REPORTED BY
Gunnar Yonker

LAB NUMBER
1

START DATE
2/3/2023

COMPLETED DATE
2/5/2023

COURSE
CYBER 742

SEMESTER
SPRING 23

INSTRUCTOR
Schoeneck

TYPE OF INVESTIGATION
Forensic Tool Setup

SUSPECT
n/a

LAB REPORT SUMMARY:

Between 2/3/2023 and 2/5/2023, I, Gunnar Yonker, created and configured multiple forensic vitural machine environments on my digital forensics workstation, a custom built desktop computer further described as follows:

Manufacturer: Custom PC(Corsair, AMD, TUF GAMING, NVIDIA)
Model: TUF GAMING X570-PRO, NVIDIA GeForce RTX 3080, AMD Ryzen 5 5600x 6-Core Processor, Corsair Vengence RAM
Serial Number: TUF GAMING X570-PRO: 200974475901766
NVIDIA GeForce RTX 3080: 1324420027508
No serial number for custom built PC as a whole
Host OS: Windows 10
Processor: AMD Ryzen 5 5600x 6-Core Processor
Storage Type: Sabrent Rocket Q NvMe PCIe M.2 2280 SSD 1000GB
RAM (GB): 16GB Corsair Vengence

I utilized Virtual Box (Version number 6.1)
to create and configure the following Virtual Machines (VM) as detailed below:

Windows
OS Type/Version: Windows 10 Home
Storage File Type: NTFS
Storage Size: 50GB
Memory (RAM): 8GB
Forensic Tools Installed: Autopsy ver 4.20, FTK Imager ver 4.7, Kroll Artifact Parser and Extractor ver 0.9.2.0, Magnet RAM Capture ver 1.0.4.0, HxD Hex Editor ver 2.5.0.0

I created a Windows VM using the Windows 10 iso file from Microsoft on the VirtualBox platform. The VM has 50GB of storage, 8GB of RAM, CPU usage of 3, and has the following forensics tools: Autopsy, FTK Imager, Kroll Artifact Parser and Extractor, Magnet RAM Capture, and HxD Hex Editor. There has been no futhter customization of the VM than the previously mentioned programs.

REPORTED BY
Gunnar Yonker
0

LAB NUMBER
1

SUMMARY CONTINUED:

Linux
OS Type/Version: Ubuntu 22.04.1
Storage File Type: OpenZFS
Storage Size: 50GB
Memory (RAM): 4GB
Forensic Tools Installed: Autopsy ver 4.20, The Sleuth Kit ver 4.12.0, Volatility ver 2.6

I created a VM running the Ubuntu 22.0.4.1 iso file on the VirtualBox platform. The VM has 50GB of storage and 4GB of RAM. The following forensic tools are installed: Autopsy, The Sleuth Kit, and Volatility. No additional forensics tools were installed and no further customizations were applied.

REPORTED BY
Gunnar Yonker
0

LAB NUMBER
1

START DATE
2/3/2023

COMPLETED DATE
2/5/2023

SUBMITTING AGENCY
CYBER 742

SEMESTER
SPRING 23

INSTRUCTOR
Schoeneck

0

TYPE OF INVESTIGATION
Forensic Tool Setup

SUSPECT
n/a

SUPPLEMENTAL INFORMATION:

Linux Familiarization Answers:

1) cd /home/[user]/cyber742/project1/src
-[user] would be replaced with user name,

2) Highest level directory: / which is the root directory
Lowest level directory: src
main.c is most likely a C/C++ source code file not a directory

3) sudo rm -rf / will remove all files in the root directory, sudo allows this command to run as superuser, -rf removes all files and directories without any confirmation.

4) man ls
To advance to the next page you press the "SPACE" key, to exit you press "q".
-a: Shows hidden files and directories
-l: shows details in long format
-h: shows file sizes in human-readable format
-R: recursive list the contents of all subdirectories
-t: sort the contents by modification time with newest listed first.

5) wc -c myfile.txt > myfile_char_count.txt
wc: counts the number of characters with the -c option for only the number of characters
output is redirect by > to myfile_char_count.txt

6) ls -a ~
ls -a shows the hidden files, any that also start in a period. The ~ is used for the home directory instead of an explicit path.

7) mv data.txt ~/experiment1/
mv will move the file to the destination given which is the experiment1 directory located in the home directory.
8) ls -laS /etc
-l shows the files in long format, -a shows the hidden files and directories, -S sorts the contents by file size largest to smallest.

9) wget http://www.google.com/doodles/roswells-66th-anniversary
wget downloads the files and saves it into the current directory with the original file name.

10) pwd
pwd will print out the directory that you are currently in, in my case it was "/home/gunnar".

11) ls -lh /boot
ls lists the contents of the directory, -lh shows contents in long form and the file sizes in human-readable units in the given directory /boot

REPORTED BY
Gunnar Yonker
0

LAB NUMBER
1

SUPPLEMENTAL CONTINUED:

12) df -h
df will report the disk space usage, -h shows the sizes in human-readable units.

13) The Linux kernal is the core of the system, it is the interface between the hardware and software running on the system. It manages system resources like CPU, time, memory, and provides services for the system/applications. It is open source and can be viewed, used and modified.

14) The Linux kernal is the core that provides functionality and services to the system. Ubuntu Linux is an operating system itself that includes the Linux kernal as well as other software such as a user interface, applications and libraries. Ubuntu Linux is a "flavor" of Linux that has a specific look and is one of many distributions of the Linux operating system.

15) A Virtual Machine allows you to emulate a computer system which is operating on your host system. It allows the user to run an isolated environment for multiple different operating systems such as running Windows or Ubuntu Linux. A host system can also run multiple VMs at a time if there are enough resources and can allow a user to run multiple tests in isolated settings and securely. They can be used for situations such as software development, testing, ethical hacking practice, and computer forensics practice using forensic tools.

16) Dual booting is when there are multiple operating systems installed on a single computer system and choosing upon boot which operating system to boot. A virtual machine runs an operating system on the host system and can have multiple different operation systems running simultaneously on the same physical hardware. A dual boot can only have one operating system controlling the full system at a time, whereas a virtual machine uses virtual hardware and can run multiple isolated operating systems.

17) Besides inflicting pain on newbies, the command line is a very powerful tool to control a computer. It is a very fast and effecient way to perform many tasks such as creating or copying files which only requires a simple command. Another advantage is that the command line allows for access to the core functionality of the system, such as performing complex low-level operations and allowing for overall greater control of the system. This is incredibly useful for system administrators and developers. Another fantastic aspect is the ability to create and store scripts using the command line that can then be set up to carry out tasks at given intervals of time becoming completely automous once set up.

18) The one dot (.) in a file path represents the current directory, so when it is used it means that the file being refrenced is the one in the current directory. Two dots (..) represents the parent directory and can be used to navigate up to the parent directory without typing the parent directory name. This can be done with "cd .." moving from subdirectory to parent