Systemdienste und Betriebssystemadministration

BSD Jails

Stephan Uhlmann <su@su2.info>
05.07.2002

- Einführung
- Funktionsweise
- Einrichten
- Starten
- Administration
- Ausbruch
- Literatur

Einführung

- Seit FreeBSD 4.0

- Poul-Henning Kamp, R&D Associates
  Robert Watson

- “God, root, what difference?”

- gefahrlose Weitergabe des root-Accounts für ein Subsystem
  (FTP, HTTP, Mail, ...)

Einführung

- Erweiterung des chroot() Systemaufrufs
- Einschränkung eines Prozesses und seiner childs auf:
  - einen Unterbaum der Verzeichnishierarchie
  - eine IP-Adresse zur Netzwerkkommunikation
  - ungefährliche Systemaufrufe

Einführung

- keine komplette virtuelle Maschine
- weiterhin systemweit: (Host System)
  - Kernel
  - ein init Prozess
  - Mounts
  - Quotas
  - Paketfilter Regeln

Funktionsweise

- chroot
- Beschränkung der IP Kommunikation auf eine Adresse
- eigenes “Userland”
  - Daemons, binaries
  - Usernamen/Passwörter
  - Konfigurationen
  - Logfiles
  - ...

Funktionsweise

- Verbot bestimmter Systemaufrufe
  - mount
  - Änderung der Netzwerkeinstellungen (Hostname, IP, Routing, ...)
  - RAW IP Sockets (ping!)
  - Anlegen von Devices
  - Laden/Entfernen von Kernelmodulen
  - System V IPC (Semaphoren, Message queues, Shared Memory)*

*kann via sysctl erlaubt/verboten werden

Einrichten

- empfohlen (laut jail(8)) :
  `cd /usr/src; make world DESTDIR=/jail`

- benötigt src Distribution, alles muss kompiliert werden

- eleganter: `/stand/sysinstall`:
  - Options -> Install Root: /jail
  - Configure -> Distributions
    * bin - komplettes Userland inkl. /etc und /dev
    * crypto - sshd zur Administration

Einrichten

- `cd /jail; ln -s dev/null kernel`
- `cp /stand/sysinstall /jail/stand/`
- `touch /jail/etc/fstab`
- `cp /var/run/dev.db /jail/var/run/`
- `mount -t procfs proc /jail/proc`
- `ifconfig xl0 add 10.1.1.1`
- /jail/etc/rc.conf anpassen

Starten

- `jail /jail testjail 10.1.1.1 /bin/csh`
  - neue Shell im Jail
  - Jail wird beendet wenn Shell beendet wird (letzter Prozess)

- `jail /jail testjail 10.1.1.1 /bin/sh /etc/rc`
  - startet normalen Multiuser-Bootvorgang

Administration

- einloggen via SSH, danach wie jedes andere System
- Jail-Prozesse erkennbar am “J”-Flag (ausserhalb des Jails)
- Beenden: `kill -TERM -1` (im Jail!)

Ausbruch

- bis FreeBSD 4.2: Buffer-Overflow im procfs Code des Kernels
- kann unter anderem genutzt werden um
  - Jail-Flag eines Jail-Prozesses zu löschen
  - Root-Verzeichnis auf / zu setzen um chroot zu umgehen
  - Security-Level des Kernels auf 0 (insecure) zu setzen

Literatur

- man jail
- Artikel iX 3/2002: `http://www.heise.de/ix/artikel/2002/03/138/`
- Paper FreeBSD Project: `http://docs.freebsd.org/44doc/papers/jail/jail.html`
- procfs Bug: `http://www.securitybugware.org/BSD/140.html`