CIS/ECE 387 Fall 2018 Lab1

Assigned: 9/17/2018
Due: **9/26/2018**

FORMAT

You should work in a group of two students (or work individually). Every student needs to sign up for one of the lab groups on canvas **no later than 9/20**.

PREPARATION: LINUX VIRTUAL WORKSTATION

This lab activities take place in a Linux system environment using **SANS SIFT Workstation**, a collection of forensic tools.

Download VirtualBox

Download VirtualBox to run SANS SIFT workstation.

VirtualBox download

Follow the instructions at the website to install the VirtualBox.

Download SANS SIFT Workstation

Download **SANS SIFT Workstation**. You have to create an account to download the free software as a .zip file.

SANS SIFT Workstation download

Download the `SIFT-Workstation.ova` file.

Open and configure VirtualBox

1. Open VirtualBox from “Applications”
2. Click "Important Appliance” under the File menu and select the SANS appliance “`SIFT-Workstation.ova`”

- You may use the suggested settings, just change Name to `SANS_SIFT.`

3. SIFT Workstation will open. You will be prompted for a username and password:

- Default username: **`sansforensics`**

- Default password: **`forensics`**

You can now begin the activities.

ACTIVITY 1: PRACTICING LINUX/UNIX COMMANDS

GOAL

In this activity, you will practice a set of basic Linux/Unix commands commonly used by an incident responder to identify security breaches from a live suspect system, as if you were examining a suspect machine that has not been shut down.

INSTRUCTIONS

1. Launch SIFT Workstation 3. The default login username is ***sansforensics***, and the default password is ***forensics***
2. Open a terminal and listen to the port 8888 by running: *nc –l 8888 &* .
3. Use command's man page (for example, man ifconfig) to check each command's description and its main options before you practice the command.
4. Practice each command to understand how you can use the result for your investigation.

To display	Command
current system date and time	date
when was the system rebooted	uptime -p
system information	uname –a
whether a network interface is running in a promiscuous mode	ifconfig
unusual and suspicious processes and services	ps –eaf
network connections	netstat lsof -i
Open in memory, but unlinked files (requested for deletion)	lsof +L1
files opened by the process PID	lsof –p (PID)

Currently logged in users (three options)	w who users
all root-owned (uid=0) SUID files.	find / -uid 0 –perm -4000 –print
logged general system activities	tail –f /var/log/messages
a list of all users with last logged in (and logged out) times stored in the log file /var/log/wtmp	last
any regular files in /directory_path that has been modified within 1 day (24 hours)	find /directory_path –type f –mtime -1 -print
free disk space	df
amount of free and used physical and swap memory in system	free

ACTIVITY 2: LINUX MEMORY ACQUISITION

GOAL

In this activity, you will learn how to use LiME (Linux Memory Extractor) to acquire a complete Linux physical memory dump.

Download LiME Module

Download (using Firefox in your VM) the open LiME source code and save it on your virtual machine.

Linux Memory Extractor (LiME), A Loadable Kernel Module for acquiring Linux/Android physical memory.

Enter the “src” folder and type “make” to compile the module. Alternatively, you can download the compiled module on canvas under the `Files->Labs-Lab1` folder.

INSTRUCTIONS

1. Insert the kernel module ang get a memory dump

- `sudo insmod lime-4.4.0-97-generic.ko “path=./mem_dump.bin format=padded”`

2. Search the memory dump file for the strings starting with “forensics” (potential password in the memory).

- `strings -n 8 mem_dump.bin | grep ^forensics`

Report

Your report should include the activity log (the main steps you take or the commands you run) with some screenshots and/or outputs and a brief reflection on what you learned (one or two paragraphs).

Please submit your lab report to Canvas under the “lab1” assignment folder. Each group just submits one report.