

Kurs: Linux/UNIX Security

© T. Birnthaler, H. Gottschalk, OSTC GmbH (www.ostc.de)

(Version 1.4 vom 30.11.2008)

Dauer: 4-5 Tage

Motivation: Das Internet wird immer unsicherer. Mails mit Viren, Trojaner und Würmer sowie Einbruchsversuche sind an der Tagesordnung. Linux/UNIX ist ein prinzipiell sehr sicheres System, das aber entsprechend administriert werden muss, damit diese Sicherheit erhalten bleibt. Die zunehmende Verbreitung von Linux auf kritischen Infrastruktur-Systemen (Web-, Mail-, File & Print-Services) erfordert hier ein systematisches Vorgehen.

Ziel: Sie lernen die grundlegenden Sicherheitsprobleme im Netzwerk (Intranet und Internet) kennen. Der Workshop vermittelt die zur Härtung von Linux-Systemen notwendigen Kenntnisse. Sie werden anschließend in der Lage sein, ihre Linux-basierten Rechner sicher und effizient zu konfigurieren, die Sicherheit bestehender Systeme einzuschätzen und zu verbessern. Anhand vieler praktischer Übungen wird die Absicherung ihres Systems gegen unbefugten Zugriff und das Erkennen von unbefugten Zugriffen geübt.

Inhalt:

- Sicherheitspolitik

- HOST-Sicherheit (Installation eines sicheren Grundsystems)
 - Physikalische Sicherheit
 - Zugangskontrolle
 - Sichere Passwörter
 - Systemhärtung
 - Dateisystem-Struktur
 - Restriktion von Dateisystemen

- Absolut notwendige Module
 - Einspielen und Integritätsprüfung von Patches
- Rechtesystem
 - Benutzer
 - Gruppen
 - Sticky-Recht
 - SUID/SGID-Programme
- Wichtige Systemdienste
 - Logging (syslog, syslog-ng, logrotate)
 - (x)inetd
 - tcpd (TCP Wrapper)
 - sudo
 - chroot
- Kryptografische Grundlagen
 - Historie und Begriffe
 - Symmetrische Verschlüsselung
 - Asymmetrische Verschlüsselung
 - Hybride Verschlüsselung
 - Signaturen
 - Zertifikate
 - SSL/HTTPS/TLS
- Sicherer Remotezugriff
 - Secure Shell (ssh, scp, sftp, OpenSSH)
 - Putty
- Wichtige Dienste
 - Mail
 - DNS
 - Webserver Apache

- Firewall
 - Wichtige TCP/IP-Grundlagen und -Begriffe
 - Grundsätzlicher Aufbau
 - Kritische Ports
 - Paketfilter (iptables)
 - Network Address Translation (NAT, Masquerading, SNAT, DNAT)
 - Proxyserver (Squid, Apache, Mail)
 - Virens Scanner

- Security-Tools
 - Netzwerkmonitoring (netcat, ethereal/wireshark)
 - Portscanner (nmap, saint)

- Intrusion Detection
 - Logdateien-Analyse
 - Tripwire
 - Snort

Schulungsunterlagen:

- Skript
- Lösungsblätter zu allen Übungen
- Zusammenfassung der wichtigsten Linux/UNIX-Befehle
- Zusammenfassung der wichtigsten Vi-Befehle
- Ausführliche Linux/UNIX-Befehlsübersicht

Voraussetzungen:

- Muss: Allgemeine Computer-Kenntnisse (Tastatur, Maus, Grafische Oberfläche, Editor)
- Muss: Allgemeine Netzwerk-Kenntnisse (TCP/IP)
- Muss: Linux/UNIX Grundlagen-Kurs (Shell-Ebene mit Kommando-Zeilen)

- Muss: Linux/UNIX Systemadministration
- Muss: Linux/UNIX Netzwerk-Administration I
- Muss: Kenntnis des Linux/UNIX-Standard-Editors vi
- Optional: Linux/UNIX Netzwerk-Administration II
- Optional: Shell-Programmierung

Abgrenzung:

- Der Kurs erfolgt auf einem eigenhändig installierten System
- Keine grafische Oberfläche (KDE oder GNOME)
- root-Rechte sind häufig notwendig
- Konfigurationsdateien werden häufig editiert (Vi-Kenntnisse!)
- Nur Aufsetzen eines lokalen Paketfilters, keine Einrichtung einer zentralen Firewall