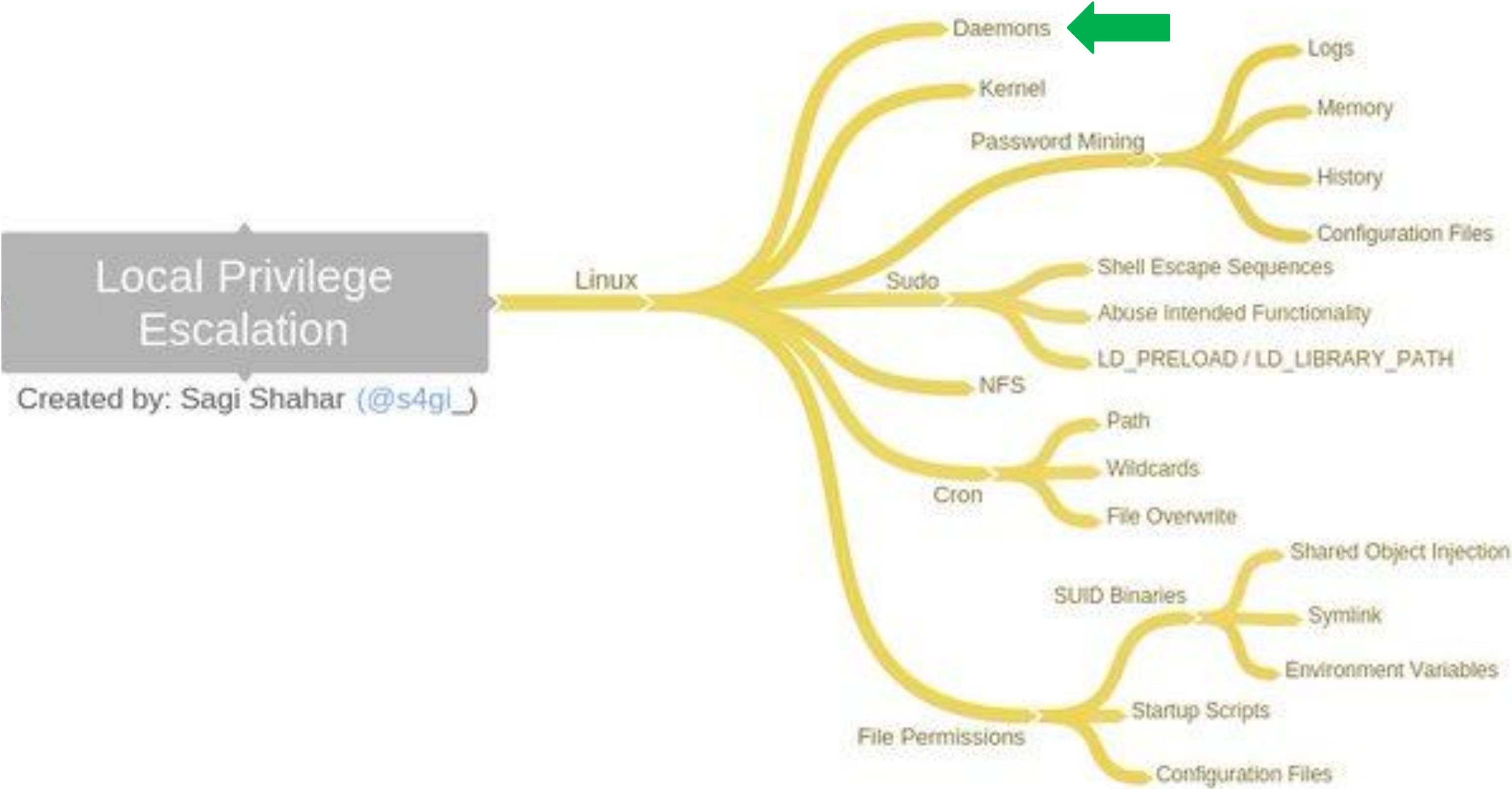




Elevación en Linux - Explotar servicios que se ejecutan como root

Escalada de Privilegios



Explotar servicios que se ejecutan como root



- **EXIM** de **EX**perimental **I**nternet **M**ailer, es un agente de transporte de correo (Mail Transport Agent o MTA) está instalado por defecto en las distribuciones Debian.
- Tiene una gran flexibilidad en los caminos que pueden seguir los mensajes según su origen y por presentar funcionalidades para control de correo basura, listas de bloqueo basados en DNS (DNSBL), virus, control de relay, usuarios y dominios virtuales y otros, que se configuran y mantienen en forma más o menos sencilla.
- Hay el **CVE-2016-1531** aplica hasta la **versión Exim < 4.86.2** que permite explotar una vulnerabilidad para la escalada de privilegios
 - <https://www.exploit-db.com/exploits/39535>
 - https://www.rapid7.com/db/modules/exploit/linux/local/exim4_deliver_message_priv_esc/



