SYNACKTIV

Exploitation kernel

Workshop HackUTT

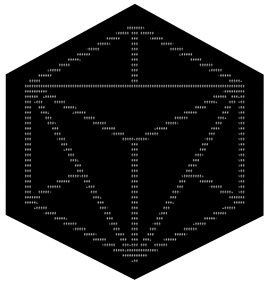
Paul Viel - Dvorhack

16/11/2023

cat /etc/passwd |grep $USER |cut -d':' -f1

SYNACKTIV

- Stagiaire reverse chez Synacktiv
- Ancien président HackUTT
- Ctf player pour HackUTT et Hexagon



Synacktiv

SYNACKTIV

- Entreprise de cybersécurité offensive
- + de 160 ninjas
- Plusieurs pôles: Reverse, Pentest, Dev, CSIRT
- Sur 5 lieux: Paris, Rennes, Lyon, Toulouse et Lille

On Recrute !!

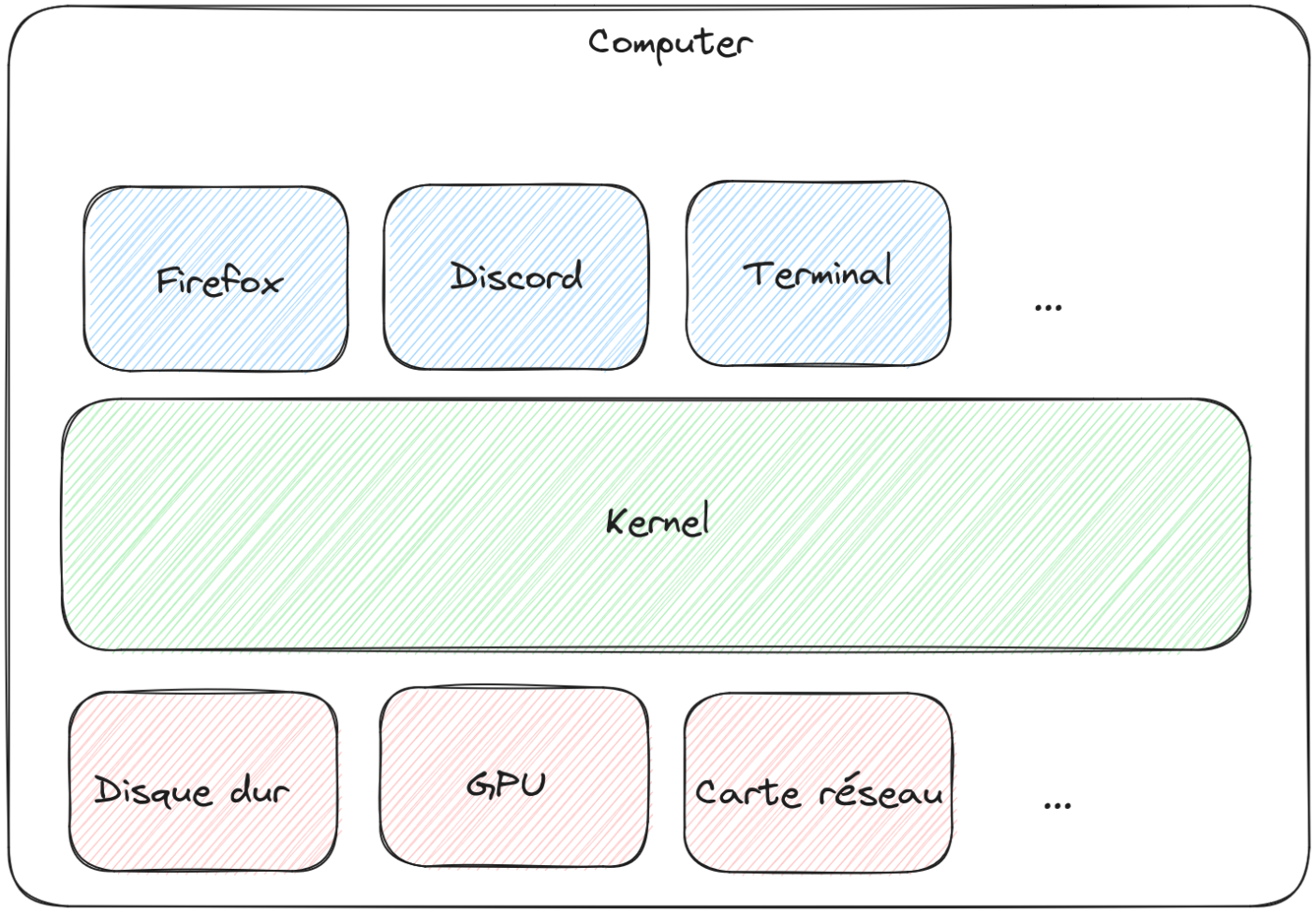
Plan

SYNACKTIV

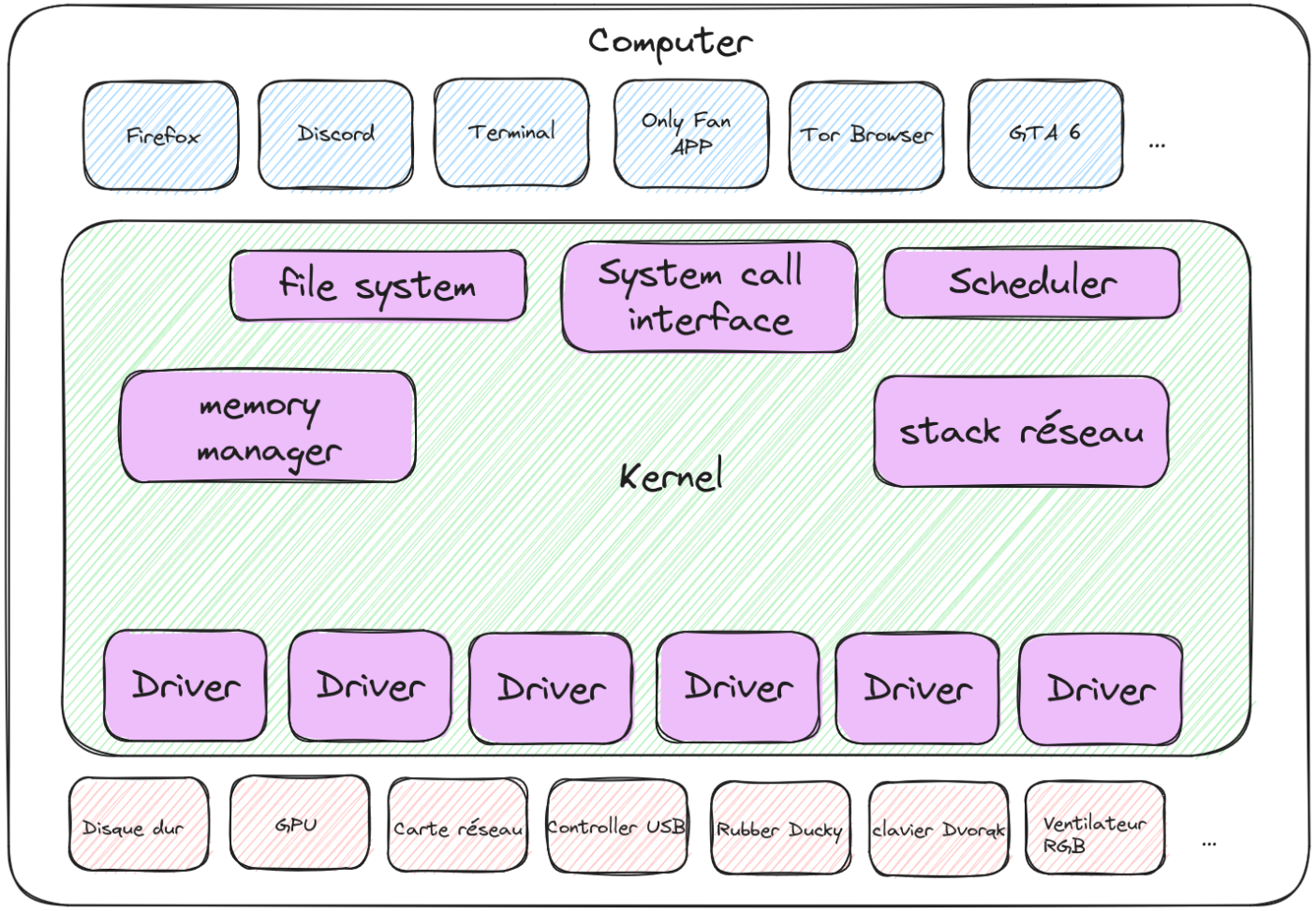
- Qu'est-ce qu'un kernel ?
- Comment fonctionne un module kernel ?
- Debug
- Exercices
- Pour aller plus loin

