This project intends to change how Linux Swap operates so that all swapped out memory pages should be encrypted before being written to disc. Depending on the configuration, the Linux swap area is either a disc partition or a file that houses memory pages for swapped-out operating processes. The issue is that those memory pages can hold crucially private information that belongs to those processes that are currently operating; this information could take the shape of a password, a crucial credential, sensitive personal data, etc. The swap partition can be accessed by an attacker in many different ways; for instance, if the system is wrongly shut down, the attacker can replicate the swap partition offline and begin extracting the data from it.The Rc4 is used as the source code of the simple fast stream cipher RC4 to integrate it within the kernel and hook it into the swap-in and swap-out code.

We found that in order to have an encrypted swap\_out and a decrypted swap\_in we needed to add the following lines in all functions that need to be edited.

Char ek[11]=’thisisatest’🡪 encryption key

Void vaddr =\*kmap\_atomic(page) 🡪 to get the address of the page

Rc4(vaddr,ek, vaddr, Page\_size, 16)🡪 for decryption and encryption

Kunmap\_atomic(page)🡪 release the address stored for the page

First function we noticed that we need to place the encryption in is end\_swap\_write.Its main aim is attempts to write *dlen* bytes from *data* to BIO *b*. If successful then the number of bytes written is stored in *\*written* unless *written* is NULL.

Text

Description automatically generated

Then we looked at the end\_swap\_bio\_read which  attempts to read *len* bytes from BIO *b* and places the data in *buf*. Text

Description automatically generated

Text

Description automatically generated

Then we edited \_swap\_writepage attempts to if we have got stale swap cache pages in memory, they are noticed here and get rid of the unnecessary final write

Text

Description automatically generated

Then we edited the \_swap\_readpage is used to locate where on disk a page belongs

Text

Description automatically generated

We edited zwap\_writeback\_entry in zwap file which is responsible for holding the recently used pages because  the cache might get filled with older pages, and newer pages are forced out to the slower swap device.

Text

Description automatically generated

Then we edited zswap\_frontswap\_load which attempts to

Text

Description automatically generated

Lastly, we worked on zswap\_frontswap\_store which does the following:

Text

Description automatically generated