Hostbasierte Sicherheit & Linux-Hardening

Ein Überblick

SLAC, 07.12.06

Steffen Wendzel
<steffen (at) ploetner-it (dot) de>

$ whoami

- Steffen Wendzel
  - steffen (at) ploetner-it (dot) de
- Open Source Entwickler
  - Projektleiter Hardened Linux
  - User-/Kernelspace Tools/Patches für Linux & OpenBSD (vstt, AstroCam, FUPIDS[1-3], ...)
- IT-Fachautor
- Informatik-Student
- Security Consultant (Ploetner-IT.de)

Überblick

- Betriebssystemunabhängige Grundlagen
- Installation
- Dateisystem
- Accounts
- Lokale Netzwerkdienste
- TCP/IP Stack absichern
- Systempatches
- Security Distributionen & Derivate
- Hardened Linux
- Diskussion (15min)

Betriebssystemunabhängige Grundabsicherung

- Physikalische Sicherheit
  - Schutz vor Naturkatastrophen
- BIOS-Passwort
  - Rechner physikal. abschließen
  - Bootreihenfolge
- Backups durchführen

Minimalisierung!

Hardening bei der Installation

- Nur installieren, was benötigt wird
- Vernünftige Partitionierung bspw. f. Read-Only Mounting
  - /, /boot, /usr, /var, /tmp, /home.
- Viel Speicher in /var für große Logs
  - Remote Logging w/ syslog-Host

Dateisystem-Hardening (1)

- User Mounting
- SUID, GUID Binarys
- Überflüssige Binarys
- chmod go-w für Verzeichnisse und Binarys des Systems
- Dateien ohne Eigentümer
  - Problem:
    - Neuer User könnte UID der Datei bekommen
      - `find / -path /proc -prune -o -nouser -o -nogroup`

Dateisystem-Hardening (2)

- ACL (Access Control Lists)
  - Zugriffsrechte für jeden User/jede Group
- Verschlüsselung von Dateien -> gnupg
- Verschlüsselung von Dateisystemen
  - loop-AES, dm-crypt, ...
- Mount-Optionen
  - noexec,nosuid,nodev
- Read-Only mount von Partitionen
- SWAP verschlüsseln ('encrypted' option)

Dateisystem-Sicherheit (3)

- Filesystem Intrusion Detection Systeme (FSIDS)
  - mtree
  - tripwire, OpenTripwire
  - aide (OpenSource-Ersatz für tripwire)
  - AFICK (Tk Oberfläche, auch für Windows)

Dateisystem-Hardening (4)

- Aide (1)
  - „Advanced Intrusion Detection System“
  - Datenbank erstellen
    - aide --init
  - Datenbank auf Veränderungen überprüfen
    - aide --check
    - Cronjob verwenden

Dateisystem-Hardening (5)

- Aide (2)
  - Leichtverst. Übersicht d. Veränderungen im Dateisystem

```
File: /etc/mtab
  Mtime     : 2006-11-03 15:30:32                , 2006-11-04 09:26:08
  Ctime     : 2006-11-03 15:30:32                , 2006-11-04 09:26:08

File: /etc/adjtime
  Size      : 45                                 , 44
  Mtime     : 2006-11-01 15:33:51                , 2006-11-03 23:56:07
  Ctime     : 2006-11-01 15:33:51                , 2006-11-03 23:56:07
  MD5       : u5ybW5uOyjE4a5cGNbVYyg==           , Me2Xsu/JeZpbMOi0LFahzQ==

File: /etc/mtools.conf
  Size      : 625                                , 624
  Mtime     : 2006-11-03 22:23:34                , 2006-11-03 22:24:50
  Ctime     : 2006-11-03 22:23:34                , 2006-11-03 22:24:50
  Inode     : 755571                             , 755570
  MD5       : 4uFAqcP4pTzsvVwNhKjYaw==           , ZZuxikSQ3LF60LATnC+2VA==
hikoki:/home/swendzel/Desktop#
```

Dateisystem-Hardening (6)

- Aide (3)
  - Zugriffsrechte, Inode, Anzahl Links, Eigentümer, Gruppe, Größe, Block-Count, Modification/Access/Creation-Time
  - Checksum Überprüfung
    - md5
    - sha1
    - rmd160
    - tiger, haval, gost, crc32
  - Mehr dazu in Hakin9 2/07
  - mtree bietet ähnliche Features + Komfort

Accounts (1)

- Unbenutzte Default-Accounts
  - anonymous FTP mit Login-Shell!
- Sichere Passwörter
  - john
- Zeitliche Gültigkeit von Passwörtern

Accounts (2)

