Kurzakte Linux-System-Sicherheit

Systemstart und -stopp

- keinen Start von Wechselmedien aus ermöglichen (BIOS, Laufwerke ausbauen)
- Bootmanager mit Passwort absichern
- Herunterfahren des Systems für Benutzer nicht erlauben (/etc/inittab)

Accounts und Passwörter

- nur nötige Logins gewähren
- UIDs und GIDs eindeutig vergeben (UID 0 !!!)
- starke Passwörter erstellen/erzwingen (pwgen, PAM)
- Erstellen sicherer Passwörter mit proaktiver Prüfung (npasswd, passwd+)
- keine offenen Accounts (leeres Passwortfeld)
- Check der eingerichteten Passwörter (crack, john the ripper)
- Einsatz stärkerer Verschlüsselungsalgorithmen (Blowfish, MD5)
- shadowing (pwunconv)
- Systembenutzer beschränken (als Shell /bin/false)
- Loginvorgang restriktiver gestalten (/etc/login.defs)
- keine r-utilities (/etc/hosts.equiv)
- PAM zur Trennung der authentifizierenden Programme vom Verfahren
- Tools: Konsistenzcheck mit Tiger oder COPS
- Authentisierung über PKI (SSL) oder Kerberos
- Root-Logins über Terminals unterbinden (/etc/securetty)
- Accounts auf verdächtige Nutzung untersuchen

Benutzerrechteverwaltung

- vernünftige umask
- kein w-Recht für den Rest der Welt
- Listing für bestimmte Verzeichnisse unterbinden
- chattr +i für Dateien in ext-Dateisystemen
- SUID-Bits sparsam vergeben
- Adminrechte mit sudo beschränken auf user, Verz., Dateien usw. (/etc/sudoers)
- Wiederherstellen der Originalrechte (rpm -setperms programmname)
- Evtl. Nutzung von cron und at verbieten (/etc/cron.allow, /etc/cron.deny)

Informationen über das System zurückhalten

- Begrüßungstexte (/etc/issue, /etc/issue.net)
- distributionsspezifische Info-Dateien löschen (/etc/SuSE-release)
- HISTSIZE und HISTFILESIZE verkleinern (z. B. auf 10)
- finger, showmount, rpcinfo abschalten

Ressourcen beschränken

- sinnvolle Partitionierung
- Partitionen sinnvoll einbinden (noexec, nosuid, ro)
- Quotas für Benutzer und Gruppen
- Anzahl offener Dateien oder Prozesse je Benutzer (ulimit und PAM)
- Dateien passwortgesichert verschlüsseln
- Kryptodateisysteme (DM-Crypt mit LUKS)

Erstellt von Dr. Jörg Meese www.doc-systems.de

Systemintegrität (gegen unbemerkte Modifikationen)

- Dateien sicher löschen (erst mit dd überschreiben, dann löschen)
- Dateileichen nicht mehr existierender User entfernen
- setuid- oder setgid-Programme sowie Gerätedateien finden
- in PATH-Variable kein "." und andere verdächtige Verzeichnisse
- Aufspüren von Änderungen im Dateisystem-Baum (Baselines)
- Aufspüren modifizierter Datei-Inhalte (md5sum)
- Nach Rootkits suchen (chkrootkit)
- Schließen von Sicherheitslöchern durch Updates und Patches
- Installation von Nicht-Systemsoftware nur mit Benutzerrechten
- Tools: tripwire, AIDE zum Festhalten des Status und Erkennen von Veränderungen

Dienste und Daemonen

- inetd selbst bzw. Dienste im inetd (Root-Login-Shell)
- Zugriffsbeschränkung (TCP-Wrapper , xinetd, in Dienst integrierte Restriktionen zB. FTP)
- unnötige permanente Daemons abschalten (at, pcmcia, inn, routed, ypserv, rwhod)
- unsichere Dienste in einem Käfig starten (chroot)
- Kontrolle auf offene Ports (netstat –tulp, lsof –i, nmap)
- Tracing von Prozessen (strace –p pid)
- Netzwerk-Traffic beobachten und nach Strings durchsuchen (tcpdump, Ethereal)
- Firewall, IDS (Snort)

Schwachstellen in Diensten für vertrauenswürdige Umgebungen

- X-Window-System (nicht xhost + oder DISPLAY, sondern Magic-Cookies)
- Setzen von DISPLAY beim Systemstart macht xhost zwecklos
- Portmapper
- NFS (root-squash), NIS (ypcat /etc/shadow)
- Email über POP3 authentifizieren und nicht über SMTP

Bugs in Systembereichen

- Schutz vor Buffer Overflows durch Systemupdates

Logdateien erzeugen und auswerten

- last, lastlog, lastb (/etc/utmp, /etc/wtmp, /etc/btmp, /etc/lastlog)
- syslogd einrichten (/var/log/messages auf "FAILED" oder " service su"-Einträge prüfen)
- Tools: grep, logwatch, Swatch, Logsurfer

verschlüsselte Verbindungen

- SSH (evtl. nur bestimmte Kommandos [publ. key] oder User [allowUsers] zulassen)
- PGP, GnuPG
- openvpn

Benutzeridentität

- nicht als root im Internet surfen
- nur als root einloggen, wenn es unumgänglich ist

übergreifende Sicherheitstools:

- lokal: Cops, Tiger
- remote: ISS, Satan