Einleitung

Ausgangsbasis:

- frische Linux-Installation
- nicht an ein Netzwerk angeschlossen

Passwörter sicher wählen

Beispiele für schlechte Passwörter:

- Eigener Name, dazu gehören auch Spitznamen usw.
- Namen von Mitgliedern der eigenen Familie, Freunden
- Geburtsdaten
- Hobbies, Namen des Haustieres, Lieblingsbier usw.

Angriffstechniken auf Passwörter

- Social engineering
- Passwörter knacken mit Tools (z.B.: John the ripper)

Sichere Passwörter:

- für jeden *wichtigen* Account ein anderes Passwort
- kein Wort das in einem Wörterbuch vorkommt
- Sonderzeichen und Zahlen einfügen
- mindestens 6 Zeichen
- auf keinen Fall aufschreiben, außer es wird in sicherer Art verwahrt

Lernhilfen für Passwörter

- mit Mantra einprägen

- Beispiel: D6UZkm2$

  Mantra: Der 6 Uhr Zug kostet mich 2 $

Grundlegende Absicherung

Offener Service = potentieller Angriffspunkt

Häufige Angriffspunkte:

- rpc-Dienste (nfs usw.)
- ftp-Dienste (z.B.: wuftpd)
- lpd (Drucker)

Weitere Probleme:

- DoS (denial of service durch chargen o.ä.)

Abhilfe

- Dienste deaktivieren:
  - /etc/inetd.conf oder /etc/xinetd.conf
  - Startskripte in /etc/init.d
- Zugriff auf die Dienste beschränken
  - /etc/hosts.allow
  - /etc/hosts.deny
- Evtl. Rechner hinter Firewall stellen

Konfiguration

- Konfiguration überprüfen
- Sicherheitsupdates einspielen
- Homepages mit Errata der anderen Hersteller besuchen

Ende der Grundkonfiguration

sicheres Grundsystem erreicht, Grundlage für jedes Sicherheitskonzept

Erst jetzt ans Netz

Sicheres Arbeiten im Netz

Datenströme in Netzwerken sind abhör- und manipulierbar

Sniffer ermöglichen das Abhören des lokalen Netzes

Sniffen: POP3

Beispiel: Das Abrufen von E-Mails

Problem: pop3 ist ein Klartext-Protokoll

--> Sensible Daten wie z.B. Passwörter werden im Klartext übertragen

Konsequenzen: Mails des Opfers abrufbar, löschbar, usw.

Sniffen: telnet

Beispiel: telnet

Problem: telnet wie pop3 Klartextprotokoll

Möglichkeiten des Angreifers:

- Sniffen der Verbindung
- Einfügen von Daten
- übernehmen der Verbindung
- usw.

Abhilfe:

Verwenden sicherer Protokolle

- spop3 statt pop3
- ssh statt telnet

Weitere häufig verwendete unsichere Protokolle und ihr sicherer Ersatz:

- ftp --> sftp
- die r-Dienste --> ssh

Sichere Protokolle: Sicherheit?

Unsicheres Verhalten --> Verkehr wird unsicher

Beispiel ssh:
Wenn der User ausdrückliche Warnungen ignoriert kann
auch ssh so unsicher sein wie telnet

Verantwortung

Mit unsicheren Rechnern schadet man sich nicht nur selbst sondern auch anderen Teilnehmern im Internet.

- Ausgangsbasis für DoS-Attacken
- Ausgangsbasis für weitere Angriffe

Fazit

sicheres Arbeiten in Netzwerken nur durch:

- sichere Ausgangsbasis
- sichere Protokolle
- ein gesunder Schuss Wissen und Paranoia

Schlusswort

Sicherheit ist ein Prozess

Teil dieses Prozesses ist
- Sicherheitsupdates einspielen
- entsprechende Mailinglisten und Webseiten lesen (z.B.: Bugtraq, www.securityfocus.com)