Working with Encrypted Storage

LPIC-2: Linux Engineer (201-450)

Objectives:

At the end of this episode, I will be able to:

1. Describe LUKS full-disk encryption under Linux.
2. Create encrypted storage and bring it online for use.
3. Configure encrypted storage to automatically mount at boot time.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- Linux Unified Key Setup (LUKS)
  - Uses a master key to encrypt a partition
  - Multiple user keys can be issued to decrypt the master key
    - 8 or less users recommended
  - Encrypts the entire block device
  - Enabling during installation uses 512bit AES encryption
  - Enabling from the CLI defaults to 256bit AES
- Enabling during install
  1. Click `Installation Destination` on the Installation Summary page
  2. Select an installation disk
  3. Scroll down and check "Encrypt my data" and click `Done`
  4. Enter a pass phrase
  5. Complete the installation as usual
- Verify the disk is unencrypted
  - `lsblk -f`
  - Type should show as ext4, xfs, etc
- Backup source data and unmount the device
- Populate unused disk space with random data
  - `shred -v --iterations=1 /dev/sdd1`
- Install the LUKS tools
  - `sudo apt install cryptsetup-bin`
- Initialize the device
  - `sudo cryptsetup -v luksFormat /dev/sdd1`
  - Enter desired pass phrase
- Verify the drive is encrypted
  - `lsblk -f`
  - Type should show as crypto_LUKS
- Open the device
  - `sudo cryptsetup luksOpen <device> <alias>`
  - `sudo cryptsetup luksOpen /dev/sdd1 storage`

- Format and mount the device
    - `sudo mkfs.ext4 /dev/mapper/storage`
    - `sudo mkdir /mnt/storage`
    - `sudo mount /dev/mapper/storage /mnt/storage`
- Update the `crypttab` file to open the device at boot
    - `sudoedit /etc/crypttab`
    - `storage /dev/sdd1 password123`
    - or
    - `storage /dev/sdd1` to prompt at boot time
- Update the `fstab` file to mount the device at boot
    - `sudoexit /etc/fstab`
    - `/dev/mapper/storage /mnt/storage ext4 defaults 0 0`
- Add keys for other users
    - `sudo cryptsetup luksAddKey /dev/sdd1`
- Remove keys as needed
    - `sudo cryptsetup luksRemoveKey /dev/sdd1`