Linux Security and Hardening Essential Training

General Security

- Linux is "secure", but it's not a panacea.
- People play a key role in security.
- Security is an ongoing process.
- Linux security features
  - Open Source.
  - It's not a popular target.
  - Package management.
  - Separation of privileges(multi-user system).
- Security Principles
  - Principles of Least Privilege
  - Use encryption
  - Shared accounts (Yes, root can be a shared account!)
  - Multi-factor authentication
  - Firewall
  - Monitoring logs

Physical Security

- Protect from Grub `e` edit single user mode
  - In systemd go to `/lib/systemd/system/`
  - Replace `sushell` with `sulogin` in emergence.service and rescue.service
- Protect Grub by password
  - Let's just say username=`grubProtect` and password=`grubzilla123`
  - In `/etc/grub.d/40_custom` add `set superuser="grubProtect"` `password grubProtect grubzilla123`
  - For encrypted password `grub-mkpasswd-pbkdf2`
  - Enter the password=`grubzilla123` and get an output like this `PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.1CAEF371E5B24AF502560031A2`
  - In /etc/grub.d/40_custom `set superuser="grubProtect"` `password_pbkdf2 grubProtect grub.pbkdf2.sha512.10000.1CAEF371E5B24AF502560031A265F2`
  - Then `update-grub`
- Disk Encryption
  - Install `cryptsetup`
  - Encrypt New Device/Disk **Encrypting Disk Will Remove All Data**
    - Fill device with random data `sudo shred -v -n 1 <e.g. /dev/sdb , i.e diskname>`
    - Now Run `cryptsetup` and put in the passphrase `sudo cryptsetup luksFormat <e.g. /dev/sdb , i.e diskname>`
    - Open the device and put in the passphrase `sudo cryptsetup luksOpen <e.g. /dev/sdb , i.e diskname> <e.g. opt,`

i.e name for the folder>
        * Since here we named the folder opt, you can find that disk on /dev/mapper/opt
        * Formating the device sudo mkfs -t ext4 /dev/mapper/opt
        * Close the device sudo cryptsetup luksClose opt
        * Updating /etc/fstab for mounting while login /dev/mapper/opt /opt ext4 defaults 0 0
        * Updating /etc/crypttab for asking passphrase while mounting opt /dev/sdb none luks
    - Encrypt a File or Folder
        * For example Make folder /data sudo mkdir /data
        * Locate 100mb to a file opt in /data sudo fallocate -l 100M /data/opt
        * Adding random data to file opt sudo dd if=/dev/urandom of=/data/opt bs=1M count=100
        * To check the random data in /data/opt sudo strings /data/opt
        * Now encrypting /data/opt sudo cryptsetup luksFormat /data/opt
        * Open sudo cryptsetup luksOpen /data/opt opt
        * Format
          sudo mkfs -t ext4 /dev/mapper/opt
        * Mount sudo mount /dev/mapper/opt /opt
    - Encrypting Device with Data
        * Backup this Device
        * Fill the Device with random data using shred or dd
        * Encrypting the Device
        * Open the Device
        * Format it, mostly ext4
        * Mount and use it
- Disable Control + Alt + Delete
    - Control + Alt + Delete in systemd, rebooting your system.
    - To disable this systemctl mask ctrl-alt-del.target systemctl daemon-reload ### Summary
- Physical security threats.
- Physical security guidelines.
- Single user mode defenses.
- Kernel Parameter Protection.
- Disk encryption with LUKS.
- Disabling reboots from Ctrl+Alt+Del

Account Security

Network Security

File System Security