzh9m86sP8PskohF645RmM2cg4aoQtDGRJyQ78xr1FykHr7vB6y/2fedCbu4mvaB./kM1:16965:0:99999:7:::

snort:\*:17114:0:99999:7:::

user@scenic:~$

# Scheduled Tasks

Tasks can be automatically scheduled. It is useful to determine what regular activities are scheduled to run.

1. List and describe the scheduled tasks.
2. What services are automatically started?

**Answer**

The function bin/date will run every second hour on the 1st and 15th of the month

user@scenic:~$ cd /var/spool/cron

user@scenic:/var/spool/cron$ crontab -l

no crontab for user

user@scenic:/var/spool/cron$ sudo crontab -l

0 \*/2 1,15 \* \* /bin/date >> /tmp/cron-out

user@scenic:/var/spool/cron$

user@scenic:~$ cd /etc

user@scenic:/etc$ ls -a grep rc\*

ls: cannot access grep: No such file or directory

rc.local

rc0.d:

. .. K09apache2 K20snort K38open-vm-tools README S20sendsigs S30urandom S31umountnfs.sh S35networking S40umountfs S60umountroot S90halt

rc1.d:

. .. K09apache2 K20snort K38open-vm-tools README S30killprocs S70dns-clean S70pppd-dns S90single

rc2.d:

. .. README S20snort S38open-vm-tools S50rsync S70dns-clean S70pppd-dns S75sudo S91apache2 S99grub-common S99ondemand S99rc.local

rc3.d:

. .. README S20snort S38open-vm-tools S50rsync S70dns-clean S70pppd-dns S75sudo S91apache2 S99grub-common S99ondemand S99rc.local

rc4.d:

. .. README S20snort S38open-vm-tools S50rsync S70dns-clean S70pppd-dns S75sudo S91apache2 S99grub-common S99ondemand S99rc.local

rc5.d:

. .. README S20snort S38open-vm-tools S50rsync S70dns-clean S70pppd-dns S75sudo S91apache2 S99grub-common S99ondemand S99rc.local

rc6.d:

. .. K09apache2 K20snort K38open-vm-tools README S20sendsigs S30urandom S31umountnfs.sh S35networking S40umountfs S60umountroot S90reboot

rcS.d:

. .. README S37apparmor S55urandom S70x11-common

user@scenic:/etc$

the main services that run are apache2,snort,open-vm-tools

# Services

Linux Servers are mainly used for the services they provide. It is useful to know how to find information on running services.

1. What services are running on the machine?
2. What port numbers are being used by these services?
3. What do each of the main services with open ports do?
4. Run the top command for fun. What are the most memory intensive processes?

**Answer**

**Services running**

sudo service --status-all | less

* Not running

+. Running

? Autonmatically running in the background

**Port numbers used**

user@scenic:/etc$ netstat -a

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address Foreign Address State

tcp 0 0 \*:www \*:\* LISTEN

tcp 0 0 \*:ssh \*:\* LISTEN

ctcp 0 0 172.25.36.3:ssh 172.25.36.254:54038 ESTABLISHED

tcp6 0 0 [::]:mysql [::]:\* LISTEN

tcp6 0 0 [::]:ssh [::]:\* LISTEN

Active UNIX domain sockets (servers and established)

Proto RefCnt Flags Type State I-Node Path

unix 2 [ ACC ] STREAM LISTENING 7175 /var/run/dbus/system\_bus\_socket

unix 2 [ ACC ] STREAM LISTENING 6193 @/com/ubuntu/upstart

unix 5 [ ] DGRAM 7266 /dev/log

unix 2 [ ACC ] SEQPACKET LISTENING 6313 @/org/kernel/udev/udevd

unix 2 [ ACC ] STREAM LISTENING 9023 /opt/wordpress-4.5.2-0/mysql/tmp/mysql.sock

unix 3 [ ] STREAM CONNECTED 134956

unix 3 [ ] STREAM CONNECTED 134955

unix 2 [ ] DGRAM 134873

unix 2 [ ] DGRAM 13077

unix 2 [ ] DGRAM 9056

unix 3 [ ] STREAM CONNECTED 7192 /var/run/dbus/system\_bus\_socket

unix 3 [ ] STREAM CONNECTED 7191

unix 3 [ ] STREAM CONNECTED 7182

unix 3 [ ] STREAM CONNECTED 7181

unix 3 [ ] STREAM CONNECTED 6897 @/com/ubuntu/upstart

unix 3 [ ] STREAM CONNECTED 6892

unix 3 [ ] DGRAM 6354

unix 3 [ ] DGRAM 6353

unix 3 [ ] STREAM CONNECTED 6301 @/com/ubuntu/upstart

unix 3 [ ] STREAM CONNECTED 6295

user@scenic:/etc$

**Port numbers**

ports 80,22,3306 are used

command netstat -an

**Main services on open ports:**

www,ssh,mysql & ssh

**Most memory Intensive process:**

Ssh,vm-tools,init

# Processes

Each service may have one or more processes. It is useful to know how to find information on running processes.

1. What processes are associated with the running services?

**Answer**

ps aux

root 1049 0.0 0.3 32868 3908 ? Sl Jul17 24:58 /usr/bin/vmtoolsd

also ps -ef

1. What is the path to the executable for the web servers?

**Answer**

Path is shown at the end of each line e.g “/usr/bin/vmtoolsd”

# Service Logs

Logs associated with Linux services. This section is to give you practice at finding important information in Linux logs.

1. Which IP address or host has been accessing the web pages the most on the web servers running on this machine?

**Answer**

cd /var/log

ls

We find apache2 so:

cd apache2

ls -al

vi access.log

sudo gunzip dmesg.1.gz

cat dmesg.1.

OR in /var/log

cd apache2

ls -l

\*see larget size\*

Inside /var/log/apache2

nano access.log

each line is of the log is an event

Most poular IP address is 192.168.246.1

1. Find two common web hacking tools have been used against the web server running on this machine.

**Answer**

Nikto and sqlmap

# Service Configuration Files

All applications have configuration and install files. Web servers have a document web root directory. It is important to be able to identify where this is, especially in non-standard installs.

1. Find the configurations for web servers on this machine.

**Answer**

Sudo su

find / -name httpd.conf

(also try “ls” here)

OR

sudo find / -name httpd.conf

1. Find the last modified WordPress application files.

**Answer**

Sudo su

find opt/wordpress-4.5.2-0/apps/htdocs/ -type f ‘printf ‘%TY-%Tm-%Td %TT %p\n’ | sort -r | less

vi <suspicious file>

reverse shell was used IP is also shown

1. Are there any files that indicate that the machine has been compromised?

**Answer**

The last wordpress file was the one compromised

# User Logs

Like Windows, Linux systems log user logins and activities.

1. Do the login logs match hacking activities?

**Answer**

Last -f /var/log/wtmp

1. Look at the shell history for two other users.

**Answer**

Sudo su

Cd Carrot

Ls -al

Look for .bash\_history

cat .bash history

\*we see they looked at sectret.txt\*

1. Was the attacker able to access the secret.txt file in the root home directory?

**Answer**

Ls /root/

Cat /root/secret.txt

# Tutorial Quiz

You have now completed the exercises for this tutorial. You can now attempt the quiz for this tutorial.