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.de/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. 3 Tage € 1.795,-**Termine in Deutschland Online Training** 3 Tage € 1.795,-Termin/Kursort Kurssprache Deutsch 16.09.-18.09.24 Wminchen 16.09.-18.09.24 Minchen 16.09.-18.09.24

Stand 10.03.2024



Inhaltsverzeichnis Linux-Sicherheit

1	Sicherheit: Einführung	4.1	Firewalls und Sicherheit	7.2.4	Festlegung der Überwachungsrichtlinien
1.1	Was ist Sicherheit?	4.2	Firewall-Bestandteile	7.3	AIDE
1.2	Sicherheit als betriebswirtschaftliches Problem	4.3	Implementierung von Firewalls	7.3.1	Einleitung
1.3	Angriffe	4.3.1	Ein einfaches Beispiel: Heim-LAN		Arbeitsmodi von AIDE
1.4	Angreifer	4.3.2	Ein Heim-LAN mit Router	7.3.3	Konfiguration von AIDE
1.5	Sicherheitskonzepte	4.3.3	Internet-Anbindung einer Firma mit DMZ	7.3.4	Beispielkonfiguration von AIDE
1.5.1	Warum?	4.3.4	DMZ für Arme: Triple-Homed Host		
1.5.2	Risikoanalyse	4.4	Firewalls und gängige Protokolle	8	Netzbasierte Angriffserkennung
1.5.3	Kosten-Nutzen-Analyse			8.1	Einleitung
1.5.4	Sicherheitsziele, Richtlinien und Empfehlungen	5	Paketfilter mit Netfilter (»iptables«)	8.2	Portscans erkennen – scanlogd
1.5.5	Audits	5.1	Sinn und Zweck von Paketfiltern	8.3	Angreifer aussperren – fail2ban
1.6	Sicherheit und Open-Source-Software	5.2	Der Paketfilter in Linux-Systemen	8.3.1	Überblick
1.7	Informationsquellen	5.2.1	Konzeption	8.3.2	Struktur
		5.2.2	Arbeitsweise	8.4	Snort: Schweinereien in Echtzeit erkennen
2	Lokale Sicherheit	5.2.3	Einbindung im Kernel	8.4.1	Grundlagen
2.1	Physische Sicherheit	5.3	Das Kommandozeilenwerkzeug iptables	8.4.2	Snort installieren und testen
2.1.1	Physische Sicherheit – warum?	5.3.1	Grundlagen	8.4.3	Snort als IDS
2.1.2	Planung	5.3.2	Erweiterungen		
2.1.3	Risiken	5.3.3	Festlegung der Aktion	9	Virtuelle private Netze mit OpenVPN
2.1.4	Diebstahl	5.3.4	Operationen auf eine komplette Kette	9.1	Warum VPN?
2.1.5	Alte Medien	5.3.5	Sichern der Filterregeln	9.2	OpenVPN
2.2	Minimalsysteme	5.3.6	PraxisbeispieL	9.2.1	Grundlagen
2.3	Den Bootvorgang sichern	5.4	Adressumsetzung (Network Address	9.2.2	Allgemeine Konfiguration
2.3.1	Bootvorgang und BIOS		Translation)	9.2.3	Einfache Tunnel
2.4	Bootlader-Sicherheit	5.4.1	Anwendungsfälle für NAT	9.2.4	OpenVPN mit TLS und X.509-Zertifikaten
2.4.1	Grundsätzliches	5.4.2	Varianten von NAT	9.2.5	Server-Modus
2.4.2	GRUB 2	5.4.3	NAT per Netfilter		
2.4.3	GRUB Legacy	5.4.4	Besonderheiten von NAT	Α	Musterlösungen
2.4.4	LILO				
		6	Sicherheitsanalyse	В	X.509-Crashkurs
3	Die Secure Shell (für Fortgeschrittene)	6.1	Einleitung	B.1	Einleitung: Kryptografie, Zertifikate und X.509
3.1	Einführung	6.2	Netzanalyse mit nmap	B.2	Eine Zertifizierungsstelle generieren
3.2	Grundlegende Funktionalität	6.2.1	Grundlagen	B.3	Server-Zertifikate generieren
3.3	Benutzer-Beschränkungen	6.2.2	Syntax und Optionen		
3.4	Tipps und Tricks	6.2.3	Beispiele	С	Kommando-Index
3.4.1	Benutzer-Konfiguration für verschiedene Server	6.3	Der Sicherheitsscanner OpenVAS		
3.4.2	Feinheiten des Protokolls	6.3.1	Einleitung		Index
3.4.3	Netz und doppelter Boden	6.3.2	Struktur		
3.4.4	Spaß mit öffentlichen Schlüsseln	6.3.3	OpenVAS benutzen		
3.5	OpenSSH-Zertifikate				
3.5.1	Überblick	7	Rechnerbasierte Angriffserkennung		
3.5.2	Benutzer-Schlüssel beglaubigen	7.1	Einleitung		
3.5.3	OpenSSH-Zertifikate für Benutzer verwenden	7.2	Tripwire		
3.5.4	Rechner-Schlüssel und -Zertifikate	7.2.1	Aufbau		
		7.2.2	Vorbereitende Arbeiten		
4	Firewall-Konzepte	7.2.3	Regel-Betrieb		











