**My progress on the topic :**

**(The memory study file has the basic information about how files and processes are structured in Windows and Linux environments. If you want you can go through that. After searching the internet I found out that the below mentioned tools are the most used and useful for linux environments. Also there are links to detailed workshops on Linux Memory Analysis. These are practical workshops! Tomorrow as soon as I am free I will start going through these workshops and hopefully by tuesday I will have some concrete results. Tuesday is on 26th Nov. If everything goes as planned I will still have 3 days to build up on the results. )**

**Tools :**

**Memdmp**

**Lime**

**Volatility**

**Linux Memory Analysis**

<https://www.jamesbower.com/linux-memory-analysis/> (Lime and Volatility)

<https://tunnelix.com/linux-memory-analysis-with-lime-and-volatility/> (Lime and Volatility)

<http://dfir.org/research/omfw.pdf> (Linux Memory Analysis With Volatility)

<https://media.blackhat.com/bh-us-11/Case/BH_US_11_Case_Linux_Slides.pdf> (Linux Memory Analysis Workshop)

**Command usage**

Gdb - attach pid - find start addr, end addr, string - dump memory /root/op start addr end addr

/proc/pid/maps

Strace

Ptrace

/proc/pid/status

**Lastpass Report**

* **No 2FA for master password. Always stays logged in. Yet to find if there is a risk of data store leakage. (If the process is always open we can easily find the hidden lastpass folder. Because you wont have to worry about dumping the memory and scouring through it. Since the proceess is open the rootkit can transmit the process data in memory at anytime and also the hidden folder.)**
* **Yet to find the password in memory. Probably that means it is nicely hidden. Encyption is as guranteed as it can be seen from the sequence of system calls from strace.**
* **Moving on to understanding the system calls and finding the important call.**
* **Out of process available. (There is a separate process created for lastpass unlike dashlane and keeper) (Yet to identify the significance of it!!)**

**Dashlane Report**

* **2FA before master password login**
* **Doesnt always stay logged in**

**Out of process extensions**

**Advantages -**

**Browser performance improves**

**Disadvantages**

**Increased Ram usage**