Lab Assignment

Cybersecurity Professional Program

Digital Forensics & Incident Response

Linux Forensics

DFIR-08-L2

Server Investigation

Lab Objective

Get hands-on experience with forensic investigation methods learned during the lesson.

Lab Mission

Investigate the server image and identify deleted and modified files.

Lab Duration

15–20 minutes

Requirements

- Working knowledge of the Linux environment
- Basic understanding of the Linux file system structure
- Basic knowledge of Bash scripting

Resources

- VirtualBox that includes NAT Network of:
  - Windows 10
    - ***putty-64bit-0.74-installer***
    - ***pscp.exe***
  - SIFT Workstation (password: **forensics**)
- Extra Lab Files
  - ***DFIR-08-L2 Hacked.rar***

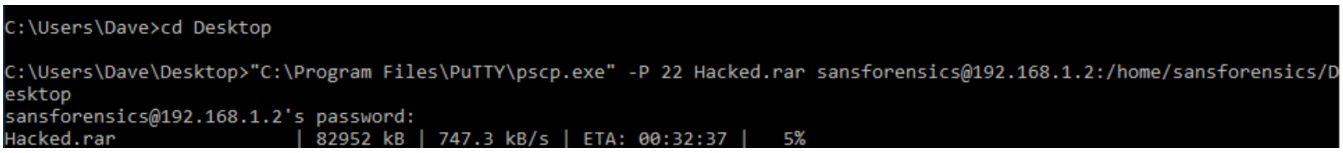
Textbook References

- Chapter 8: Linux Forensics
  - Section 3: Linux File Systems
  - Section 4: File System Analysis

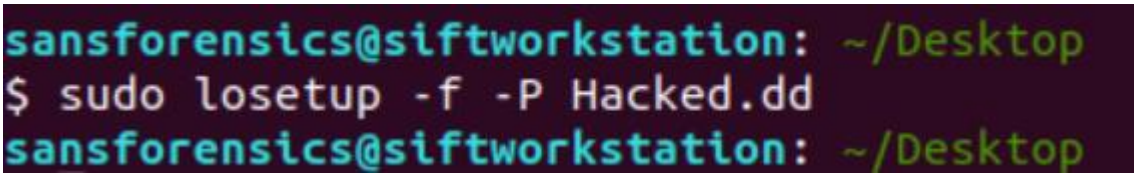
Lab Task: Investigate a Server Image and Identify Deleted and Modified Files

Investigate the server image and identify deleted and modified files.

1. Move the ***DFIR-08-L2 Hacked.rar*** file to Windows 10 and rename the file to ***Hacked.rar*.**
2. Start the SSH service on SIFT with ***sudo service ssh start***.
3. Transfer the file ***Hacked.rar*** to the SIFT workstation with the help of the Windows 10 machine and ***pscp.exe.*** Unzip the file in SIFT. Use the command ***"C:\Program Files\PuTTY\pscp.exe" -P 22 [Filename] sansforensics@[IP]:/home/sansforensics/Desktop***.



4. Unzip the ***Hacked.rar*** file with the command ***unrar x Hacked.rar***.
5. Use the ***losetup*** commands to mount the ***Hacked.dd*** image. First, use ***losetup --help*** to see the options. Then, use the ***sudo losetup -f -P Hacked.dd*** to set up a loop device. After, you will list the ***losetup*** with ***sudo losetup -l***.



6. Use the ***mount*** command. First, create a directory for the ***mnt*** with ***mkdir /mnt/dd***. Then, use ***sudo mount -o loop,ro,noload /dev/loopXXp1 /mnt/dd*** to mount the file. Go to ***/mnt/dd*** directory and list the disk image.

7 Inspect the content of the web server and note the creation dates of files and folders. Use the command ***sudo ls -lah /mnt/dd/var/www/html/wordpress***.

```
sansforensics@siftworkstation: ~/Desktop
$ sudo ls -lah /mnt/dd/var/www/html/wordpress/
total 224K
drwxr-x---  5 www-data www-data 4.0K Jan 16  2020 .
drwxr-xr-x  3 root     root     4.0K Jan 16  2020 ..
-rw-r--r--  1 www-data www-data  481 Jan 16  2020 .htaccess
-rw-r--r--  1 root     root      926 Jan 16  2020 index.html
-rw-r-----  1 www-data www-data  20K Jan  1  2019 license.txt
-rw-r-----  1 www-data www-data 7.2K Sep  2  2019 readme.html
-rw-r--r--  1 root     root     2.0K Jan 16  2020 style.css
-rw-r-----  1 www-data www-data 6.8K Sep  3  2019 wp-activate.php
drwxr-x---  9 www-data www-data 4.0K Dec 18  2019 wp-admin
-rw-r-----  1 www-data www-data  369 Nov 30  2017 wp-blog-header.php
-rw-r-----  1 www-data www-data 2.3K Jan 21  2019 wp-comments-post.php
-rw-r-----  1 www-data www-data 2.9K Jan 16  2020 wp-config.php
drwxr-x---  5 www-data www-data 4.0K Jan 16  2020 wp-content
-rw-r-----  1 www-data www-data 3.9K Oct 10  2019 wp-cron.php
drwxr-x--- 20 www-data www-data  12K Dec 18  2019 wp-includes
-rw-r-----  1 www-data www-data 2.5K Sep  3  2019 wp-links-opml.php
```

8 Check the logs for malicious web traffic with ***ls -lah /mnt/dd/var/logs***. List out the Apache2 log files. List out the ***access.log*** and ***grep*** with ***DO_NOT_EXIST***. Note the attempts to execute a reverse shell.

