# INTRODUCTION TO LINUX SECURITY

THE LINUX FOUNDATION TRAINING PUBLICATION

**Material From**
**Linux Security (LF416) Linux Training Course**

THE LINUX FOUNDATION

# OVERVIEW

Needless-to-say, having multiple, diverse layers of security is a good idea. It helps protect your network and systems, in the event that there is a failure in one of the layers. The diversity of the layers is also important, as you are only as strong "as your weakest link." If you have multiple layers of the same type of security, a single bug or breach may bypass all of them at once.

Strong logging and auditing will help to mitigate problems when they do occur. Make sure your auditing system has checks and balances to avoid manipulation by an unwanted party. Log to a remote server if possible.

# INTRODUCTION To Linux Security

Given the choice between a protocol which is encrypted, and one that is not, you should choose the encrypted one.

## Principle of Least Access

A common issue facing network security is the failure to follow the "Principle of least privilege." Not everyone needs full super-user access. Limit access using tools such as sudo or su.

## "Confused Deputy" Problem

The "confused deputy" is an example of a privileged escalation attack.

1. A user makes a request to a service on a network or host (the deputy), and specifies an output file they normally wouldn't have access to.
2. The deputy, with it's increased or different access control modifies the file the user wouldn't have been able to modify directly.
3. The user reaps the benefits of whatever the modification was.

## "Mostly Closed" System

Start your security mindset in a "mostly closed" paradigm. Restrict all access, only opening those things which need to be open. This will protect you if you inadvertently enable a service which should not be.

## Use Keys/Tokens Instead of Passwords

Token or key based access is also a better bet than passwords. Passwords are easily guessed, or brute-force attacked. Cryptographically strong keys are less likely to be compromised in that manner.

## Service Practices

- Use encrypted protocols if possible
- Log success AND failure
- Restrict access to users that need it

Given the choice between a protocol which is encrypted, and one that is not, you should choose the encrypted one. It is also a good idea to log not only failures in authentication/ authorization, but to log successes as well. This helps give you a proper audit trail if the "successful" login was an intrusion.

## Demilitarized Zone (DMZ)

A DMZ or "demilitarized zone" is a special-purpose network where business critical servers which need access to a large untrusted network. When setting up a DMZ, proper auditing is also important.

Firewalls can be set between the DMZ and the external "untrusted" network, as well as between the DMZ and the internal "trusted" network. Be aware that hosts can also fall prey to the "confused deputy" problem.

# INTRODUCTION To Linux Security

Awareness is one of the best ways to combat insecurity. Be aware of "phishing" scams or other types of social engineering attacks. Train your users how to avoid falling prey to these attacks.

## Application Security

- No clear-text storage of credentials
- Sanitize input
- Use security frameworks

When designing systems and applications, it is important to keep security front-of-mind. Passwords should never be stored in plain text and should be stored in a one-way hash mechanism.

User input should be sanitized. This will help eliminate the possibility that an external attack can take control of your system. Instead of blindly trusting your SQL or command queries build them as stored procedures or functions which have well controlled options.

Learn and make use of the newer security frameworks. Many people, when they run into an application fighting against something like SELinux, opt to turn it off. A better choice would be to figure out what is causing the error and fix it.

## Security Awareness

- Monitor security lists
- Think like a bad guy
- Distribution errata
- Beware the "layer 8" (human) errors

Awareness is one of the best ways to combat insecurity. Security related mailing lists like CVE (http://cve.mitre.org) and the CERT-Tech Alerts (http://www.us-cert.gov/cas/techalerts), help to inform systems and network admins of current known vulnerabilities.

It also helps to think like a bad guy. Have a non-production lab you attempt to break into, do security drills, use resources like the "hacker's quarterly" (2600 magazine) to see how someone could infiltrate your network. And never underestimate the power of human nature. Be aware of "phishing" scams or other types of social engineering attacks. Train your users how to avoid falling prey to these attacks.

## Network Inspection

For tools that help secure your network, consider the following tools:

- A port scanner used for detecting open or listening network ports remotely
- Tools which listen to traffic "on the wire" to help diagnose network issues.
- Network-based intrusion detection system (IDS) that listens on the network for traffic signatures of known exploits.
- Host-based intrusion detection systems that keep a database of your system state and alerts if it changes without your knowledge.

