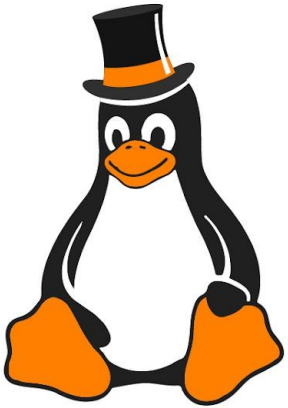
CWL
CyberWarFare Labs

Tux's Magic Hat: Tricks for Linux Persistence



About CyberWarFare Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions :

1. Cyber Range Labs

2. Up-Skilling Platform

About Speaker :

Abhijeet Kumar (Security Researcher)

His areas of interests includes Red Team Operations, Network Security, Cloud Infrastructure, and Linux Systems. Apart from this, he enjoys researching Adversarial TTPs and experimenting in his homelab.

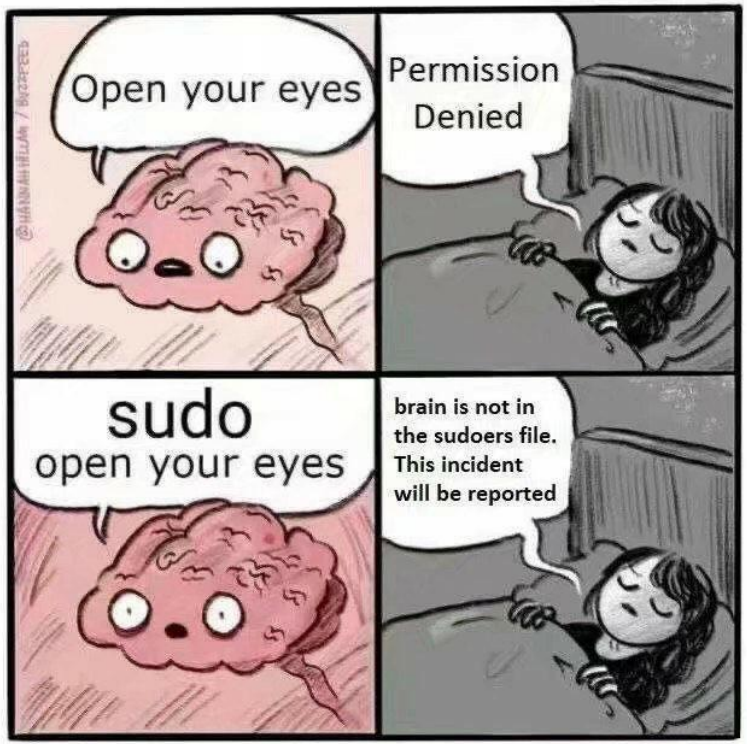
Agenda

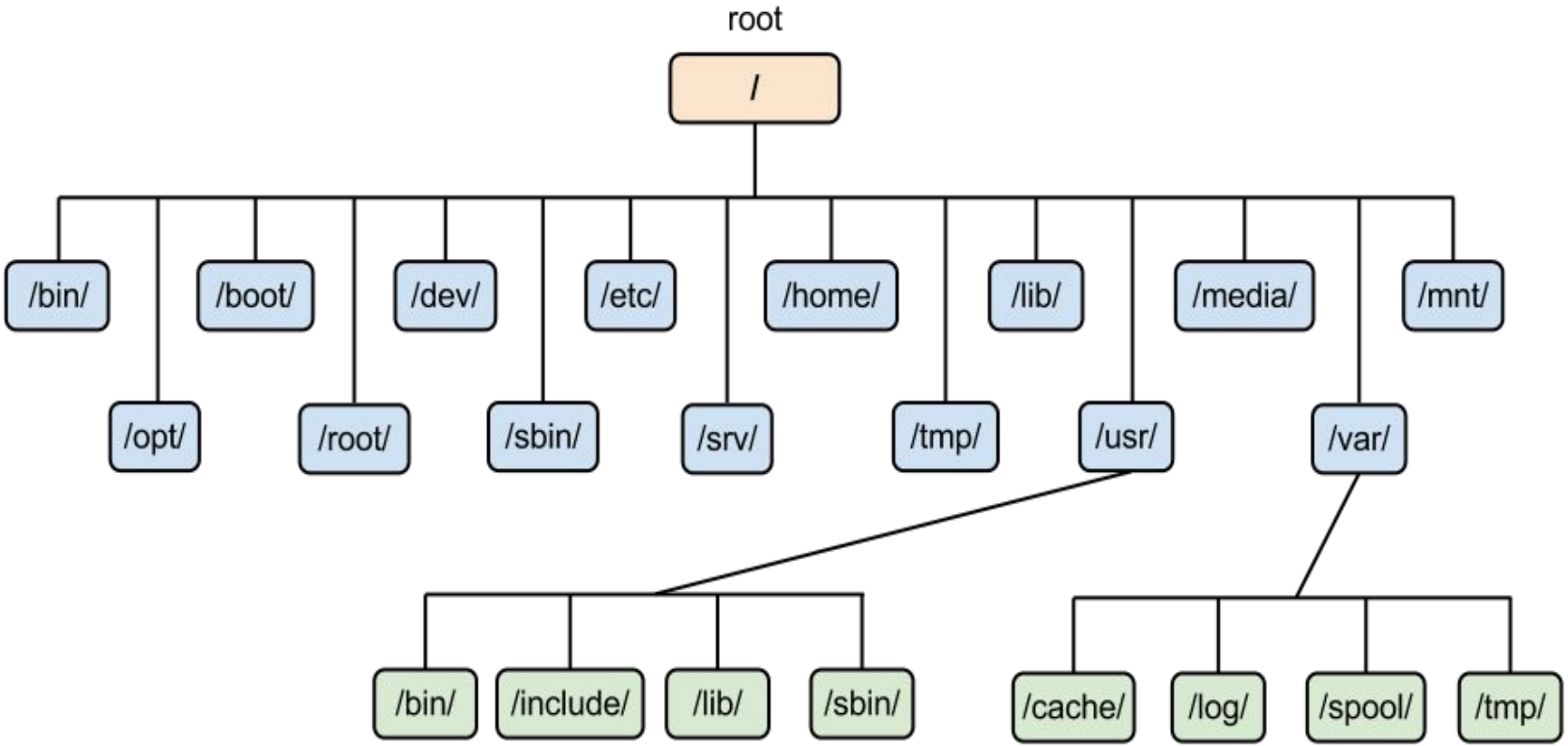
- ★ Linux 101
- ★ Persistence 101
- ★ Techniques
  - Profile Files
  - User Accounts
  - SSH Authorized Keys
  - Cron Jobs

- Systemd Service Files
- Kernel Modules
- Shared Libraries

Linux 101

- ★ Open-source GNU distros based on Linux Kernel
- ★ Highly customisable and comes in different flavours
- ★ Everything is essentially a file





Persistence 101

- ★ Techniques to gain continuous access to a compromised machine
- ★ Happens after initial compromise or after privilege escalation
- ★ A good mapping available at:

  https://attack.mitre.org/tactics/TA0003

Techniques

Profile Files [T1546.004]

- ★ Used for SHELL initialisation
- ★ Loads during booting or user logon or manually with *source <filename>*
- ★ Locations include *~/.bashrc, ~/.profile, and /etc/profile.d/*

User Accounts [T1136.001]

- ★ Used for interaction with the OS & underlying services
- ★ Can be local user accounts or service accounts
- ★ Locations include */etc/shadow*, */etc/passwd*

SSH Authorized Keys [T1098.004]

- ★ Used to allow easy access to the system via SSH
- ★ Public key is added to the *authorized_keys* file
- ★ Locations include *~/.ssh/authorized_keys*

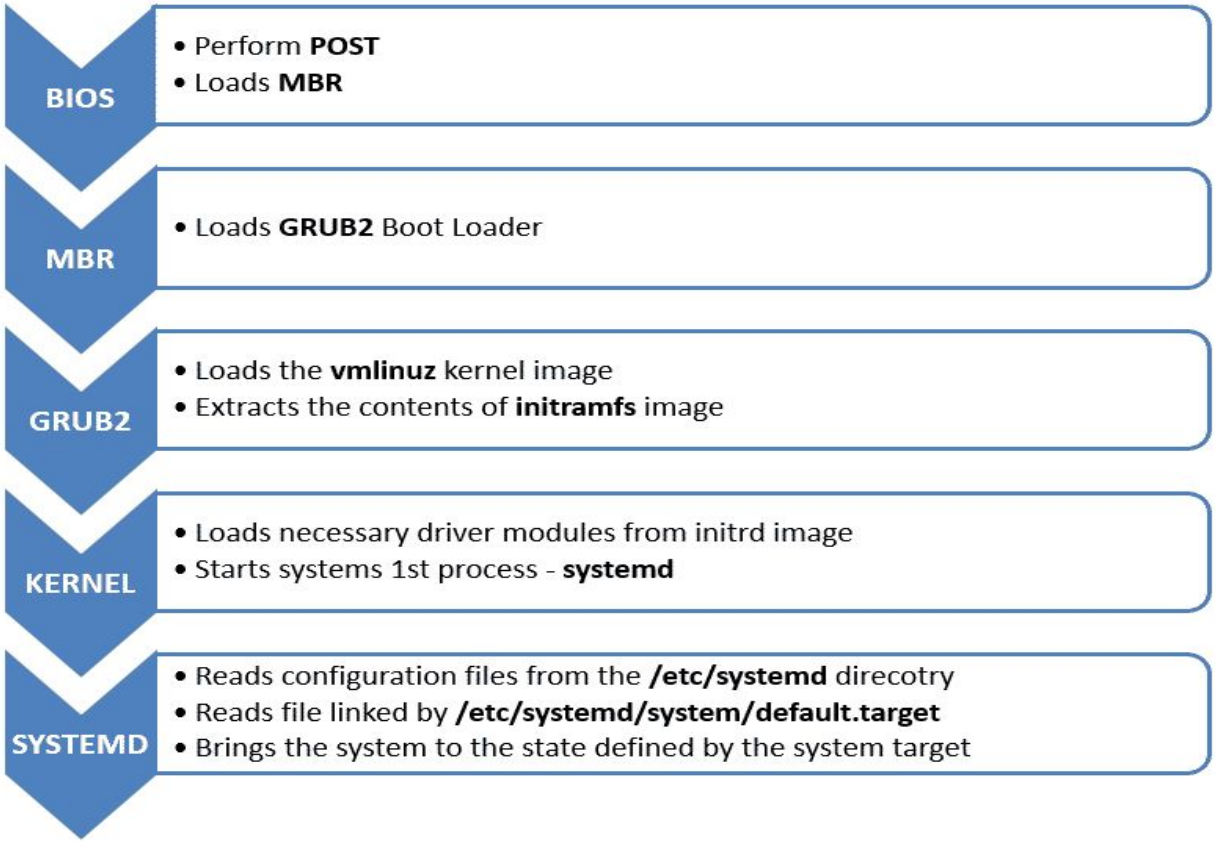
Cron Jobs [T1053.003]

- ★ Used to automate system tasks such as running scripts at pre-allocated timings
- ★ Locations include */etc/cron.d/*, */etc/cron.daily/*, */etc/cron.hourly/*, */etc/cron.monthly/*, */etc/cron.weekly/*

Systemd Service Files [T1543.002]

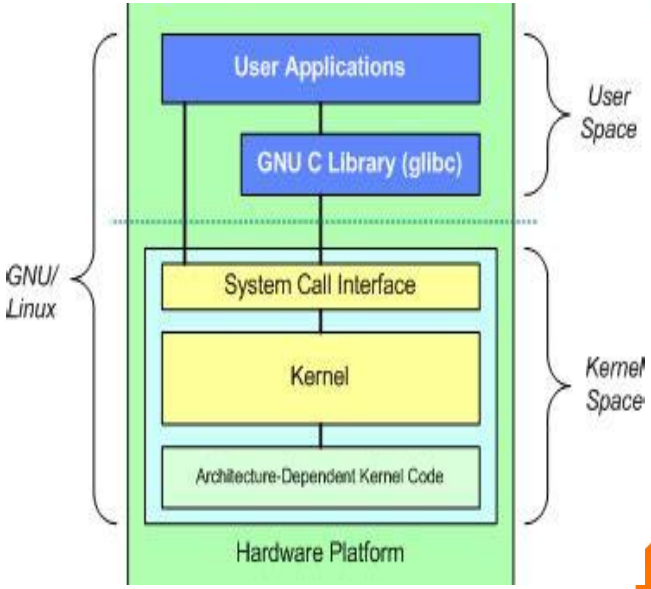
- ★ Configurations related to a service & its behaviours
- ★ Locations include */etc/systemd/system/*,

