ENPM687 – Digital Forensics and Incidence Responses

Assignment – 4

Author – Syed Mohammad Ibrahim

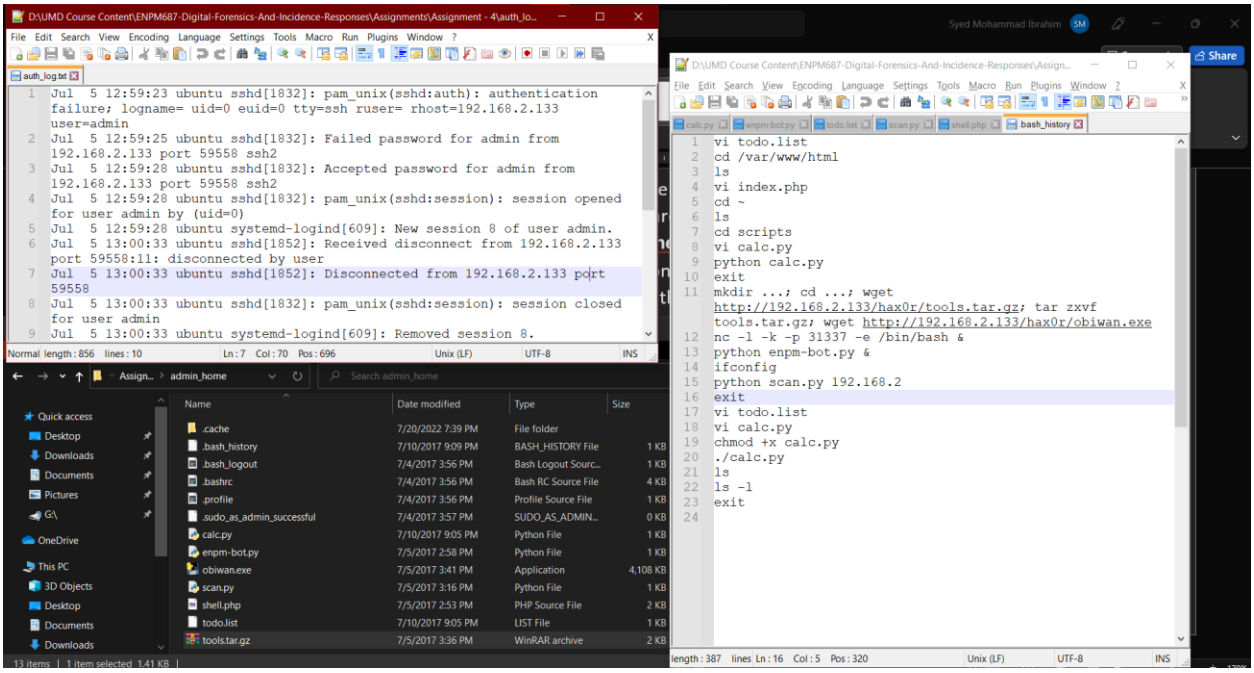
UMD ID: iamibi

UID: 118428369

Email: iamibi@umd.edu

Part – 1 – Attack Narrative

- I downloaded the log file and directory content tar file from the given location.
- First, after examining the **auth_log.txt** file, it seemed that the attacker tried to ssh into the system as an **admin** user but failed the first time. However, the next try was a success and the attacker had complete privileges. The compromised system's IP address was **192.168.2.133**.
- The successful login incident was recorded around **July 5, 12:59:28**.
- Next, I examined the files present in the home directory of the compromised admin user. The first place to look for was the **.bash_history** file which contained the list of commands that were executed on the system.
- The attacker first created a todo.list file which may have been the stuff that the attacker was trying to perform.
- The attacker proceeds to access the index.html which is the webpage entry and potentially may have added malicious scripts as part of it or retrieved sensitive credentials that may get them into any other server(s) on the network or the database.
- Then the attacker creates a file calc.py which is a python script. The attacker updates the file and runs the script and then modify the file again to make it look like an unharmful simple script.
- In between changing the contents of the file, the attacker then fetched two more files – a tar file and a binary which is highly likely to be a malware called **obiwan.exe**. The tar file contained three files, namely **enpm-bot.py**, **scan.py** and **shell.php**.
- After this, the attacker opens a netcat listener on the system on port 31337 with a shell access, potentially trying to get the machine shell from their remote location. This was run in the background and in parallel with enpm-bot.py which I believe was checking network connectivity with a 2 second sleep time.
- The scan.py is run to enumerate the network within the current IP range and check for any open SSH port within the network.
- Then the attacker updates the todo.list and calc.py and exits the current session.



