



Sicherheitsschulung

Unix Datensicherheit

IP-Schulung

Gesamtüberblick

- Installation und Patches
- Services
- boot-time start processes
- system Einstellungen
- secure shell
- tcp_wrappers
- Hardening tools
- ip filter
- intrusion detection systems

IP-Schulung

Datensicherheit UNIX

- **Ist Solaris sicher?**
- 78 Programme sind setuid
- 30 Programme sind setgid
- 29 offene tcp ports
- 29 offene upd ports
- Über 70 verschiedene empfohlene patches

Datensicherheit UNIX

Installation und Patches

- Installation OHNE Netzwerkzugang
- Neueste Patch-CD bereit halten
- CD mit Zusatz—Software bereithalten
- Netzwerk erst am Ende nach der Sicherung einstecken

Datensicherheit UNIX

Services

- Prüfen Sie unbedingt die Datei /etc/inetd.conf
- Sie kann bei den meisten Systemen komplett leer sein
- Unbedingt sind folgende Dienste auszuschalten
 - Shell, login, exec (Klartext passworte und unsichere Authentisierung)
 - Sadmin (remote exploit)
 - rstatd (remote exploit)
- Manche sind einfach überflüssig
 - fs (sun font server)
 - tftp (trivial file transfer server)

Datensicherheit UNIX

boot-time prozesse

- Entfernen Sie alle ‚unnötigen‘ Startskripte aus ‚/etc/rc2.d‘ und ‚/etc/rc3.d‘
- (LINUX) Editieren Sie rc.local, um alle ‚unnötigen‘ Prozesse zu beseitigen
- Prüfen Sie direkt nach dem Installieren welche Prozesse laufen und fragen Sie sich was die eigentlich machen

Datensicherheit UNIX

Systemeinstellungen

- Banner für Dienste editieren oder löschen
- ftp Benutzung einschränken
- /etc/motd editieren
- Löschen Sie den "decode" Eintrag aus der Alias Konfiguration von sendmail
- Löschen Sie unbenutzte cron jobs
- Setzen Sie die core dump size auf null
- Passwd Einstellungen /etc/default/passwd

Datensicherheit UNIX

Systemeinstellungen Netzwerk

- Durch Veränderung der Netzwerk-Schnittstellungen wird das System sicherer
- Verhinderung von smurf Angriffen
 - `ndd -set /dev/ip ip_forward_directed_broadcasts 0`
- Verhinderung von routing
 - `ndd -set /dev/ip ip_strict_dst_multihoming 1`
 - `ndd -set /dev/ip ip_forwarding 0`
- Nachzulesen in den SUN Blueprints

IP-Schulung

secure shell

- Bei den Protokollen ftp und telnet werden die Passworte im Klartext über das Netzwerk geschickt. Das darf nicht sein!
- Installieren Sie unbedingt ssh! Verwenden Sie deshalb immer ssh statt telnet und scp statt ftp.
- Tcp_wrapper support einschalten
 - `./configure --with-tcp-wrappers`
- Nach der Installation das sftp subsystem einschalten
- Übertragen Sie die Binaries nicht von einer Architektur zur anderen
- rsh, rlogin und rexec ersetzen
- <http://www.openssh.com/manual.html>
- Nur an Admin-LAN binden
- Unterstützung für Protokoll 1 rausnehmen

Datensicherheit UNIX

tcp_wrappers

- Installieren Sie unbedingt "tcp_wrappers"!
- Language-Extension einschalten
- Compilieren, installieren
- /etc/inetd.conf konfigurieren
 - telnet stream tcp root nowait /usr/local/sbin/tcpd in.telnetd
- /etc/hosts.allow
 - Sshd: .berkom.de
- /etc/hosts.deny
 - ALL: ALL
- /etc/hosts.deny:
 - in.tftpd: ALL: (/some/where/safe_finger -l @%h | /usr/ucb/mail -s %d-%h root) &

Datensicherheit UNIX

ip_filter

- Ip_filter sind eine Host-Basierte Firewall
 - ... Weil doppelt hält besser
- Ip_filter sind statefull (auch bei icmp Packeten)
- Ip_filter filtern kleine IP-Packete
- Ip_filter filtern nach tcp-flags
- Default sollte alles blockieren und loggen
 - `block in log on hme0`

Datensicherheit UNIX

sudo

- Sudo ist ein Programm, mit dem man einem Benutzer erlauben kann, etwas als root oder als ein anderer Benutzer zu tun.
- Anwendungsbeispiel
 - Erlaube Betriebsüberwachung den httpd neu zu starten
- Nutzen
 - Root kann alles, deshalb sollten nur wenige das passwort wissen
 - Mit sudo muss man das root passwort nicht mehr jedesmal ändern, wenn jemand das Unternehmen verlässt
 - Selective root-Rechte
 - Logging der Commandos
 - Eine sudoers Datei für alle Rechner möglich
- Sie WOLLEN sudo!

Datensicherheit UNIX

hardening tool

- YASSP is "Yet Another Solaris Security package,,
 - Alles aus einer Hand
- TITAN
 - Kleine Module, Wahlfreiheit
- SIUX
- Solaris Security Comparison

- => Verwenden Sie YASSP!

Datensicherheit UNIX

intrusion detection systems

- Snort ist ein netzwerkbasierendes Intrusion Detection System, das in Realzeit Netzwerkpackete analysiert und protokolliert.
- Es kann portscans, trojanische Pferde, cgi-Attacken, buffer-overflow-Attacken erkennen
- Snort läuft auf fast jedem Betriebssystem und es ist umsonst

Datensicherheit UNIX

Solaris fingerprints

- SUN bietet eine Datenbank mit Signaturen/MD5-Hashes der Solaris binaries
- WebInterface lässt Prüfung von 256 Werten zu
 - <http://sunsolve.Sun.COM/pub-cgi/fileFingerprints.pl>
- DB kann man runterladen

Datensicherheit UNIX

Literatur

- Solaris-Security
 - <http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec>
 - <http://www.sun.com/blueprints>
 - <http://www.rvs.uni-hannover.de/people/voeckler/tune/EN/tune.html>
- Hardening Tools
 - <http://www.fish.com/titan/>
 - <http://www.yassp.org/>
- Allgemeines
 - <http://www.sans.org/>
 - <http://www.cert.org/security-improvement/>
 - <http://www.ciac.org/ciac/>
 - <http://www.bsi.de/>
 - http://www.accs.com/p_and_p/SolSec/
 - <http://www.cisecurity.org/>
 - http://www.cert.org/tech_tips/usc20_full.html

Datensicherheit UNIX

Ansprechpartner

Axel Nennker

T-Systems International GmbH

SSC ENPS / Technologiezentrum

Tel: 030 / 34 97 - 3256

Fax: 030 / 34 97 - 3257

email: axel.nennker@t-systems.com

Datensicherheit UNIX

Fragen

Zusammenfassung

Fragen???