Linux RAM capture instructions

1 Check system settings (on target system)

IMPORTANT NOTE: due to the complexity of memory acquisition on Linux systems, this guide considers only best-case scenario, a target system running a 64-bit version of Linux, with /proc/kcore enabled. This kernel device, which allows access to memory, is enabled by default on modern Linux distributions.

For other scenarios, please get in contact with IRIS to get a customized set of instructions.

To check if these conditions are met:

1. Connect to target machine
2. Open terminal
3. Run command

   ```
   $ uname –m
   ```

   if output is

   ```
   x86_64
   ```

   the system is a 64-bit one
4. Run command

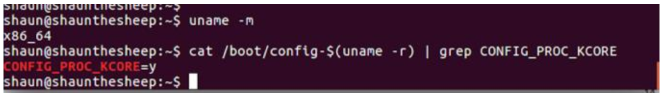
   ```
   $ cat /boot/config-`uname -r` | grep
   CONFIG_PROC_KCORE
   ```

   if output is

   ```
   CONFIG_PROC_KCORE=y
   ```

   the system has device Proc Kcore enabled.

   An example can be seen below



```
shaun@shaunthesheep:~$
shaun@shaunthesheep:~$ uname -m
x86_64
shaun@shaunthesheep:~$ cat /boot/config-$(uname -r) | grep CONFIG_PROC_KCORE
CONFIG_PROC_KCORE=y
shaun@shaunthesheep:~$
```

If above conditions are met, proceed with the following steps of this instruction. Otherwise reach out to IBM X-Force IRIS consultant for guidance.

2 Preparation (on standalone machine)

2.1 Download Linpmem

The PMEM suite is a collection of acquisition tools created by Google. It consists of utilities that can be used to acquire memory dumps on all major Operating systems. For Linux, the linpmem tool is available as an already compiled 64-bit executable. It can be obtained from official c-aff4 Releases website: https://github.com/Velocidex/c-aff4/releases. The latest version at the time of writing this guide is **linpmem-v3.3-rc3.3-rc2**, however please check if a newer version is available.

2.2 Prepare storage media

1. Find removable storage media:
   a. ensure that the its capacity is <u>larger</u> (not equal) that amount of RAM memory of target machine,
   b. it will be formatted and data <u>may be irrecoverably lost!</u>
2. Format the media using ext3 or ext4 filesystem.
3. Copy previously downloaded Linpmem onto the media.

3 Information capture (on target machine)

It is **<u>required is to have administrative rights on the machine</u>**.

1. Connect previously prepared removable media.
2. Open a terminal
3. Gain root rights and change directory to removable media containing Linpmem
4. Launch Linpmem tool with command:

   ```
   # ./linpmem-2.1.post4 -c snappy -o
   ./<HOSTNAME>.aff4
   ```

5. **<u>IMPORTANT:</u>** <u>Do not store RAM image file on any internal storage of target system, always create it on removable media. If necessary, adjust output path after “–o” option</u>
6. When completed, close terminal and safely disconnect media from the system.

4 Preparation for delivery to IBM X-Force IRIS team (on standalone machine)

4.1 Connect removable media to a Linux workstation

If the storage media is a USB drive, it is possible, that it has become infected. To limit chance of spreading potential infection, this stage should be performed with some care. Specifically:

1. autorun feature for removable media should be disabled,
2. system should be fully updated,
3. antivirus scan of a media with updated signature set should be performed.

4.2 Calculate hash value

To calculate hash values on Linux machine, launch shell (most probably bash) and calculate checksums of a file using following commands, redirecting output to the file:

```
$ md5sum ram_image_file >>
memory_image_checksum.txt
```

```
$ sha1sum ram_image_file >>
memory_image_checksum.txt
```

4.3 Verify Hash output

Check whether output file contains information about calculated hash values. If everything is fine, place the output file memory_image_checksum.txt in the same location as the memory image.

4.4 Compress and encrypt

1. Copy memory_image_checksum.txt to the same location where RAM capture is.
2. Preferably use 7-zip as compression and security are better than other tools. Run the command

   ```
   $ 7z a -p <name of compressed file>.7z
   </path/to/Folder to compress>
   ```

3. you will be asked for a password to set. Choose a complex password (16 characters, mixed case letters, numbers, and special symbols)
4. Test the archive with the command

   ```
   $ 7z t <name of compressed file>.7z
   ```

5. If archive testing was successful, encryption was successful. Original file should be securely wiped, using your organization approved method.

4.5 Delivering file to IRIS

1. Compressed archive and text file are ready for delivery to IBM X-Force IRIS team via agreed method of delivery.
2. Share complex password used to for encryption with IBM X-Force IRIS team using different communication channel then used to share forensic image.