Linux-Sicherheit

Linux hat einen sehr guten Ruf als sicheres und effizientes Betriebssystem. Deswegen ist es ein unverzichtbarer Baustein im Aufbau sicherer Gesamtsysteme. Dieser Kurs vermittelt fundiertes Wissen über den Einsatz verschiedener Sicherheitstechniken auf der Basis von Linux, etwa die Konfiguration und den Betrieb von Linux-Systemen als Firewalls und Router oder die Secure Shell. Ferner geht er im Detail auf Techniken ein, mit denen Sie Linux-Systeme selbst sichern können, die zum Beispiel als Web- oder Mailserver fungieren. Sie lernen außerdem die Grundzüge des Umgangs mit Einbruchs-Erkennungssystemen wie Snort und Sicherheitsscannern wie OpenVAS.

Kursinhalt
- Sicherheit: Einführung
- Lokale Sicherheit
- Abhörsicherer Shellzugriff mit OpenSSH
- Serverdienste sichern
- Firewall-Konzepte
- Paketfilter mit Netfilter (»iptables«)
- Sicherheit im lokalen Netz
- Sicherheitsanalyse
- Rechnerbasierte Angriffserkennung
- Netzbasierte Angriffserkennung

Verwendet werden deutschsprachige Unterlagen.

Zielgruppe
Dieser Kurs richtet sich an Planer und Betreiber von Netzwerken sowie Systemadministratoren, die eingehende Kenntnisse zu Sicherheitsproblemen in IP-Netzen und deren Lösung auf Linux-Basis erwerben möchten.

Voraussetzungen
Zum Verständnis der Themengebiete tragen fundiertes Basiswissen im Umgang mit der Netzwerk-Terminologie sowie tiefergehende Protokollkenntnisse der TCP/IP-Welt bei. Erfahrungen mit der grundlegenden Administration von Linux-Maschinen sind ebenfalls notwendig.

Dieser Kurs im Web
Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.at/go/**LISU**

Vormerkung
Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine
Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert
Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.
Termine in Deutschland	**3 Tage**	**€ 1.995,-**
Online Training	**3 Tage**	**€ 1.995,-**

Termin/Kursort — Kurssprache Deutsch

10.11.-12.11.25 München 10.11.-12.11.25 Online

Stand 07.05.2025

Inhaltsverzeichnis

Linux-Sicherheit

1 Sicherheit: Einführung
1.1 Was ist Sicherheit?
1.2 Sicherheit als betriebswirtschaftliches Problem
1.3 Angriffe
1.4 Angreifer
1.5 Sicherheitskonzepte
1.5.1 Warum?
1.5.2 Risikoanalyse
1.5.3 Kosten-Nutzen-Analyse
1.5.4 Sicherheitsziele, Richtlinien und Empfehlungen
1.5.5 Audits
1.6 Sicherheit und Open-Source-Software
1.7 Informationsquellen

2 Lokale Sicherheit
2.1 Physische Sicherheit
2.1.1 Physische Sicherheit – warum?
2.1.2 Planung
2.1.3 Risiken
2.1.4 Diebstahl
2.1.5 Alte Medien
2.2 Minimalsysteme
2.3 Den Bootvorgang sichern
2.3.1 Bootvorgang und BIOS
2.4 Bootlader-Sicherheit
2.4.1 Grundsätzliches
2.4.2 GRUB 2
2.4.3 GRUB Legacy
2.4.4 LILO

3 Die Secure Shell (für Fortgeschrittene)
3.1 Einführung
3.2 Grundlegende Funktionalität
3.3 Benutzer-Beschränkungen
3.4 Tipps und Tricks
3.4.1 Benutzer-Konfiguration für verschiedene Server
3.4.2 Feinheiten des Protokolls
3.4.3 Netz und doppelter Boden
3.4.4 Spaß mit öffentlichen Schlüsseln
3.5 OpenSSH-Zertifikate
3.5.1 Überblick
3.5.2 Benutzer-Schlüssel beglaubigen
3.5.3 OpenSSH-Zertifikate für Benutzer verwenden
3.5.4 Rechner-Schlüssel und -Zertifikate

4 Firewall-Konzepte
4.1 Firewalls und Sicherheit
4.2 Firewall-Bestandteile
4.3 Implementierung von Firewalls
4.3.1 Ein einfaches Beispiel: Heim-LAN
4.3.2 Ein Heim-LAN mit Router
4.3.3 Internet-Anbindung einer Firma mit DMZ
4.3.4 DMZ für Arme: Triple-Homed Host
4.4 Firewalls und gängige Protokolle

5 Paketfilter mit Netfilter (»iptables«)
5.1 Sinn und Zweck von Paketfiltern
5.2 Der Paketfilter in Linux-Systemen
5.2.1 Konzeption
5.2.2 Arbeitsweise
5.2.3 Einbindung im Kernel
5.3 Das Kommandozeilenwerkzeug iptables
5.3.1 Grundlagen
5.3.2 Erweiterungen
5.3.3 Festlegung der Aktion
5.3.4 Operationen auf eine komplette Kette
5.3.5 Sichern der Filterregeln
5.3.6 PraxisbeispieL
5.4 Adressumsetzung (Network Address Translation)
5.4.1 Anwendungsfälle für NAT
5.4.2 Varianten von NAT
5.4.3 NAT per Netfilter
5.4.4 Besonderheiten von NAT

6 Sicherheitsanalyse
6.1 Einleitung
6.2 Netzanalyse mit nmap
6.2.1 Grundlagen
6.2.2 Syntax und Optionen
6.2.3 Beispiele
6.3 Der Sicherheitsscanner OpenVAS
6.3.1 Einleitung
6.3.2 Struktur
6.3.3 OpenVAS benutzen

7 Rechnerbasierte Angriffserkennung
7.1 Einleitung
7.2 Tripwire
7.2.1 Aufbau
7.2.2 Vorbereitende Arbeiten
7.2.3 Regel-Betrieb
7.2.4 Festlegung der Überwachungsrichtlinien
7.3 AIDE
7.3.1 Einleitung
7.3.2 Arbeitsmodi von AIDE
7.3.3 Konfiguration von AIDE
7.3.4 Beispielkonfiguration von AIDE

8 Netzbasierte Angriffserkennung
8.1 Einleitung
8.2 Portscans erkennen – scanlogd
8.3 Angreifer aussperren – fail2ban
8.3.1 Überblick
8.3.2 Struktur
8.4 Snort: Schweinereien in Echtzeit erkennen
8.4.1 Grundlagen
8.4.2 Snort installieren und testen
8.4.3 Snort als IDS

9 Virtuelle private Netze mit OpenVPN
9.1 Warum VPN?
9.2 OpenVPN
9.2.1 Grundlagen
9.2.2 Allgemeine Konfiguration
9.2.3 Einfache Tunnel
9.2.4 OpenVPN mit TLS und X.509-Zertifikaten
9.2.5 Server-Modus

A Musterlösungen

B X.509-Crashkurs
B.1 Einleitung: Kryptografie, Zertifikate und X.509
B.2 Eine Zertifizierungsstelle generieren
B.3 Server-Zertifikate generieren

C Kommando-Index

Index

ExperTeach Training & Consulting GmbH
Handelskai 94-96 · 1200 Wien · Telefon: +43 1 2350 383-0 · Fax: +43 1 2350 383-19 · info@experteach.at · www.experteach.at