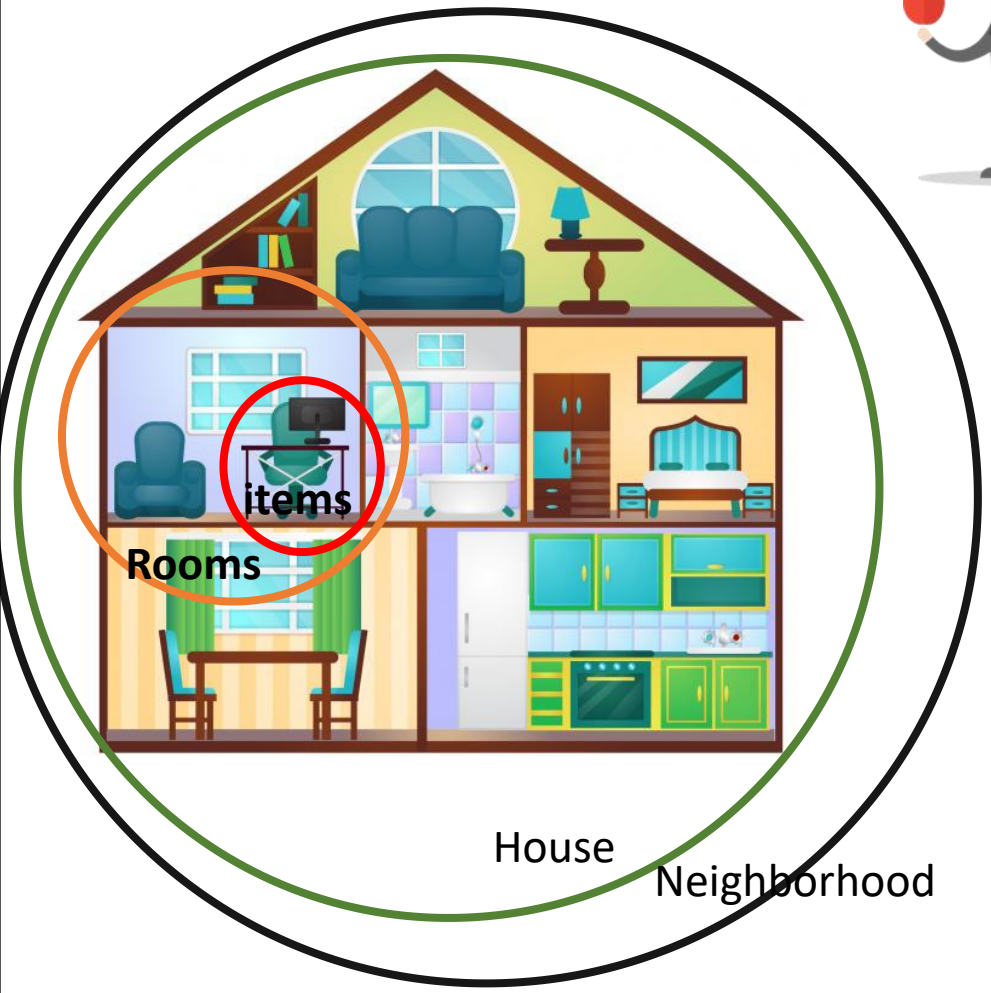
Operating System Security
#1 Security Concepts

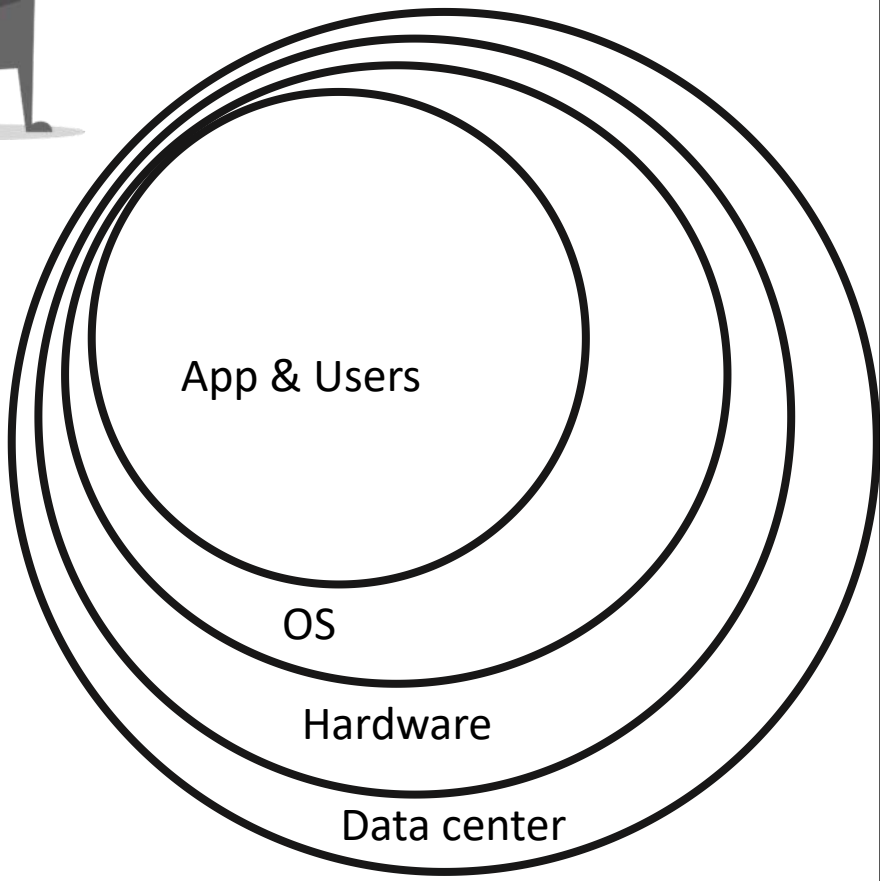
Herman Kabetta, M.T.

