Linux Intrusion Detection System (LIDS, www.lids.org)

oder: wie mache ich mein System sicher...
und mir das Leben schwer :-)

Michael Würtz
TU Darmstadt, HRZ
10/2003

Inhalt

1. Intrusion Detection in Kurzform
2. Linux Intrusion Detection System
    1. Konzept
    2. Funktionsweise
    3. Installation / Konfiguration
    4. Beispiel
3. (Probe aufs Exempel)

Intrusion Detection

- Ziele:
  - Einbruch, Einbruchsversuch erkennen
  - Admin alarmieren
- Arten:
  - Netzwerk-basiert (snort, Firewall-Logs)
    - ungewöhnlichen Verkehr melden
    - Voraussetzung: genaue Regeln
  - System-basiert (tripwire bzw. aide, LIDS)
    - Datei-Veränderungen melden
    - Voraussetzung: Datenbank mit Fingerprints

Intrusion Detection - Probleme

Netzwerk-basierte IDS:

- erkennen keine Systemveränderungen
- Beispiel: root-shell auf WWW-Server: Port 80

System-basierte IDS:

- funktioniert ein IDS nach einem Einbruch noch?
- Beispiel: tripwire, Aufruf?
  - Datenbank?
  - tripwire-binary?

Intrusion Prevention

- besser: Einbruch verhindern
  - z.B. Openwall-patch: verhindert die Ausführung von Code im Stack
  - es gibt aber noch viele andere Möglichkeiten (race conditions, format strings, etc.)

➔bei der Komplexität und Vielfalt der Anwendungen ist das Verhindern eines Einbruchs praktisch unmöglich

- noch besser: Folgen eines Einbruches minimieren

Linux Intrusion Detection System

- root darf nicht mehr alles
- Schutz des Systems durch granulares Zuweisen von Rechten, ACLs
  - Dateien, Verzeichnisse (VFS): Schreibschutz, verstecken, append
  - Prozesse: verstecken, vor Signalen schützen, Zugriff auf ein Verzeichnis beschränken
  - Hardware, IO-Zugriffe: beschränken
  - Netzwerk: Zugriff auf bestimmte Ports beschränken
- An: (root), Prozesse (zu einer bestimmten Zeit)

LIDS Funktionsweise

- der Kernel ist die höchste Autorität im System
- Programme im user space setzen Systemaufrufe ab (z.B. open), kernel prüft und handelt ggf.
- LIDS erweitert die Sicherheitsabfragen im Kernel von EUID=0? auf einzelne Capabilities
- Wer diese besitzt, steht in der ACL
- Wenn versucht wird, die Rechte zu übertreten, wird ein Alarm generiert. (syslog, Mail)

Capabilities, CAP_...

- CHOWN, FOWNER, FSETID, LINUX_IMMUTABLE
- KILL, SETGID, SETUID, SETPCAP, SYS_CHROOT, SYS_PTRACE, PACCT
- NET_BIND_SERVICE, NET_BROADCAST, NET_ADMIN, NET_RAW
- IPC_LOCK, IPC_OWNER, DAC_OVERRIDE, DAC_READ_SEARCH
- SYS_MODULE, SYS_RAW_IO, SYS_ADMIN, SYS_BOOT, SYS_NICE, SYS_RESOURCE, SYS_TIME
- SYS_TTY_CONFIG, MKNOD, LEASE
- LIDS-spezifisch: HIDDEN, PROTECTED, KILL_PROTECTED

LIDS features

- LIDS kann ohne reboot abgeschaltet oder teil-abgeschaltet werden oder die Konfiguration neu einlesen
- Port Scan Detector im Kernel
- Meldungen per SMTP-client im Kernel

Installation / Konfiguration

- www.lids.org
- kernel patch + lidsadm + lidsconf
- Konfigurationsdateien in /etc/lids anpassen
- /etc/lids/lids.conf (ACL) erzeugen
- LIDS-Passwort setzen
- beim Hochfahren kernel versiegeln: lidsadm -I
- im Zweifelsfall booten mit: "lids=0"

LIDS: Beispiel

- in /etc/lids/:
  - lids.cap: regelt die „Standard-Umgebung“ (für root)
  - lids.net: enthält die Mail-Einstellungen
  - lids.pw: enthält das LIDS-Passwort (Ripe-MD160)
  - lids.conf: enthält die ACLs
  - lids.sh: mein Skript, das die ACLs setzt

LIDS: ACLs

- lidsconf -Z # erstmal alle ACLs löschen
- lidsconf -A -o /etc/lids -j DENY # verstecken
- lidsconf -A -o /sbin -j READONLY # Schreibschutz
- ... -s logrotate -o /var/log/ -t 0600-0700 -j WRITE
  nur logrotate darf die Logs verändern, zw. 6 und 7 Uhr
- ... -s apache -o CAP_NET_BIND_SERVICE 80,443 -j GRANT
- ... -s apache -o CAP_SETUID -j GRANT
- und viele weitere...

LIDS: ACLs

- Frage: wie erhalte ich die richtigen Sätze von ACLs?
- Antwort:
  1. Versuche, Prozess zu starten
  2. Alarme ansehen
  3. ACLs ändern
  4. goto 1

Arbeiten mit LIDS

- lidsadm -S -- -LIDS : *eine* LIDS-freie shell
- lidsconf -U : update ACLs, Inode-Tabelle,...
- lidsadm -S -- +RELOAD_CONF
- LIDS deaktivieren:
  lidsadm -S -- -LIDS_GLOBAL (keine gute Idee)

Noch Fragen?

Michael Würtz
wuertz@hrz.tu-darmstadt.de