

Linux Basterei Teil 1: Sicherheit

Nico -telmich- Schottelius,
nico-ccc-easterhegg2004 (BEI) schottelius.org
<http://nico.schotteli.us/papers/speeches/easterhegg2004/>

04-04-04
(vierte April zweitausend und vier)

1 Einleitung

Dieser Workshop...

- ...ist kein Monolog
- ...ist nicht vollständig
- ...ist dynamisch

2 Ziele der Sicherheit

- Was wollen wir erreichen?
- Zielsysteme
- Ende der Sicherheit

3 Angriffsmöglichkeiten

- Pre-Boot
- Beim Booten
- Laufender Betrieb

4 Angriffe & Fixes

4.1 Pre-Boot: Bootloader

- grub
password <md5hash> , beschränkt die Funktionen
lock für jeden Eintrag, beschränkt die Auswahl
- lilo
password=<deinpasswort>
- yaboot, andere, infos?

4.2 Beim Booten

- Shellskript - unterbrechbar - wichtige Dienste möglicherweise abstellbar
- Netzwerk läuft - „Firewall“ nicht
- Dienstreihenfolge ist wichtig

4.3 Laufender Betrieb

- Unsichere Dæmons
 - chroot()
 - suid
 - daemon seperation
- offene Shells (vlock/-a)
- X11 Service - keylogger - Beispiel xterm (secure mode)

4.4 Aus einem anderen System heraus

- Kompromitierung mit externen Medium (Floppy,CD,USB-Stick, Netzwerk)
- Beschlagnahmung / Auseinanderbau

5 Anhang und Literatur

- Cryptoloop partial security: <http://nico.schotteli.us/papers/linux/cryptoloop-partial-security>

6 Ende

- Sicherheit ist ein laufender Prozess, kein Einmalhandeln

Vielen Dank für die Teilnahme, bis zum nächsten Mal

Auf <http://nico.schotteli.us/papers/speeches/easterhegg2004/>
gibt es jetzt die Latex Quellen