Linux Persistence Map v0.2

Pepe Berba | pberba.github.io

This was created for blog series on
"Hunting for Persistence in Linux"

/sbin/init [PID 1] (System systemd)

`/etc/systemd/system.conf`

All paths in "**systemd-analyze unit-paths**":
`/lib/systemd/system/*`
`/etc/systemd/system/*`
...

systemd-generators

Executes the following:
`/etc/systemd/system-generators/*`
`/usr/local/lib/systemd/system-generators/*`
`/lib/systemd/system-generators/*`

Generates services files from:
`/etc/init.d/*`
`/etc/rc.local`

MITRE: T1037, T1547, T1037.004

systemd timers
MITRE: T1053.006

systemd services
MITRE: T1543.002

web server (web shells)

`/var/www/html/[bad.php]`
`/etc/nginx/`
`/etc/apache2/`

MITRE: T1505.003

systemd-logind

systemd --user (User systemd)

`/etc/systemd/user.conf`

All paths in "**systemd-analyze unit-paths --user**":
`/lib/systemd/user/*`
`/etc/systemd/user/*`
...

/usr/sbin/sshd (SSH Daemon)

Defined in
`/lib/systemd/system/ssh.service`

Configured in:
`/etc/ssh/sshd_config`

Runs:
`~/.ssh/rc, /etc/ssh/sshrc`

/usr/sbin/cron (Cron Scheduler)

Defined in
`/lib/systemd/system/cron.service`

Searches for cron jobs in:
`/etc/crontab`
`/var/spool/cron/crontabs/*`
`/etc/cron.d`

/etc/crontab runs jobs for anacron:
`/etc/cron.hourly/*`
`/etc/cron.daily/*`
`/etc/cron.weekly/*`
`/etc/cron.monthly/*`

MITRE: T1053.003

user systemd-generators

Executes the following:
`/etc/systemd/user-generators/*`
`/usr/local/lib/systemd/user-generators/*`
`/usr/lib/systemd/user-generators/*`

MITRE: T1037

Pluggable Authentication Modules (PAM)

`/etc/pam.conf`
`/etc/pam.d/*`

MITRE: T1556.003

User Accounts

User Info:
`/etc/gshadow  /etc/sudoers`
`/etc/passwd   /etc/sudoers.d/`
`/etc/groups`

Authentication Info:
`/etc/shadow`
`~/.ssh/authorized_keys`

MITRE: T1136.001,T1078,T1098.004 T1098

motd

`/etc/update-motd.d/*`

MITRE: T1037

user systemd timers
MITRE: T1053.006

user systemd services
MITRE: T1543.002

rootkits

User Mode Rootkits:
`/etc/ld.so.preload`

Kernel Mode Rootkits:
`/lib/modules/`

Look for usage of:
`modprobe, insmod,lsmod,rmmod`

MITRE: T1547.006, T1574.006

infected client software

OS and User Binaries:
`/bin, /sbin, /usr/bin/, /lib, ...`

Example Python and unattended-upgrades:
`/usr/lib/python3*`
`/usr/local/lib/python3*/dist-packages`
`/usr/share/unattended-upgrades/`
`unattended-upgrade-shutdown`

MITRE: T1554

/bin/bash (Login Shell)

`/etc/bash.bashrc`
`~/.bashrc`

`/etc/profile`
`/etc/profile.d/*`
`~/.profile`
`~/.bash_profile`
`~/.bash_login`

`/etc/bash.bash_logout`
`~/.bash_logout`

MITRE: T1546.004

*Note: Strictly, the **pam_systemd** module is what launches user systemd and registers the session to **systemd-logind** but this interaction is not captured by this map to make it less messy*