Elevating Privileges in Linux

Andrew Mallett

Linux Author and Trainer

@theurbanpenguin www.theurbanpenguin.com

Overview

Becoming the Boss

- Privilege escalation
    - su
    - sudo
    - environment variables and sudo
    - using PolKit (PolicyKit)

UID 0, usually root, manages your Linux System. Using **su, sudo, pkexec** we can elevate to UID 0

```
$ su

$ su -

$ su -l

$ su - bob
```

su - Substitute User

Using the command su we can change to the root account, or any account that we have the password for. If the root account does not have a password, then this is not an option. We can just change to the account, or we can execute a full login

Having all administration team all knowing the root password is not the best of ideas!

Demo

Let's begin by using the su command:

- Login or non-login shell
- Testing user accounts

```
$ sudo less /etc/sudoers
$ sudo ls /etc/sudoers.d/
```

Sudo

Using sudo, we can delegate administrative tasks without the need to divulge the root password or give access to all commands

```
$ sudo visudo

$ sudo visudo -f /etc/sudoers.d/bob
```

Editing the Sudoers Files

Using the command visudo to make changes to the configuration will enforce a syntax check when the file is saved. A misconfigured sudo entry will disable sudo access to your system.

```
tux 192.168.33.13=(root) NOPASSWD: ALL
%wheel ALL=(root) ALL
%helpdesk ALL=(root) /usr/bin/passwd, !/usr/bin/passwd root
```

Sample Entries

We illustrate 3 entries that you may be able to use

Demo

Creating Sudoers Entries:

- syntax checking
- delegating tasks to users

```
$ sudo visudo -f /etc/sudoers.d/defaults
Defaults env_keep += "EDITOR"

$ export EDITOR=nano

$ sudo visudo
```

Using Another Editor

In RedHat based systems the default editor will be vi, other distributions may use nano. You can set the EDITOR variable but this needs to be allowed to pass though to sudo.

Demo

Using a different editor

- sudo -i
- using environment variables with sudo

```
$ pkaction
$ sudo cat /etc/polkit1/rules.d/50-default.rules
$ echo $$

$ pkttyagent --process 5296

$ pkexec cat /etc/shadow

$ enter password
```

Using Polkit (Formerly PolicyKit)

Designed more for desktop systems we have PolKit. A separate authenticator program is required to authenticate users. Make sure your user has a password and you belong to the wheel group. We require the authenticator to monitor the process in another window

Demo

Using a default PolKit rules

- use pkttyagent and pkexec
- recover from failed sudo system

Summary

In this module we have introduced privilege escalation in Linux

- su
- su -
- su -l
- sudo
- visudo
- visudo -f
- visudo -c
- Defaults env_keep += "EDITOR"
- /etc/polkit-1/rules.d
- pkexec / pkttyagent

Managing Local Users