INFOSOFT IT SOLUTIONS

Training | Projects | Placements

Revathi Apartments, Ameerpet, 1st Floor, Opposite Annapurna Block,
Infosoft It solutions, Software Training & Development Institute, 9059683947|9182540872

Linux Security Fundamentals

Introduction to Linux Security

- Overview of Linux Security: Importance and key principles
- Understanding Threats: Common security threats and vulnerabilities
- Security Layers: Defense in depth approach

Linux Security Basics

- User and Group Management: User permissions, sudo usage
- File System Security: File permissions (chmod, chown), Access Control Lists (ACLs)
- Service Management: Securing network services (SSH, Apache, FTP)

Linux Security Hardening

- System Hardening Techniques: Disabling unnecessary services, kernel hardening
- Securing Configuration Files: Managing configuration files securely
- Using Firewalls: iptables and firewalld basics, configuring firewall rules

Authentication and Access Control

- Password Policies: Implementing strong password policies
- SSH Security: Configuring SSH keys, disabling root login

- PAM (Pluggable Authentication Modules): Overview and configuration

Linux Auditing and Monitoring

- Linux Audit Framework: Auditing system events and logs
- Monitoring Tools: Using tools like syslog, auditd, and logwatch
- Intrusion Detection Systems (IDS): Implementing and configuring IDS on Linux

Cryptography in Linux

- Introduction to Cryptography: Symmetric vs. asymmetric encryption
- Using GPG (GNU Privacy Guard): Encrypting files and communications
- SSL/TLS Certificates: Managing and securing web services with certificates

Network Security in Linux

- Network Configuration: Securing network interfaces and IPtables
- VPN (Virtual Private Network): Implementing VPN solutions on Linux
- DNS Security: Securing DNS servers and configurations

Linux Malware Detection and Prevention

- Understanding Malware Threats: Types of malware affecting Linux
- Antivirus Solutions for Linux: Implementing and configuring antivirus software
- Malware Prevention Best Practices

Incident Response and Forensics

- Incident Response Plan: Developing and implementing a response plan
- Forensics Basics: Collecting and analyzing evidence

- Recovering from Security Incidents: Steps to recover from breaches

Linux Security Tools

- Vulnerability Assessment Tools: Using tools like Nessus, OpenVAS
- Security Scanning Tools: Nmap, Nikto for scanning vulnerabilities
- Security Information and Event Management (SIEM): Implementing SIEM solutions

Secure Software Development in Linux

- Secure Coding Practices: Writing secure scripts and applications
- Code Review and Testing: Importance of code review and testing
- Secure Software Deployment: Best practices for deploying applications securely

Linux Security Best Practices

- Continuous Security Monitoring: Implementing continuous security monitoring practices
- Patch Management: Importance of timely updates and patching
- Security Compliance: Ensuring compliance with standards and regulations

Ethical Hacking and Penetration Testing

- Introduction to Ethical Hacking: Understanding penetration testing
- Conducting Penetration Tests: Techniques and methodologies
- Reporting and Mitigating Vulnerabilities

Linux Security Case Studies and Projects

- Real-world Case Studies: Analyzing security incidents and solutions
- Hands-on Projects: Implementing security measures on Linux systems
- Presentation and Documentation of Security Projects