Security & OS Hardening

- Security
  - Any type of protection against harm
- Computer Security
  - Computer security, cybersecurity or information technology security (IT security) is the **protection of computer systems** from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. (wikipedia)
- Linux Security
  - Linux is an open source OS whose code can be easily be read by the users, but still, it is the more secure OS when compared to the other OS. (itsfoss.com)
  - The need of Linux security arises for 2 reasons
    - Internal = No access to outside world (protect from your own mistakes)
    - External = Serving outside services such as http, ftp, smtp, etc.
- OS Hardening
  - OS Security or hardening used interchangeably
  - In simple words, hardening is used when making the OS so hard to break

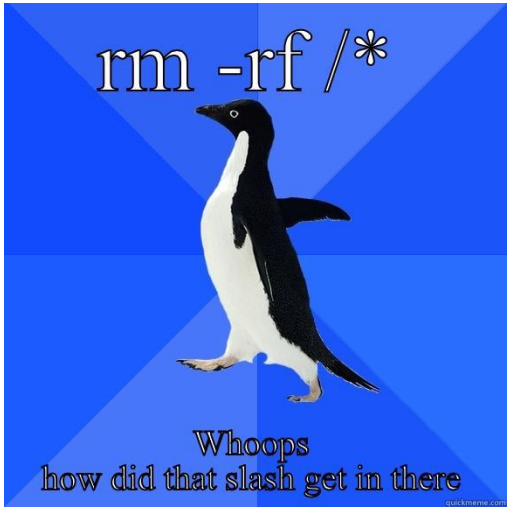
The Analogy


items
Rooms
House
Neighborhood


App & Users
OS
Hardware
Data center

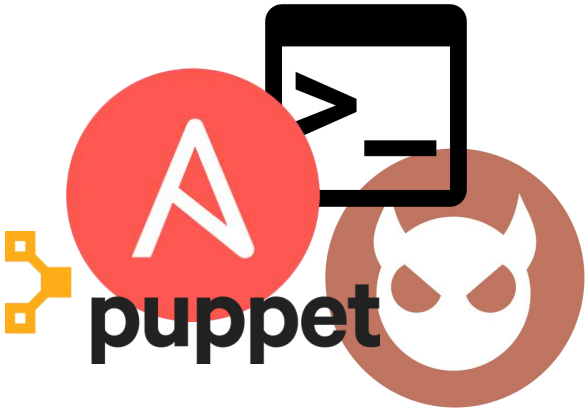
Linux Security, why so important?

- Data protection -> the primary reason
- Protect system resources (memory, CPU, disk etc.)
- Protect application workflows
- Audit compliance (service organization controls – SOC reports)
  - SOC became effective on June 15th, 2011
- Less human errors
- Control management (who gets what, who can access what)
- Peace of mind



Security Implementation Tools

- **Manual security configuration**
  - User Accounts
  - File Systems
  - System access
  - System security (system configuration files)
  - Configuration files in /etc directory
  - OS network layer security



- **Automate through scripts**
  - Create a script
  - Copy over or access over network
  - Execute one by one on each server

- **Deployment tools (Ansible, Puppet etc.)**
- **3rd part security software (e.g. ClamAV) – Not for all security measures**

Types of Security Breach

- **Data**
  - Steal
  - Corrupt
  - Remove
- **Application**
  - Apache
  - Database
  - Financial App
- **Operating System**
  - Filesystem corruption
  - System failure
  - process management
- **Hardware (Attack on CPU, memory, etc.)**

Lab Preparations

- Oracle VirtualBox
- CentOS 7 iso
- Putty or SSH Client Terminal

CentOS Installation

- **SOFTWARE SELECTION (Tick as shown below)**
  - Infrastructure server > DNS Name Server
  - Server with GUI > Java Platform
    > KDE
  - GNOME Desktop > GNOME Application
  - Done.

- **NETWORK & HOST NAME**
  - Input “Host name” as you want
  - Click “Configure..” button, tick “Automatically connect to ...” on General tab
  - Done.

- **USER SETTINGS**
  - Input root password
  - make a new user, dont forget to tick “Make this user administrator”