- Sichere Authentifizierung
  - Viele Möglichkeiten
    - One Time Passwords (S/Key, OPIE), Kerberos-Authentifizierung, Authentication/Autorization/Accounting (RADIUS, TACACS+), Authentifizierung/Verschlüsselung via SSL und IPSec, biometrische Authentifizierung, ...
  - PAM
    - Viele Programme (Telnet, FTP, ...)
    - Viele Authentifizierungsmöglichkeiten
    - Administrator konfiguriert Verhalten

Accounts (3)

- Restricted Shells
  - Schreibrechte(!)
- chroot Umgebung
  - z.B. bei FTP-Accounts

Netzwerkdienste detektieren

- Unbemerkt offene Ports
  - netstat, lsof
- grep -R <appname> /etc/*
- egrep -v '^#.*$|^$' \ /etc/inetd.conf
- rpcinfo -p
- Scans mit nmap
- Detektion von nicht UDP-/TCP-Backdoors:
  - tcpdump, NIDS

TCP/IP Stack Hardening (1)

- /proc
- sysctl (Linux, BSD)
  - wenn /proc nicht verfügbar
- ndd (Solaris, HP-UX)
- no (AIX)
- systune (IRIX)

TCP/IP Stack Hardening (2)

- Linux: /proc
  - /proc/sys/net/ipv4/conf/*
    - accept_redirects
    - icmp_echo_ignore_broadcasts
    - log_martians
    - send_redirects
    - ip_forward
  - /proc/sys/net/ipv6/*
    - accept_ra
    - accept_redirects

TCP/IP Stack Hardening (3)

- Linux: sysctl
  - sysctl -w <var>=<wert>
    - net.ipv4.conf.all.accept_redirects=0, ...
- OpenBSD: sysctl
  - sysctl -w <var>=<wert>
    - net.inet.ip.accept_sourceroute=0, net.inet.icmp.rediraccept=0, ...
- Solaris: ndd
  - ndd -set /dev/ip <var> <wert>
    - ip_respond_to_timestamp 0, ip_respond_to_echo_broadcast 0, ip(6)_ignore_redirect 1, ip(6)_forward_source_routed 1, ...

Weitere Maßnahmen zur Sicherung eines Hosts (1)

- BSD: Securelevel
- Port Knocking
- Firewalls
- TCP Wrapper
- HIDS
  - RootKit Detektion
- NIDS
- IPS (z.B. systrace)

Weitere Maßnahmen zur Sicherung eines Hosts (2)

- Logdateien überwachen
- Standardtools verwenden
  - who, w, last, netstat, lsof, find, ...

Patches (1)

- Security Patches - klar!
- Stack Smashing Protection
- OpenWall
  - SSP, Restriktionen für /tmp, /proc, FIFOs, ...
- Mandatory Access Control (MAC)
  - Zugriffsrestriktionen für Bentzer/Prozesse auf Objekte
  - Diverse Kernel-Patches für Linux und BSD
  - Implementiert in div. Distributionen, TrustedBSD und in Trusted Solaris

Patches (2)

- PaX
- GrSecurity
- SeLinux
- apparmor
- Systrace
  - Bestandteil von NetBSD, OpenBSD und OpenDarwin, Linux-Port verfügbar
- Linux Intrusion Detection System (LIDS)
  - Prozesse verstecken, Zugriffsrestriktionen für Dateien, Trusted Path Execution (TPE), ...
- Papillon, FUPIDS, ...

Sichere Distributionen

- Linux Distributionen
  - Adamantix (Debian basiert)
  - Annvix (Mandriva basiert)
  - Hardened Gentoo
  - Hardened Linux (Slackware basiert)

Sichere BSD-/Unix-Derivate

- OpenBSD
- Trusted BSD (FreeBSD basiert)
- Trusted Solaris

Hardened Linux (1) => Features im Groben

- Für IDS, VPN, Authentifizierung
- Open Source Projekt
- Mind. 3 Jahre Sicherheits-Updates
- SSP, GRSecurity, PaX
- Keine offenen Ports (!22) by default
- Standardpakete zusätzlich abgehärtet
- HLHS
- TODO: Webinterface
  - Zur Administration & Konfiguration
  - Neues Runlevel-Konzept

Hardened Linux (2) => Hardening Scripts

- Skripte zur autom. Absicherung d. Systems
- Ncurses basiert
- Ein Klick, Eine Aktion (kinderleicht)
  - Autom. Dateisystemüberwachung m. AIDE
  - Swap-Encryption
  - TCP Portscan Protection
  - TCP/IP Stack Protection via /proc
  - Zugriffsrestriktionen für Binarys
  - Wir überlegen uns noch weitere Features!

Folien, Literaturliste, ...

www.ploetner-it.de

www.doomed-reality.org

www.hardened-linux.org

Vielen Dank ...

... für Ihre Aufmerksamkeit.

Fragen?