# INTRODUCTION To Linux Security

A good network design combines a front-end firewall (either software or hardware appliance), as well as per-host firewalls.

## Firewalls

Network firewalls provide protection to your server from the outside world. They can be implemented as a service running on your server (Netfilter). Network firewalls can also be implemented as an appliance built with specialized hardware.

A good network design combines a front-end firewall (either software or hardware appliance), as well as per-host firewalls. The important part of creating these layers is to keep them complex enough to protect without being burdensome to configure/change.

Tcpwrappers is an application-layer firewall which started as an ACL system for the inet daemon. Now, any tool which links against the libwrap library can have an application-layer firewall.

Netfilter, via the iptables interface, is a software based network firewall which exists in the Linux kernel.

## Application Access Control

- Secure your apps
- Pluggable Authentication Modules (PAM)
- Use jail roots (chroot)

Applications themselves also have security tools in the form of ACLs or configuration options. Certain daemons can also make use of the knowledge of a given protocol to block only parts of it. For example, the Apache daemon can block per-method access to the web server (denying POST). The Linux system uses a framework for authentication called PAM.

## Chroot

The chroot() system call, and the chroot command, will change the apparent root directory of a process. The root user is the only user allowed to make the chroot() system call. Chroot “Jails”, as the new root environments are called can then be used for many purposes:

- Building software – Eliminates dependency poisoning, every build can have the exact needed dependencies
- Securing network daemons – Suspect system daemons can be run in a “jail”, thus limiting damage any security breach may cause
- Testing software – Installing and testing software in a “jail” will protect the parent system from the outcome of bugs

# WHY TRAIN WITH THE LINUX FOUNDATION

We needed someone who could fully engage with Ph.D.-level developers. We had no doubt that we'd found the right instructors.

Dana Krokosky, *Compunetix*

The willingness of the Linux Foundation to customize the course to our needs was the biggest determining factor for choosing them.

Matthew Cheng, *Broadcom*

The Linux Foundation really had the best credibility out there, and they were flexible and tailored the class to what I needed for my developers.

Paul Beer, *Optelian*

The Linux Foundation's system administration courses that cover Linux security:

### Linux Security

Learn to assess security risks in your enterprise Linux environment, apply techniques and use tools to increase security, deploy monitoring and attack detection tools, gain visibility into possible vulnerabilities and develop your Linux security policy and response strategy.

### Linux Network Management

This course will teach you how to design, deploy and maintain a network running under Linux and to administer the network services most commonly found in enterprise environments.

### Linux System Administration

This course helps you discover the tools used by system administrators in enterprise Linux environments, install new systems with a variety of Linux distributions and configure systems with new hardware and software combinations

### Additional Sysadmin Training Courses

The Linux Foundation offers a full selection of Linux training courses for developers, including courses that focus on Device Drivers, Kernel Internals & Debugging, and Developing Applications. See a Complete List of Sysadmin Courses.

## Distribution-Flexible

The Linux Foundation's courses are built to be distribution-flexible, allowing companies or students to easily use any of the big three distribution families: Red Hat/Fedora, Ubuntu/Debian, SUSE/OpenSUSE. If your company runs one of these Linux distributions and needs an instructor who can speak deeply on it, we have a Linux expert who knows your distribution well and is comfortable using it as the basis for any corporate Linux training. For our open enrollment students who take our online training or classroom training, our goal is to help them, first and foremost, to become Linux professionals, rather than focusing on how to use one particular set of tools.

## Technically-Advanced

The Linux Foundation's training program has a clear advantage. As the company that employs Linux founder Linus Torvalds, we are fortunate in our ability to leverage close relationships with many of the top members of the Linux community, including Linux kernel maintainers. This led to the most comprehensive Linux training on the market, delivered through rigorous five-day courses taught by Linux experts who bring their real world experiences to every class.

Since Linux is always evolving, our course materials are regularly refreshed and up-to-date with stable versions of the Linux kernel. We deliver our advanced Linux training in a 50/50 training format, where 50 percent of a student's time is spent learning from an instructor and the other 50 percent doing exercises in hands-on learning labs.

For more information about our Linux training, please visit **training.linuxfoundation.org** and contact us today.