Linux Networking Fundamentals

Course Number: WA3630

Duration: 3 days

Course Description

This Linux Networking course focuses on understanding, configuring, and managing Linux networking. Participants learn foundational concepts, advanced configurations, and troubleshooting techniques to manage network operations effectively.

Skills Gained

- Understand Linux networking fundamentals, including interfaces, IP addressing, and routing.
- Configure and manage networking services like DHCP, DNS, and firewalls.
- Analyze and troubleshoot networking issues using Linux tools.
- Secure Linux-based networks against common threats.
- Implement advanced networking techniques, including VLANs, bonding, bridging, and VPNs.

Prerequisites

Students must have taken Linux System Administration or have equivalent experience.

Course Details

Introduction to Networking Concepts

- Overview of the OSI Model
- Understanding TCP/IP and its Components
- Networking Protocols in Linux

Linux Networking Basics

- Understanding Network Interfaces
- Tools for Managing Network Interfaces
- Configuring Static and Dynamic IPs
- Basics of Subnetting and CIDR Notation
- Setting Up Hostnames and Editing

Routing and ARP

- Default Gateways and Static Routes
- Viewing and Managing the Routing Table (route, ip route)
- Understanding ARP and using arp and ip neigh

Configuring Networking Services

- Setting Up a DHCP Server with isc-dhcp-server
- Configuring a Local DNS Server with bind9
- Introduction to Web Servers (Apache/Nginx Basics) for Testing

Firewall Configuration and NAT

- Introduction to Firewalls: iptables vs nftables
- Creating Basic Firewall Rules (Allow/Deny Traffic)
- Configuring Network Address Translation (NAT)
- Port Forwarding Examples

Networking Tools for Analysis and Monitoring

- Packet Sniffing and Analysis with tcpdump and Wireshark
- Monitoring Network Traffic with iftop, iptraf, and nload
- Using netstat and ss for Active Connection Tracking

Advanced Networking Techniques

- Setting Up VLANs with vconfig or ip link
- Network Bonding for Redundancy (mode 0 vs mode 1)
- Configuring Network Bridges for Virtual Machines
- Deploying VPNs with OpenVPN and WireGuard

Securing Linux Networks

- Hardening SSH
- Protecting Against Brute-Force Attacks

- Using tcp_wrappers and ufw for Service-Specific Restrictions
- DoS/DDoS Prevention (Rate Limiting with iptables)

Troubleshooting Linux Networks

- Diagnosing Connection Issues (ping, traceroute, mtr)
- Debugging DNS Problems (dig, nslookup)
- Checking Interface and Link Status (ethtool, ip link)
- Comprehensive System Logs Analysis

Conclusion