# Using Open Source to get above the security poverty line

By Christopher Coffey RHCE, CISSP

# whoami:

chris@cybermercindustries.com

- 20+ years working with *nix
- Worked in the security field (within both the DoD and the banking sectors).
- Worked as a Linux Admin/Engineer for various companies including last 7 years Rackspace

# What is the Security Poverty Line ?

- Loosely defined as any entity that does not have the technical ability and/or the financial resources to hire security expertise

# What am I here to show?

- What is a functional baseline for Linux security?
- How we can help make it easy and cheap using open source solutions.

# What is a functional Linux security baseline?

- DISCLAIMER: This is opinionated…
- Proactive patching policy
- Don’t use login as root ever…
- SSH Hardening
- Log Monitoring

# Proactive patching policy

- At a minimum auto-patch on a set schedule
- Yeah really patch - No excuses…

# Non-root admin user

- If your logging in as root - YOUR DOING IT WRONG **PERIOD**

# SSH Hardening

- Disable Root login
- Set users lists that is allowed to login via SSH
- Use of SSH key login at a minimum, optionally use key and password even better.

# Log Monitoring

- Setup remote log monitoring if possible
- at a minimum use a tool such as logwatch to flag important issues and notify via email (setup via cron)

# Demo scripts

https://github.com/cybermerc/tlf_talk/tree/master/scripts