  /etc/systemd/system/default.target.wants/

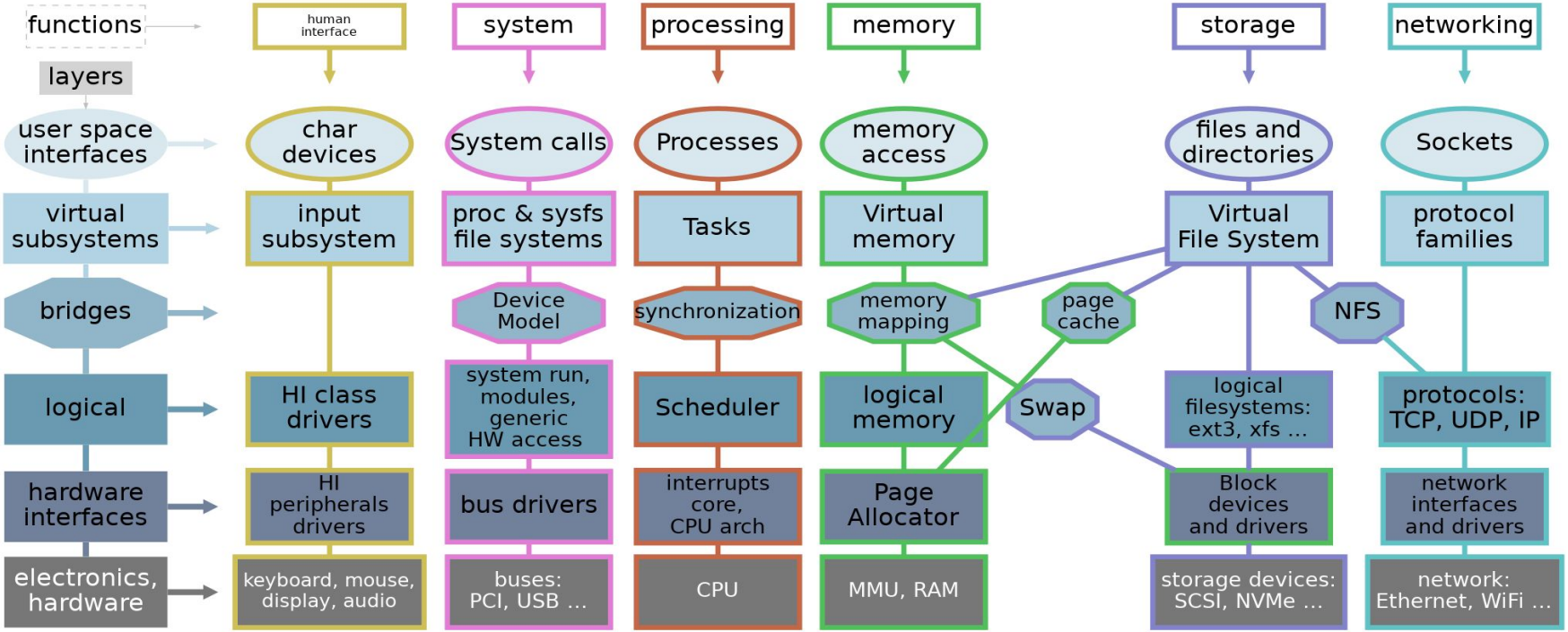


Kernel Modules [T1547.006]

- ★ Pieces of code that can be loaded/unloaded into the Kernel per requirement
- ★ Module can ONLY be loaded if its compiled for the exact same Kernel version
- ★ Commands: *insmod, rmmod, modprobe*



Linux kernel diagram

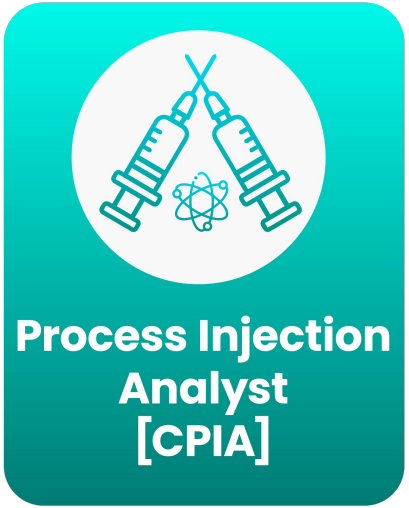


Shared Libraries [T1574.006]

- ★ Libraries loaded by a program during runtime
- ★ Process is controlled by environmental variables starting with *LD_* or *RTLD_*
- ★ Some commonly used environmental variables are *LD_LIBRARY_PATH, LD_DEBUG*

Giveaway Alert :

Certified Process Injection Analyst (CPIA)



CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team,
Cloud Cyber Range labs / Courses / Trainings, please contact

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live