Linux Security

This intermediate Linux security training covers key concepts for securing Linux systems, focusing on CompTIA Linux+ exam objectives. You'll learn about PAM configuration, SSH key management, file permissions, multi-factor authentication (MFA), firewalls, and encryption. This Linux training can be used for XK0-005 exam prep, or as a Linux resource for systems engineers.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Understand Cryptography and Certificates — 66 min.

Introduction	1
Asymmetric and Symmetric Encryption	1
Working with Encryption	1
Digital Signatures and Hashing	1
Understanding SSL and TLS	1
Understanding Self-Signed Certificates	1

Understand Authentication

Overview	1
Introduction	1
Understanding PAM	1
Common PAM Modules	1
LDAP	1
AAA Servers	1
Tokens	1
MFA, SSO & SSSD	1

Harden Linux Systems

Overview	1
Introduction	1
Security Scanning	1
Insecure Protocols and Secure Boot	1
Enforcing Strong Passwords	1
Harden Kernel Parameters	1
Service Accounts and Unused Packages	1

Implement Identity Management

Overview	1
Introduction	1
Creating and Deleting Users	1
User Modification	1
Groups	1
Modifying Identity Management Files	1
Viewing Account Information	1
Shell Configurations	1

Configure Firewalls

Overview	1
Introduction	1
Understanding iptables	1
Configuring iptables	1
Working with firewalld	1
Exploring ufw & nftables	1

Configure and Execute Remote Connectivity

Overview	1
Introduction	1
Configuring SSH Servers	1
Configuring SSH Clients	1
Authenticating with Keys	1
SSH Tunneling	1
Elevated Privileges	1

Understand Security-Enhanced Linux & Access Control

Overview	1
Introduction	1
Understanding Attributes	1
The Append Attribute	1
Access Control Lists	1
Understanding SELinux	1
Managing SELinux Contexts and Booleans	1
AppArmor	1

Understand Permissions

Overview	1
Introduction	1
Owners, Groups and Others	1
Symbolic Notation	1
Octal Notation	1
SUID and SGID	1
The Sticky Bit	1
The Umask Command	1