Part – 2 – File Analysis

1. What files do you find?

A. I found two files that were recovered by the foremost. They were jpg files.

2. What are the contents of the files?

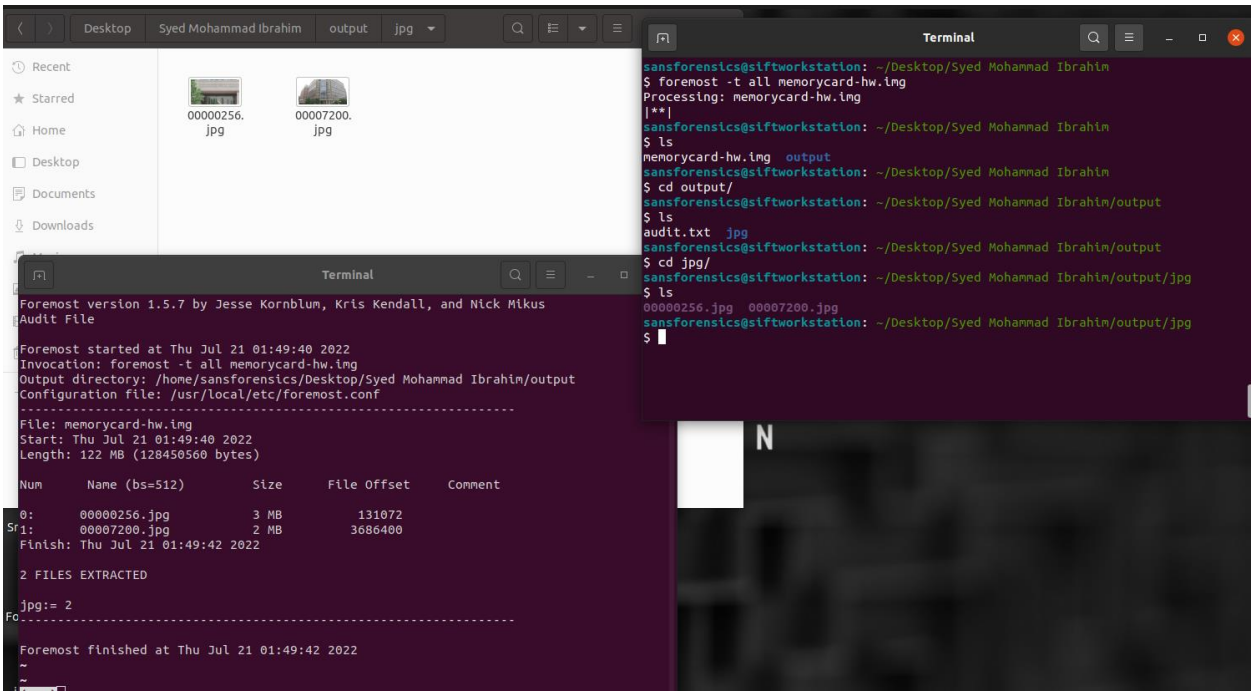
A. Both the images seem to be of a place called National Science Foundation. The picture's meta-data reported that they were taken from Canon PowerShot SX260 HS camera model in 2013:06:02 15:42:33 and 2013:06:02 15:42:47.

3. What command or tool did you use to find the files? (Give lots of detail)

A. I used the foremost tool to extract the data from the given image file. The command I used was "foremost -t all memorycard-hw.img". The "-t" flag points to what type of file the foremost is expecting and the "all" parameter is the type which includes all the file types that are non-standard to foremost program. The ".img" files are non-standard and thus need to be used with the "all" flag.

4. Provide a screenshot of your command/tool usage with your name on the command line and in original context (ex. working from a FolderName that is your name)

A.


Desktop
Syed Mohammad Ibrahim
output
jpg
Recent
Starred
Home
Desktop
Documents
Downloads
00000256.jpg
00007200.jpg
Terminal
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Thu Jul 21 01:49:40 2022
Invocation: foremost -t all memorycard-hw.img
Output directory: /home/sansforensics/Desktop/Syed Mohammad Ibrahim/output
Configuration file: /usr/local/etc/foremost.conf
File: memorycard-hw.img
Start: Thu Jul 21 01:49:40 2022
Length: 122 MB (128450560 bytes)
Num Name (bs=512) Size File Offset Comment
0: 00000256.jpg 3 MB 131072
1: 00007200.jpg 2 MB 3686400
Finish: Thu Jul 21 01:49:42 2022
2 FILES EXTRACTED
jpg:= 2
Foremost finished at Thu Jul 21 01:49:42 2022
Terminal
sansforensics@siftworkstation: ~/Desktop/Syed Mohammad Ibrahim
$ foremost -t all memorycard-hw.img
Processing: memorycard-hw.img
|**|
sansforensics@siftworkstation: ~/Desktop/Syed Mohammad Ibrahim
$ ls
memorycard-hw.img output
sansforensics@siftworkstation: ~/Desktop/Syed Mohammad Ibrahim
$ cd output/
sansforensics@siftworkstation: ~/Desktop/Syed Mohammad Ibrahim/output
$ ls
audit.txt jpg
sansforensics@siftworkstation: ~/Desktop/Syed Mohammad Ibrahim/output
$ cd jpg/
sansforensics@siftworkstation: ~/Desktop/Syed Mohammad Ibrahim/output/jpg
$ ls
00000256.jpg 00007200.jpg
sansforensics@siftworkstation: ~/Desktop/Syed Mohammad Ibrahim/output/jpg
$