Kernel 1/4

SYNACKTIV

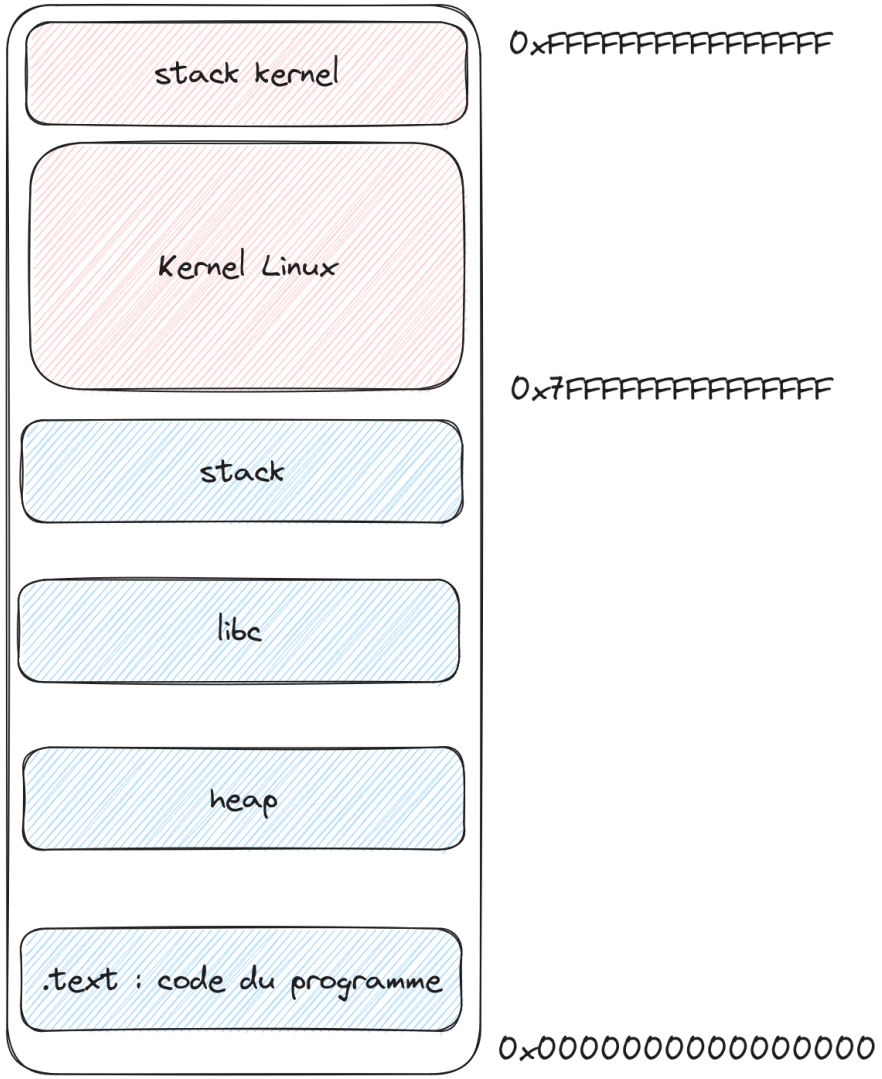


Kernel 2/4


Computer
Firefox
Discord
Terminal
Only Fan APP
Tor Browser
GTA 6
...
file system
System call interface
Scheduler
memory manager
Kernel
stack réseau
Driver
Driver
Driver
Driver
Driver
Driver
Disque dur
GPU
Carte réseau
Controller USB
Rubber Ducky
clavier Dvorak
Ventilateur RGB
...

Kernel 3/4

SYNACKTIV



Kernel 4/4

SYNACKTIV

Linux est open source !

Vérifiez vous même: https://elixir.bootlin.com/linux/latest/source

Demo 1

SYNACKTIV

- booter la vm: `./run.sh ./bzImage ./initramfs.cpio.gz`
- compress & decompress
- bzimage = noyau linux
- initramfs = filesystem

Module Kernel 1/2

SYNACKTIV

- On peut le charger au runtime
- C'est un ELF, comme les programme userland
- Extension `.ko`
- Ecrit en C (rust possible depuis Linux 6.1)
- Soumis aux buffer overflow, format string, memory leak, ...

Module Kernel 2/2

SYNACKTIV

- Pas de main() mais:
  - Obligatoire: `init`, `exit`
  - Si interaction utilisateur: `open`, `read`, `write`, `ioctl`, `close`
- Pas de printf et scanf !

```c
#include <linux/init.h>
#include <linux/module.h>
#include <linux/kernel.h>

static int __init my_module_init(void) {
    printk(KERN_INFO "Hello, World!\n");
    return 0;
}
static void __exit my_module_exit(void) {
    printk(KERN_INFO "Goodbye, World!\n");
}
module_init(my_module_init);
module_exit(my_module_exit);
```

Demo 2

SYNACKTIV

- interaction avec module
- dmesg: printk

Comment on debug ?

Reverser le noyau

SYNACKTIV

On va utiliser un outil pour convertir le noyau en un ELF importable dans Ghidra

Pour ça on utilise l'outil https://github.com/marin-m/vmlinux-to-elf

On peut maintenant importer ce ELF dans Ghidra et reverse le noyau Linux
ps: ne faites pas ça, il est open source ;)

Par contre ça nous permet de savoir l'adresse de toutes les fonctions !

Gdb dans le kernel (Demo 3)

SYNACKTIV

- /proc/kallsyms: liste des symboles
- break syscall

A vous de jouer

Exercices

SYNACKTIV

- https://github.com/Dvorhack/exercices_kernel
- `ssh 'hackutt:wskernel@warpgate.undefined-dev.fr' -p 2022`
- Exercices:
  - Chall1: Faire un kernel panic
  - Chall2: Trouver le flag
  - Chall3: devenir root

Pour aller plus loin

SYNACKTIV

- stack overflow (écraser saved RIP)
- ROPchain
- heap exploitation
- bug autre part -> comment trigger ?