

# Securing Linux systems

A 5 day **Hands on** training course



## Description

This course teaches you everything you need to know to build a safe Linux environment. The first section handles cryptography and authentication with certificates, openssl, mod\_ssl, DNSSEC and filesystem encryption. Then Host security and hardening is covered with intrusion detection, and also user management and authentication. Filesystem Access control is then covered. Finally network security is covered with network hardening, packet filtering and VPNs.



## Key outcomes

By the end of the course delegates will be able to:

- ✓ Secure Linux accounts.
- ✓ Secure Linux file systems.
- ✓ Secure Linux access through the network.



## Training Approach

This structured course uses Instructor Led Training to provide the best possible learning experience. Small class sizes ensure students benefit from our engaging and interactive style of teaching with delegates encouraged to ask questions throughout the course. Quizzes follow each major section allowing checking of learning. Hands on sessions are used throughout to allow delegates to consolidate their new skills.



## Details

### Who will benefit?

Linux technical staff needing to secure their systems.

### Prerequisites

Linux system administration (LPIC-1)

**Duration:** 5 days

**Customer rating:** ★★★★★

### Generic Training



Generic training compliments product specific courses covering the complete picture of all relevant devices including the protocols "on the wire".

*"Friendly environment with expert teaching that teaches the why before the how."*  
G.C. Fasthosts

### Small Class Sizes



We limit our maximum class size to 8 delegates; often we have less than this. This ensures optimal interactivity between delegates and instructor.

*"Excellent course. The small class size was a great benefit..."*  
M.B. IBM

### Hands On Training



The majority of our courses use hands on sessions to reinforce the theory.

*"Not many courses have practice added to it. Normally just the theoretical stuff is covered."*  
J.W. Vodafone

### Our Courseware



We write our own courses; courseware does not just consist of slides and our slides are diagrams not bullet point text.

*"Comprehensive materials that made the course easy to follow and will be used as a reference point."*  
V.B. Rockwell Collins

### Customise Your Course



Please contact us if you would like a course to be customised to meet your specific requirements. Have the course your way.

*"I was very impressed by the combination of practical and theory. Very informative. Friendly approachable environment, lots of hands on."*  
S.R. Qinetiq

# Securing Linux systems

## Course Content

### Cryptography

#### Certificates and Public Key Infrastructures

X.509 certificates, lifecycle, fields and certificate extensions. Trust chains and PKI. openssl. Public and private keys. Certification authority. Manage server and client certificates. Revoke certificates and CAs.

#### Encryption, signing and authentication

SSL, TLS, protocol versions. Transport layer security threats, e.g. MITM. Apache HTTPD with mod\_ssl for HTTPS service, including SNI and HSTS. HTTPD with mod\_ssl to authenticate users using certificates. HTTPD with mod\_ssl to provide OCSP stapling. Use OpenSSL for SSL/TLS client and server tests.

#### Encrypted File Systems

Block device and file system encryption. dm-crypt with LUKS to encrypt block devices. eCryptfs to encrypt file systems, including home directories and, PAM integration, plain dm-crypt and EncFS.

#### DNS and cryptography

DNSSEC and DANE. BIND as an authoritative name server serving DNSSEC secured zones. BIND as an recursive name server that performs DNSSEC validation, KSK, ZSK, Key Tag, Key generation, key storage, key management and key rollover, Maintenance and re-signing of zones, Use DANE. TSIG.

### Host Security

#### Host Hardening

BIOS and boot loader (GRUB 2) security. Disable useless software and services, systemctl for security related kernel configuration, particularly ASLR, Exec-Shield and IP / ICMP configuration, Exec-Shield and IP / ICMP configuration, Limit resource usage. Work with chroot environments, Security advantages of virtualization.

#### Host Intrusion Detection

The Linux Audit system, chkrootkit, rkhunter, including updates, Linux Malware Detect, Automate host scans using cron, AIDE, including rule management, OpenSCAP.

### User Management and Authentication

NSS and PAM, Enforce password policies. Lock accounts automatically after failed login attempts, SSSD, Configure NSS and PAM for use with SSSD, SSSD authentication against Active Directory, IPA, LDAP, Kerberos and local domains, Kerberos and local domains, Kerberos tickets.

#### FreeIPA Installation and Samba Integration

FreeIPA, architecture and components. Install and manage a FreeIPA server and domain, Active Directory replication and Kerberos cross-realm trusts, sudo, autofs, SSH and SELinux integration in FreeIPA.

### Access Control

#### Discretionary Access Control

File ownership and permissions, SUID, SGID. Access control lists, extended attributes and attribute classes.

#### Mandatory Access Control

TE, RBAC, MAC, DAC. SELinux, AppArmor and Smack.

#### Network File Systems

NFSv4 security issues and improvements, NFSv4 server and clients, NFSv4 authentication mechanisms (LIPKEY, SPKM, Kerberos), NFSv4 pseudo file system, NFSv4 ACLs. CIFS clients, CIFS Linux Extensions, CIFS security modes (NTLM, Kerberos), mapping and handling of CIFS ACLs and SIDs in a Linux system.

### Network Security

#### Network Hardening

FreeRADIUS, nmap, scan methods. Wireshark, filters and statistics. Rogue router advertisements and DHCP messages.

#### Network Intrusion Detection

ntop, Cacti, bandwidth usage monitoring, Snort, rule management, OpenVAS, NASL.

#### Packet Filtering

Firewall architectures, DMZ, netfilter, iptables and ip6tables, standard modules, tests and targets. IPv4 and IPv6 packet filtering. Connection tracking, NAT. IP sets and netfilter rules, nftables and nft. ebtables. conntrackd

#### Virtual Private Networks

OpenVPN server and clients for both bridged and routed VPN networks. IPsec server and clients for routed VPN networks using IPsec-Tools / racoon. L2TP.

