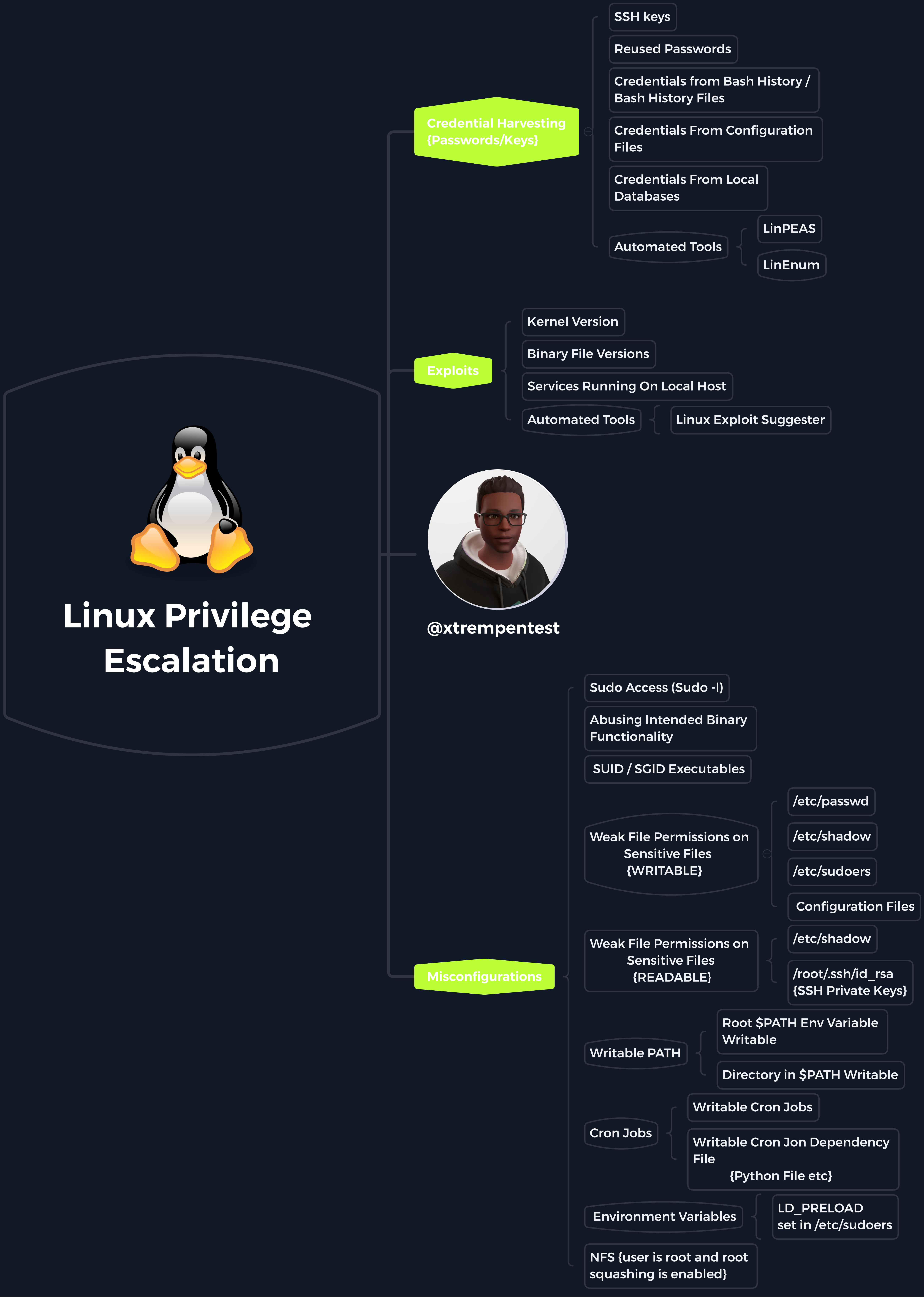

Linux Privilege Escalation

@xtrempentest

- Credential Harvesting {Passwords/Keys}
  - SSH keys
  - Reused Passwords
  - Credentials from Bash History / Bash History Files
  - Credentials From Configuration Files
  - Credentials From Local Databases
  - Automated Tools
    - LinPEAS
    - LinEnum
- Exploits
  - Kernel Version
  - Binary File Versions
  - Services Running On Local Host
  - Automated Tools
    - Linux Exploit Suggester
- Misconfigurations
  - Sudo Access (Sudo -l)
  - Abusing Intended Binary Functionality
  - SUID / SGID Executables
  - Weak File Permissions on Sensitive Files {WRITABLE}
    - /etc/passwd
    - /etc/shadow
    - /etc/sudoers
    - Configuration Files
  - Weak File Permissions on Sensitive Files {READABLE}
    - /etc/shadow
    - /root/.ssh/id_rsa {SSH Private Keys}
  - Writable PATH
    - Root $PATH Env Variable Writable
    - Directory in $PATH Writable
  - Cron Jobs
    - Writable Cron Jobs
    - Writable Cron Jon Dependency File {Python File etc}
  - Environment Variables
    - LD_PRELOAD set in /etc/sudoers
  - NFS {user is root and root squashing is enabled}