15.12 Security Best Practices

As you study this section, answer the following questions:

- What security best practices can be followed to secure data on a disk drive?
- What are the benefits of UEFI/BIOS passwords and bootloader passwords?
- Why is it a good practice to use a message-of-the-day login banner?
- What is multifactor authentication?
- How can a Linux system use public key infrastructure (PKI)?
- What can be done to make the cron and at utilities more secure?
- How can monitoring the common vulnerabilities and exposures (CVE) system assist in making a Linux system more secure?

Key terms for this section include the following:

Term	Definition
Disk encryption	A technique that requires a user to enter a password to access decrypted data from a disk drive.
Bootloader password	A password that prevents attackers from using the bootloader to boot Linux into the insecure single user mode.
Message-of-the-day (MOTD)	A message that's presented when a user first connects to a Linux machine.
Public key infrastructure (PKI)	The hardware, software, and people necessary to support the creation and distribution of digital certificates.
chroot jail	A technique used with the **chroot** command to remap the root directory to include only certain directories and files.
Common vulnerabilities and exposures (CVE)	A database of publicly known security vulnerabilities maintained by the US government.

This section helps you prepare for the following certification exam objectives:

Exam	Objective

CompTIA Linux+	3.3 Summarize security best practices in a Linux environment.
	• Boot security
	  ◦ Boot loader password
	  ◦ UEFI/BIOS password
	• Additional authentication methods
	  ◦ Multifactor authentication
	  ▪ Tokens

- (i) Hardware
- (ii) Software
- OTP
- Biometrics
- RADIUS
- TACACS+
- LDAP
- Kerberos
- kinit
- klist

- Importance of disabling root login via SSH
- Password-less login
  - Enforce use of PKI
- Chroot jail services
- No shared IDs
- Importance of denying hosts
- Separation of OS data from application data
  - Disk partition to maximize system availability
- Change default ports
- Importance of disabling or uninstalling unused and unsecure services
  - FTP
  - Telnet
  - Finger
  - Sendmail
  - Postfix
- Importance of enabling SSL/TLS
- Importance of enabling auditd
- CVE monitoring
- Discouraging use of USB devices
- Disk encryption
  - LUKS
- Restrict cron access
- Disable Ctrl+Alt+Del
- Add banner
- MOTD