9 Perform a manual check for deleted inodes with the use of ***ils -f ext4 -o 2048 Hacked.dd***. Inspect inode 22416 with the command ***istat -f ext4 -o 2048 Hacked.dd 22416***.

```
sansforensics@siftworkstation: ~/Desktop
$ ils -f ext4 -o 2048 Hacked.dd
class|host|device|start_time
ils|siftworkstation||1616168461
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_crtime|st_mode|st_nlink|st_size
22345|f|0|0|1579169605|1579169605|1579169605|1579169605|755|0|0
22353|f|0|0|1579168209|1579168205|1579168209|1579168203|644|0|0
22354|f|0|0|1579168209|1579168203|1579168209|1579168203|755|0|0
22355|f|0|0|1579168209|1579168204|1579168209|1579168203|644|0|0
22356|f|0|0|1579168209|1579168205|1579168209|1579168203|644|0|0
22357|f|0|0|1579168209|1579168205|1579168209|1579168203|644|0|0
22358|f|0|0|1579168209|1579168204|1579168209|1579168203|644|0|0
22359|f|0|0|1579168209|1579168205|1579168209|1579168203|644|0|0
22360|f|0|0|1579168209|1579168203|1579168209|1579168203|755|0|0
22361|f|0|0|1579168209|1579168204|1579168209|1579168203|644|0|0
22362|f|0|0|1579168209|1579168205|1579168209|1579168203|644|0|0
22363|f|0|0|1579168209|1579168205|1579168209|1579168203|644|0|0
22364|f|0|0|1579168209|1579168205|1579168209|1579168203|644|0|0
22365|f|0|0|1579168209|1579168203|1579168209|1579168203|755|0|0
22366|f|0|0|1579168209|1579168205|1579168209|1579168203|644|0|0
22367|f|0|0|1579168209|1579168205|1579168209|1579168203|644|0|0
22368|f|0|0|1579168209|1579168205|1579168209|1579168203|644|0|0
```

10 Use this Bash script to inspect the file names: ***for inode in $(ils -f ext4 -o 2048 Hacked.dd | awk -F"|" '{print $1}'); do ffind -f ext4 -o 2048 Hacked.dd $inode; done.***

Note: The script will run showing the file names.

11 Check if there were any recent modifications to the file system by running ***jls -f ext4 -o 2048 Hacked.dd | grep -v unallocated***. Then, inspect the journal entries with ***for j in $(jls -f ext4 -o 2048 Hacked.dd | grep -v Unallocated | awk -F: '{print $1}'); do jcat -f ext4 -o 2048 Hacked.dd $j | strings; echo -e "\n---------$j----------\n"; done***.

Note: the script loops and extracts the block number of each entry with the content.

12 Identify modified files that are unusual with the listed journal entries from step 11, starting from entry number 4008 and going to 4173. Search for server files.

13 Search for the ***cron*** entry in the listed journal blocks. Once found, verify that there are no cronjobs; from the terminal, run ***gedit /mnt/dd/etc/crontab***.

Hints

- It is recommended to shut down the NAT NIC before using SSH on the internal network.
- Use the ***sudo ip link set enp0sXX*** down/up to turn on/off the network interface card in SIFT.
- To enable SSH, execute ***service ssh start*** (SSH was introduced in NET-02).
- The SSH default port is 22.
- Use ***"C:\Program Files\PuTTY\pscp.exe" -P [port] [file] [username]@[IP]:/[path to save]*** to transfer a file.
- To extract the content of the RAR file, use the **unrar** tool.
- Set the ***dd*** file as a loop device to mount it later with ***sudo losetup*** (Chapter 8).
- Create a mounting point before trying to mount the device with ***mkdir***.
- Use this command if the command from the book does not work: ***sudo mount -o loop,ro,noload /dev/[loopXXp1] /mnt/[directoryname]***.
- Apache's logs should be checked for malicious traffic.
- Search for the logs at the end of the log files with ***cmd***.
- The command ***ils*** can be used to check for deleted nodes (DFIR-08).
- The command ***istat -f ext4 -o 2048 Hacked.dd [inode]*** can be used to check inode numbers (DFIR-08).
- The script ***for inode in $(ils -f ext4 -o 2048 Hacked.dd | awk -F"|" '{print $1}'); do ffind -f ext4 -o 2048 Hacked.dd $inode; done;*** can be used to view file names.
- The **jls** tool can be used to find allocated blocks (DFIR-08).
- The script ***for j in $(jls -f ext4 -o 2048 Hacked.dd | grep -v Unallocated | awk -F: '{print $1}'); do jcat -f ext4 -o 2048 Hacked.dd $j | strings; echo -e "\n---------$j---------\n"; done*** can be used to inspect journal entries.
- The root directory of the web server files is ***var/www/html/***.
- The scheduled tasks can be found at ***/etc/crontab***.