Section Overview

What You Will Learn

- Linux security features.
- The superuser.
- Why Linux is avoided by many attackers.
- Open source and security.
- Software management.
- User and administrator roles and responsibilities.

What You Will Learn

- Security Principles
- Software and services
- Encryption
- Accounts
- Multi-factor authentication
- Principle of Least Privilege

Is Linux Secure?

Is Linux Secure?

- Nothing is perfectly secure.
- Security is a series of trade-offs.
  - convenience vs security
    - No passwords = easy to use, not secure.
    - System powered off = secure, not usable.

Risk Assessment

- What is the severity of the risk?
- What is the probability of the risk occurring?
- What is the cost to mitigate the risk?
- What is the effectiveness of the countermeasure?

Linux is only as secure as you make it!

- Linux can be configured to be unsecure.
- Users may employ lax file permissions.
- System administration mistakes.
- Users could use easy to guess passwords.

Linux is only as secure as you make it!

- Data transmitted in the clear.
- Malicious software installed on the system.
- Lack of training or security awareness.

It’s a trap!

- Just because you are using Linux, doesn’t mean you are “secure.”
- Security is an ongoing process.
- Stay vigilant!

What Makes Linux Secure?

Multiuser System

- Linux is a multiuser system.
- The superuser is the root account.
  - root is all powerful.
  - Required to install system-wide software, configure networking, manager users, etc.
- All other accounts are “normal” accounts.
  - Can be used by people or applications (services).

Advantages to a Multiuser System.

- File permissions.
- Every file has an owner.
- Permissions can be granted to other accounts and users as needed.
- Breaking into one account does not necessarily compromise the entire system.

Advantages to a Multiuser System.

- Process permissions.
- Every process has an owner.
- Each account can manage *their* processes.
  - * root can do anything.
- Breaking into one account does not necessarily compromise the entire system.

Attackers Are "Lazy"

- More Windows computers than Linux.
- Linux user base is technical.
- Windows is an easier target.

Linux is Open Source

- You don’t have to trust one company.
- Practically impossible to sneak malicious code into the Linux Kernel.
- Open source increases the discovery of security holes.
- Windows is a black box.

Centralized Software Management

- Packages are managed by package managers.
- Linux distros provide package repositories.
- Most OS software is open source.
- Easy to keep up with security updates.
- When updating, you can update everything.

Linux vs Windows Software Installation

- Linux
  - Search the repository and install with the package manager.

Linux vs Windows Software Installation

- Linux
  - Search the repository and install with the package manager.
- Windows
  - search the Internet and install from a third party.
  - untested software.
  - closed source, most likely.
  - you may not know what you're going to get.

Linux is not immune!

Security Guidelines

Minimize Software and Services

- If you don’t need a piece of software, don’t install it.
- If you don’t need a service, don’t start it.
- If you no longer need the software or service, stop and uninstall it.

Run Services on Separate Systems

- Minimizes the risk of one compromised service leading to other compromised services.

Encrypt Data Transmissions

- Protect against eavesdropping and man-in-the middle attacks.
- Examples:
  - FTP -> SFTP
  - telnet -> SSH
  - SNMP v1/v2 -> SNMP v3
  - HTTP -> HTTPS

Avoid Shared Accounts

- Each person should have their own account.
- Each service should have its own account.
- Shared accounts make security auditing difficult.
- Lack of accountability with shared accounts.

Avoid Direct `root` Logins

- Do not allow direct login of shared accounts.
- Users must login to their personal accounts and then switch to the shared account.
- Control and monitor access with sudo.

Maintain Accounts

- Create and use a process for removing access.

Use Multifactor Authentication

- Something you know + something you have or something you are.
- Examples:
  - account password + phone to receive the one time password (OTP).
  - account password + fingerprint

The Principle of Least Privilege

- AKA, the Principle of Least Authority.
- Examples:
  - Only use root privileges when required.
  - Avoid running services as the root user.
  - Use restrictive permissions that allow people and services enough access to do their jobs.

Monitor System Activity

- Routinely review logs.
- Send logs to a central logging system.

Use a Firewall

- Linux has a built-in firewall. Netfilters + iptables.
- Only allow network connections from desired sources.

Encrypt Your Data

- Encryption protects your data while it is “at rest” (on disk).

Section Summary

Summary

- Linux is “secure,” but it’s not a panacea.
- People play a key role in security.
- Security is an ongoing process.

Summary

- Linux security features
  - Open source.
  - It’s not a popular target.
  - Package management.
  - Separation of privileges (multiuser system).

Summary

- Security Principles
  - Principle of Least Privilege
  - Use encryption
  - Shared accounts (Yes, root can be a shared account!)
  - Multifactor authentication
  - Firewall
  - Monitoring logs