15.12.1 Security Best Practices

Click one of the buttons to take you to that part of the video.

Security Best Practices 0:00-0:11

There are several common-sense things you can do to make your Linux system more secure. In this lesson, we'll talk about a few best practices concerning security in a Linux environment.

Basic Pointers 0:12-1:04

Let's start with some basic pointers. USB storage devices can be an entry point for unwanted files, malicious scripts, and other software to enter a system. You should discourage users from using USB storage devices. Additionally, you can disable USB storage support by removing the storage driver.

Disk encryption is also an effective security practice. Linux Unified Key Setup (LUKS) is an open-source disk encryption software. It requires a user to enter a password to access data on a disk.

Often, when Linux is installed, an independent partition is added for user data. This keeps the operating system files separated from user data. If the user data partition inadvertently fills up, the Linux system can continue to operate while you consider how to increase user data storage or free up storage by moving or deleting user files. I strongly recommend storing user data on a separate partition if you aren't doing that already.

Boot Security and Banners 1:05-2:02

A computer's BIOS or UEFI can be configured to require a user to enter a password before it will boot an operating system. This is only a minor deterrent, since you can reset the BIOS or UEFI by removing the motherboard battery, but it can be part of a good security plan.

There's another level of passwords that can be set in a bootloader, such as GRUB. These passwords help prevent others from booting to Linux and entering single user mode.

Anyone that has physical access to the keyboard can type Ctrl+Alt+Delete to reboot the server without having to log on. It's a good practice to disable this key combination. Doing so also prevents accidental reboots.

A login banner or message-of-the-day (MOTD) is a message that's presented when a user first connects to a Linux machine. A banner that states that only authorized users are allowed might not deter malicious users, but the banner is also there for legal and privacy reasons. The banner should also inform the user that their actions on the system may be monitored.

Multifactor Authentication 2:03-2:46

Authentication is a major concern in the security world. A weak authentication strategy can leave your Linux system vulnerable. An overly complicated strategy may drive your users to find unsecure workarounds, like hiding their password in a desk drawer.

Multifactor authentication adds an extra layer of security to user logins. In the past, only one factor was used to authenticate a user. The user presented something they knew, like a password. Today, good authentication methods use more than one factor. Other factors might include something the user possesses, like a fob or card, or something that the user is, like a fingerprint or iris pattern. Increasingly popular is a one-time-password (OTP) that's delivered to the user via text message or email.

Authentication Technologies 2:47-3:44

Once a user has authenticated and logged into a Linux system, there are several technologies and protocols that allow the user to access other resources beyond the local computer. These include RADIUS, TACACS+, LDAP, and Kerberos.

RADIUS, the remote authentication dial-in user service, provides centralized authentication. A RADIUS server can act as a proxy client to other kinds of authentication servers. TACACS+, (the terminal access controller access-control system plus protocol), is similar to RADIUS.

With Lightweight Directory Access Protocol, or LDAP, the user authenticates to an LDAP server to access directory information about users, computers, and services in a network.

The Kerberos protocol is based on tickets that allow nodes communicating over a non-secure network to prove their identity. The kinit shell command authenticates with a Kerberos server, and the klist command lists the Kerberos tickets held in a credentials cache.

PKI and SSH 3:45-4:39

Another authentication best practice is the use of public key infrastructure (PKI). PKI has all the hardware, software, and people necessary to support the creation and distribution of digital certificates. You will need these certificates to enable SSL and TLS cryptographic security protocols to secure communication.

One of the benefits of using PKI is that you can set up password-less SSH logins by distributing a server SSH certificate.

And, speaking of SSH, it's important that you disable root login via SSH. This is usually the configuration when SSH is first installed.

Another technique to secure SSH is to chroot jail the SSH service. You can also do this with other services. The chroot jail notion uses the chroot command to remap the root directory to include only certain directories and files. This makes it harder for malicious users to gain access to other sensitive information.

Services and Ports 4:40-5:28

Services can become unsecure when there's weak or nonexistent authentication or encryption. This also happens when services run as root. Be sure to use safe authentication methods and encryption, especially when dealing with sensitive information.

Protocols define basic rules for exchanging information, and they can become unsecure too. Older protocols may lack encryption, making it easy to sniff credentials on the network. Some of these protocols are FTP, HTTP, IMAP, Telnet, Finger, Sendmail, and Postfix. Avoid using these protocols for services that share sensitive data. Also, if you find a service is not being used or is vulnerable, consider disabling or uninstalling it.

To increase security, you can change the default TCP and UDP ports for commonly used services and applications.

Linux Monitoring 5:29-6:20

Another vulnerability is the use of the cron and at commands. Malware often uses these utilities to make sure malicious code persists even after it's been removed. Normally, these commands are only available to Linux administrators. You should monitor your cron and at jobs and consider restricting access to these commands.

You can also enable auditd to monitor log files and audit access to system files, directories, and resources. The auditd utility can also monitor application misconducts or code malfunctions. You can configure a set of rules to ensure any security policy violation is addressed.

Finally, you should also monitor the CVE (common vulnerabilities and exposures) system, which is maintained by the US government. It's a reference for publicly known security vulnerabilities. There are applications and scripts that can automate this task and make recommendations to mitigate vulnerabilities.

Summary 6:21-6:38

And that's it for this video. In this lesson, we talked about security best practices in a Linux environment. We covered some basic pointers and security practices during boot and login. We discussed multifactor authentication and authentication technologies. We talked about PKI, SSH, and security practices involving services and ports. And we ended with Linux monitoring best practices.
