UNIVERSITY OF ALASKA FAIRBANKS

# Linux User Management

Arsh Chauhan

11/18/17

*Celebrating a century 1917–2017*

# This Week in Security

- https://krebsonsecurity.com/2017/11/ddos-for-hire-service-launches-mobile-app/

# User Management

# What is it?

Managing access rights to a computer on a per user basis. Why is this important?

# Why is it Important?

- ALL computers have multiple users

# Why is it Important?

- ALL computers have multiple users
- Each user needs access to their files

# Why is it Important?

- ALL computers have multiple users
- Each user needs access to their files
- Users expect their files to be private

# Why is it Important?

- ALL computers have multiple users
- Each user needs access to their files
- Users expect their files to be private
- May need file access based on groups

# Why is it Important?

- ALL computers have multiple users
- Each user needs access to their files
- Users expect their files to be private
- May need file access based on groups
- Bad things happen when this breaks (DirtyCOW)

# Linux User Management

# Theory

Linux handles user management using groups

# Theory

Linux handles user management using groups

- Users can edit their own files

# Theory

Linux handles user management using groups

- Users can edit their own files
- Users can edit/view files based on their groups

# Theory

Linux handles user management using groups

- Users can edit their own files
- Users can edit/view files based on their groups
- Root can do everything

# Theory

Linux handles user management using groups

- Users can edit their own files
- Users can edit/view files based on their groups
- Root can do everything
- Some users can become root with sudo

# Groups

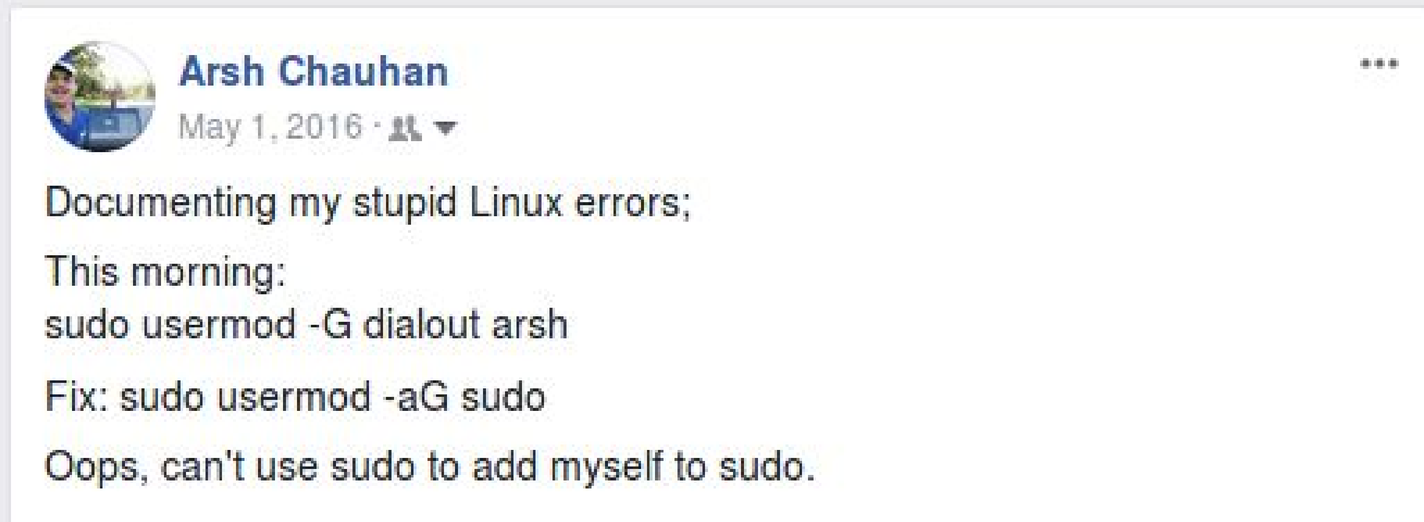
# Theory

- Each user has their own group
- Users can be part of multiple groups
- Some groups are special
  - dialout, sudo, admin, wheel
- Used for file permissions

# Useful Group Management Commands

- adduser: Add a new user
  - sudo adduser bob # Use this for non-scripts
- useradd: Alternate way to add a new user
  - Easy to script
- usermod: Modify a user
  - usermod -a -G sudo bob # add bob to group sudo
- userdel: Delete a user or remove from a group
- getent : Can be used to see users in a group

# Be careful !!



Arsh Chauhan

May 1, 2016 ·

Documenting my stupid Linux errors;

This morning:
sudo usermod -G dialout arsh

Fix: sudo usermod -aG sudo

Oops, can't use sudo to add myself to sudo.

# Sudo

# What is Sudo

- Allows some users to run commands as root

# What is Sudo

- Allows some users to run commands as root
- Originally “SuperUser DO” since you could only do stuff as root
  - substitute user do

# What is Sudo

- Allows some users to run commands as root
- Originally “SuperUser DO” since you could only do stuff as root
    - substitute user do
- Now you can use it to run commands as any user

# What is Sudo

- Allows some users to run commands as root
- Originally “SuperUser DO” since you could only do stuff as root
- Now you can use it to run commands as any user
- Need to be in sudo or wheel group

# Sudoers File

- Describes how sudo works
- Located in /etc/sudoers
- ALWAYS use visudo to edit
  - sudo visudo -f /etc/sudoers
  - Syntax dependent, visudo checks syntax
- **Keep a root terminal open as backup**

# Bad Things

- Misconfigured sudoers can circumvent security
- Common examples
  - bob ALL=(ALL:ALL) ALL #Allow bob sudo
  - ellliot ALL=NOPASSWD:ALL #elliot can sudo without a password
  - %hr ALL=(ALL:ALL) ALL #users in hr group get sudo
- These examples overwrite the sudo group

# Lab

Allsafe

Cybersecurity

# Scenario

You’re a cyber security analyst for AllSafe CyberSecurity, the security contractor for E-Corp. You’ve been assigned to audit the user accounts on some of their machines after the F-Society hack and Tyrrell Wellick being fired. Attached is an organization chart for everyone that matters. Based on this information, complete the following tasks and write a report for Gideon Goddard.

- Provide a list of all user accounts
- Provide a list of all sudo users
- List users you removed from sudo (if any)
- Add the current CTO to sudo
- Add a user for Gideon Goddard with sudo
- Any weird sudo configuration issues

Creds:eanderson/mrrobot

# Org Chart

| Full Name | Position | Status |
|---|---|---|
| Phillip Price | CEO | Employed |
| Terry Colby | CTO | Fired 02/15 |
| Tyrell Wellick | Interim CTO/ Ladies man | Fired |
| Scott Knowles | CTO | Employed |
| Angela Moss | Risk Management/ Pretty face | Employed |
| Elliot Anderson | AllSafe Analyst | Employed |