# SYSTEMD TIMERS

Hal Pomeranz

# WHO IS HAL POMERANZ?

Started as a Unix Sys Admin in the 1980s

Independent consultant since 1997

Digital forensics, incident response, expert witness

Have done some interesting Linux/Unix investigations

hrpomeranz@gmail.com

@hal_pomeranz@infosec.exchange

*https://archive.org/details/HalLinuxForensics*

# WHAT ARE SYSTEMD TIMERS?

Yet another task scheduler in Linux

*Realtime timers*

Fire at particular times, like cronjobs

*Monotonic timers*

"Run 30 minutes after boot time", etc

# BASIC CONFIGURATION FILES

`*.timer` file

- When does it run?
- Usually triggers `*.service` file (or `Unit=`)

`*.service` file

- `ExecStart=` script path to execute
- Other options, security configs, etc

Must live in standard Systemd directories

# STARTING A TIMER

```
# ls -l /etc/systemd/system/local-stuff.*
-rw-r--r-- 1 root root 100 Jan  8 22:56 /etc/systemd/system/local-stuff.service
-rw-r--r-- 1 root root 115 Jan  8 22:54 /etc/systemd/system/local-stuff.timer
# systemctl enable local-stuff.timer
Created symlink …/multi-user.target.wants/local-stuff.timer → …/local-stuff.timer.
# systemctl start local-stuff.timer
```

*Start timer at next boot*

*Start timer right now*

# CREATE TIMERS ON THE FLY

```
# systemd-run --on-calendar='*-*-* *:*:15' /tmp/.ICEd-unix/startup.sh
```

Creates `run-`*`<hash>`*`.timer` and `.service` files in `/run/systemd/transient`

Won't survive reboot

# GET TIMER STATUS

```
systemctl list-timers --all
```

```
systemctl status *.timer
```

# PER-USER TIMERS

Normal users can access Systemd timers interface by including `--user` on all command lines

Unit files in `$HOME/.config/systemd/user/`

`systemd-run --user …` files found in `/run/user/<uid>/systemd/transient/`

# ARTIFACTS TO COLLECT

Command output (as root)

```
systemctl list-timers --all
systemctl status *.timer
```

Directory contents

```
/usr/lib/systemd/system
/etc/systemd/system
/home/*/.config/systemd
/root/.config/systemd
/run/systemd/transient
/run/user/*/systemd/transient
```

# THANK YOU!

Any final questions?

Thanks for listening!

hrpomeranz@gmail.com

@hal_pomeranz@infosec.exchange

*https://archive.org/details/HalLinuxForensics*