CompTIA Linux+: Security

Securing Linux Systems

Andrew Mallett
Linux Author and Trainer

@theurbanpenguin www.theurbanpenguin.com

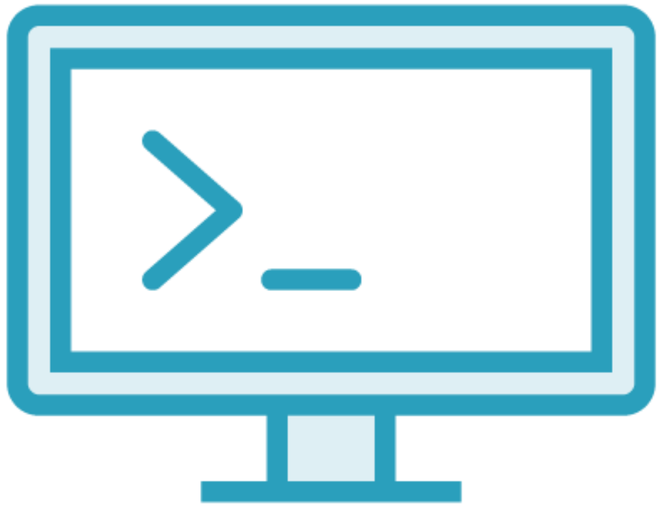
Overview

Working with Pluralsight and CompTIA's certification will help you learn and secure Linux

Course Overview

- File Permissions and ACLs
- SELinux and AppArmor
- Securing SSH
- IDM, Users, Privileges and Elevation
- SSL/TLS and PKI
- Firewalls

Distribution Agnostic Lab Systems



CompTIA recommend using a mix of distributions, we include

- Alma Linux 8.5 (RHEL Rebuild)
- Ubuntu 20.04 LTS
- openSUSE Leap 15.2

Building in Vagrant/VirtualBox allows use of our Vagrantfile shared in the exercise files download.

CompTIA Linux+ is a distribution agnostic Linux certification helping you to get started in Linux administration and DevOps

```
$ sudo yum install -y httpd

$ ls -ld /var/www/html
```

Accept the Defaults?

Using Enterprise Linux, you might expect the defaults to work for you, just as an example the file permissions in both the green and red enterprise distributions expect the web server to gain access to HTML pages using permissions granted to others!!

NEVER accept DEFAULTS

Learn and SECURE

Demo

Installing the Apache Web Server

- We illustrate weaknesses in leaving default file system permissions

```
$ openssl passwd -1 Password1
$ openssl passwd -1 -salt mysalt Password1
```

Documentation may be Wrong!

When setting user passwords programmatically, always use random SALT
Let's investigate passwords, salt and authentication

https://docs.ansible.com/ansible/latest/reference_appendices/faq.html#how-do-i-generate-encrypted-passwords-for-the-user-module

Demo

Documentation may not be Correct

- SALT
- Passwords and Authentication

RELY on YOUR SKILLS

NOT JUST

VENDORS

```
$ ls -l /etc/ssl/certs
```

PKI and Trusted Certificates

When browsing the web, we do not need to trust each web site we visit as we trust certificate issuing authorities as part of the browser or OS. We will see more on PKI later in the course, but for the moment let's locate these certificates

Demo

OpenSSL and Trusted Certifcates

- /etc/ssl/certs

Summary

We have introduced the Linux+ Security course to you:

- During this course we will:
- Manage File Permission
- ACLs
- SELinux
- AppArmor
- Identity Management and Users
- PKI and and Certificate Management
- Host Based Firewalls

Understanding the File Mode (Permissions)