Hilfe, man sieht mein Haus!

Grundsätzliches zur Sicherheit von Linux-Systemen

Philipp Grau
phgrau@Piak.DE

28. September 2002

Notes:

Organisatorisches

- Fragen jederzeit!
- Mobil–Telefone bitte nicht!

Notes:

Ziele

- Grundlagen
- Sicherheit
- Sicherheit testen
- Angriffe und Einbrüche erkennen
- Weiterführende Informationen

Notes:

Fragen

- Wer hat einen Rechner mit Linux?
- Wer hat mehr als einen Rechner (und diese vernetzt)?
- Wer arbeitet beruflich mit Linux?
- Wer hat DSL/Standleitung zu Hause?

Notes:

Grundlagen 1

- IP-Nummer (192.168.192.20)
- Name (tiuri.piak.de)
- Protokoll und Port (http 80, smtp 25)

Notes:

Grundlagen 2

- Client/Server
- Serverdienst
- Internet „Super-Server“: (x)`inetd`
- Standalone Server

Notes:

Server

- Wartet auf bestimmtem Port einer IP-Nummer auf eine Verbindungsaufbau.
- Bearbeitet Anfragen
- Beendet Verbindung
- Wartet auf Verbindungsaufbau

Notes:

Sicherheit

- Warum Sicherheit
- Prozess, Status Quo
- Auch für mich?!

Notes:

Grundsätzliches zur Sicherheit

- Schutz der eigenen Daten (Datenklau, -verfälschung)
- Schutz des eigenen Rechners vor Missbrauch (DoS)
- Schutz des eigenen Netzes (Sicherstellung des Betriebs)
- Schutz fremder Rechner vor eigenem Rechner (Distributed DoS)

Notes:

Schutzmöglichkeiten

- Konfiguration der Software
- Kneifzange
- Firewall
- Paketfilter auf Rechner

Notes:

Software–Konfiguration

- `/etc/inetd.conf` oder `/etc/xinetd.conf`
- `/etc/hosts.allow` für tcpwrappers
- pro Appilkation (`httpd.conf`, `smb.conf`, ...)

Hardware–Konfiguration

- geswitchtes Netzwerk (kann man sniffen?)
- ein Ein- und Ausgang für Netzwerkverkehr
- Einwahlzugänge

Notes:

Firewall

- Hardware- und Softwarelösung
- Konzept
- Pflege und Wartung

Notes:

Die Sache mit dem Haus 1

- Rechner wird mit Haus verglichen
- Darf man klingeln?
- Schauen ob Türen offen sind?
- Oder gar nichts...
- Technisch möglich, rechtlich erlaubt?!

Notes:

Die Sache mit dem Haus 2

Frage[a]

Mein Haus steht an einer öffentlichen Straße. Ich möchte nicht, daß man das Haus von dort aus sehen kann. Ich habe gehört, daß man mit Hilfe von Taschenlampen auch bei ausgeschalter Sonne, Mond und Beleuchtung mein Haus sehen kann. Wie kann ich mich nun schützen?

Gewünschte Antwort

Es gibt da extrem coole Folien mit dem Aufdruck 'Das ist kein Haus.', die man in die Fenster kleben kann. Kostenlos und besonders bunt sind die von Zonealarm.

[a] Message-ID: <slrn9tfi1v.i4.lutz@taranis.iks-jena.de>

Notes:

Personal–Firewall

Anmerkung der Redaktion: Desktop Firewalls bieten keinen automatischen Schutz und bleiben nutzlos, wenn das System der Firewall nicht verstanden wird. Beachten Sie dazu unseren Hinweis zur Installation sowie einen Einführungsartikel bei Trojanerinfo.de

`http://www.sicherheit-im-internet.de/`[a]

[a] http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=61&tsid=269&tdid=1562&page=0

Notes:

Paketfilter

- Alles verbieten
- Nur Erlaubtes erlauben
- Pflege und Wartung

Notes:

Sicherheit testen

- Geht das?
- Was braucht man
- Einmal getestet, immer glücklich?

Notes:

Scan–Programme

- Kommandozeilenwerkzeug: `nmap`
- GUI-Applikation: `nessus`
- DS-Niedersachsen[a]
- Der Klassiker unter den Sicherheitscannern `satan`
- und viele mehr

[a] `https://check.lfd.niedersachsen.de/Selbsttest/service/selbsttest.php`

Notes:

`nmap`

- Portscanner
- viele Scan-Optionen
- TCP/UDP Scan
- OS-Erkennung

Notes:

`nessus`

- Sucher nach Sicherheitslücken (Security scanner)
- erkennt viele aktuelle und alte Sicherheitslöcher
- hat eine GUI
- kennt Lücken verschiedener Betriebssysteme

Notes:

Einbruch

- Unerlaubter Zugang zum Rechner
- Erkennung durch: Logfile-Analyse, Dateisystem-Prüfsummen,...

Notes:

Angriffserkennung

- War eine ganze Zeit hip
- Im Moment nicht mehr ganz so attraktiv
- snort, aide, portsentry, harden-nids
- Angriffserkennung erfolgt durch Analyse des Netzwerkverkehrs

Notes:

Angreifen

- rootkits
- selber programmieren und testen

Notes:

Informationsquellen

Newsgruppen (deutsch)

- `de.comp.security.firewall`
- `de.comp.security.misc`

Newsgruppen (international)

- `comp.risks`
- plus 80 weitere mit security im Namen

Notes:

Mailinglisten

- Bugtraq: `http://www.securityfocus.com/forums/bugtraq/intro.html`
- Ankündigungslisten der Distributionen
- DFN-CERT `http://www.cert.dfn.de/`
- RUS-CERT `http://cert.uni-stuttgart.de/`

Notes:

URL-Sammlung

- `http://www.belug.org/index.php3?links`

Notes:

Bücher

Practical Unix and Internet Security Simson Garfinkel, Gene Spafford

Linux System Security: The Administrator's Guide to OS Security Tools; Scott Mann, Ellen L. Mitchell

Building Linux and Openbsd Firewalls Wes Sonnenreich, Tom Yates

Maximum Linux Security A Hacker's Guide to Protecting Your Linux Server and Workstation

Linux Firewalls Konzeption und Implementierung für kleine Netzwerke und PCs, Robert L. Ziegler

Linux Hacker's Guide Sicherheit für Linux- Server und -Netze. Anonymus

Linux Netzwerke. Aufbau, Administration, Sicherheit Stefan Fischer, Ulrich Walther;

Notes:

Das Ende

- Fragen
- Ergänzungen
- Hinweise

Notes:

Der Vortrag wird in den nächsten Tagen
unter folgender URL zu finden sein:

- `http://www.piak.de/linux/`

Unter folgender URL finden sich
bereits jetzt Links zum Thema Sicherheit:

- `http://www.belug.org/index.php3?links`

Notes:

Danke!

Notes: