Who am I?

- Network Administrator - Hobson Wildenthal Honors College
- Infrastructure Maintainer - Void Linux
- Software Engineer - BEST Robotics
What is this "Linux Security" you speak of?

- Isn't Linux secure by default?
- I have a new server, what do I do?
- Ok, what goes into the day to day security operations?
- Uh oh, I think someone's in my box...
Just how secure is Linux?

This depends on who you ask and what you're doing. It can range from "very" to "not at all".
Some glaring holes

- X
  - Just... In general. X is really bad for security

- Complex System Software
  - How do you know if it's a legitimate process if you don't know what it does?
  - Not really a huge issue (svchost.exe...) but still something to be aware of

- Of Many Firewalls
  - Iptables, arptables, ufw, pf-fork, etc.
Things that Just Work™

- File Permissions
  - User, Group, Mode
  - ACLs for the adventurous
- User Groups
- root authority
But Wait!! You didn't talk about SELinux

- SELinux is a mixed bag
- Very complex to understand what it's doing
- Often treated like voodoo magic
- Really narrowly supported, not available on most distros
- There are certainly cases to use SELinux, but they tend to be after other steps
- [The SELinux Coloring Book](https://example.com/selinux-coloring-book)
Overall Linux is Decently Secure

- A well maintained system would be fairly difficult to compromise
- Modern distros try to be fairly secure by default
- Most 'important' programs don't let you do insecure things
First 10 minutes on a box

- Do you have sudo?
  - Yes - lock the root account
  - No - configure sudo

- Is the firewall up
  - Yes - audit the ruleset, can you explain everything that's there?
  - No - configure an iptables ruleset

- Reconfigure SSHd
  - ED25519 Host Keys
  - Turn off root logins if they were on
  - Keyed login only
  - Consider 2-factor authentication
Next 10 minutes on the box

- Can you explain every non-system account with access?
- Can you explain all the system accounts (or at least pick out bad ones)?
- Do only users with justification have sudo rights?
- Are the file permissions/checksums on all the base files correct?
  - debsum/clever shell script/etc.
  - Some package systems provide a way to get a diff
Daily Upkeep

● Install the updates (duh)
● Skim logs periodically
● Look for anomalous trends
● Install a monitoring suite
  ○ Preferably something with graphs
  ○ Ideally something with alerts that support e-mail
I get the feeling I'm not alone here...
Has something changed?

- What's in the authlog?
- What's the mtime on files in /etc
- What's the atime (if enabled) in /etc
- What is the output of `who`
- Did sshd see anything unusual in the logs?
What to do after a breach

- Tell internal security there's been a breach
- Assume the box is totally compromised
- Back up production data
- Optional: Take a full system image
  - Perform a root cause analysis on this image later
- Re-format & Reinstall (Or redeploy from your tested, regular backups)
- Disclose the issue responsibly
Root cause analysis

- Full system diff
- Audit software versions
- Audit application logs
- Review firewall rules

Ultimately you want to know who got in to what by means of which vulnerability in exactly what subsystem!
Easy Tools of the Trade

- Iptables
- Man
- Netdata
- Pam_google_authenticator
- Strong passphrase

- Less
- Tail
- Journalctl
- Svlogtail
- Rsyslogd
More complex tools

- Snort
- Honeypot (cowrie, VM, etc.)
- Centralized Authority
- Physical authority tokens
- Mandatory 2-Factor
- Network level security
  - 802.1X
  - IPSec
  - Krb5p

- ELK Stacks
- Centralized Logging
- Centralized Pager management
- OOB Management
Questions?