Restricting Access to SSH

LPIC-2: Linux Engineer (202-450)

Objectives:

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

1. List the methods available for controlling access to SSH.

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

- Restricting Access to SSH
    - Limiting user access to SSH
    - Controlling the root user
    - Using TCP wrappers with SSH
- Restricting SSH
    - SSH is a management protocol
    - Default configuration
        - Any valid user can access it
        - The root user is a known entity
        - Susceptible to brute force attacks
        - Open in most firewalls by default
- Limiting user access to SSH
    - Modify the SSH config file
        - `sudoedit /etc/ssh/sshd_config`
        - `sudoedit /etc/ssh/sshd_config.d/hardened.conf`
    - Restricting User Access
        - `AllowUsers user1 user2 user3`
        - `AllowGroups group1`
- Controlling the root user
  - `PermitRootLogin no`
- Using TCP wrappers with SSH
    - `/etc/hosts.allow`
        - `sshd : LOCAL,10.222.0.`
    - `/etc/hosts.deny`
        - `sshd : ALL`
- Controlling SSH access with a firewall
    - `sudo ufw allow from 10.222.0.0/24 proto tcp to any port 22`