HP-UX 11i Security Features

Ute Schüller

HP TSG – Solution Center Unix

© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice

Überblick

- Konfigurationsmöglichkeiten
  - Welche sicherheitsrelevanten Einstellungen bietet das HP-UX Betriebssystem?
- Produkte und Tools
  - Ein Überblick über die bei HP erhältlichen Sicherheits-Produkte
- Schnittstellen
  - Eine Aufstellung der verfügbaren Programmierschnittstellen

2

Trusted System & Auditing

- Trusted System
  - Shadow-Passwd
  - Passwort-Management
  - Zeitgesteuerter Benutzerzugriff
  - Protokollierung auf Aktions- und Benutzerebene
- Auditing
  - Protokollierung auf Aktionsebene

3

Auditing

- `$ audisp -u ute1 -e login -e create /.secure/etc/audfile1`

```
users and aids:
ute1  20
Selected the following events:
login  create
1024 9216
All ttys are selected.
Selecting successful & failed events.
TIME              PID E  EVENT    PPID   AID  RUID RGID  EUID   EGID TTY
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  ~~~
020914 15:10:46 23207 S   9218  23206    20     0    0     0      0
  pts/tb
[ Event=login; User=ute1; Real Grp=root; Eff.Grp=root;  ]
SELF-AUDITING TEXT: User= ute1 uid=9999 audid=20 Successful login
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  ~~~
020914 15:10:46 23207 S     42  23206    20  9999   20  9999     20
  pts/tb
[ Event=pipe; User=ute1; Real Grp=users; Eff.Grp=users;  ]
     RETURN_VALUE 1 = 3; RETURN_VALUE 2 = 4
     PARAM #1 (file desc's) =     fd#1:   0xffffffff (idev); 7784 (inum)
```

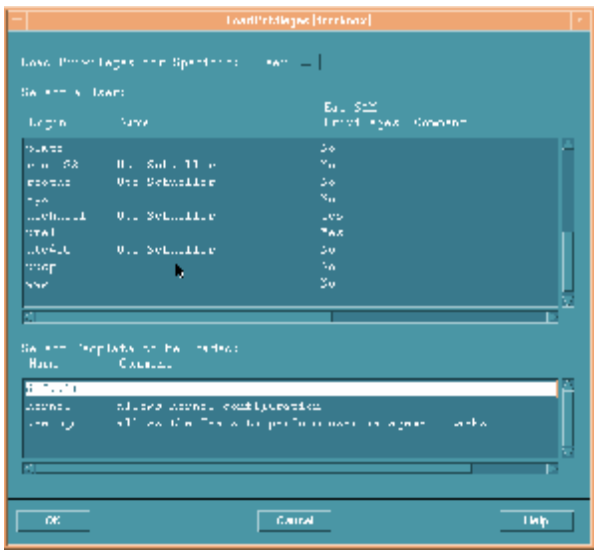
4

Restricted SAM

- Mit Hilfe des Restricted SAM können einzelnen Benutzern erweiterete Berechtigungen gegeben werden, ohne daß diese User eine root-Berechtigung erhalten müssen.
- Aufruf: sam –r (als root zur Konfiguration der Privilegien)

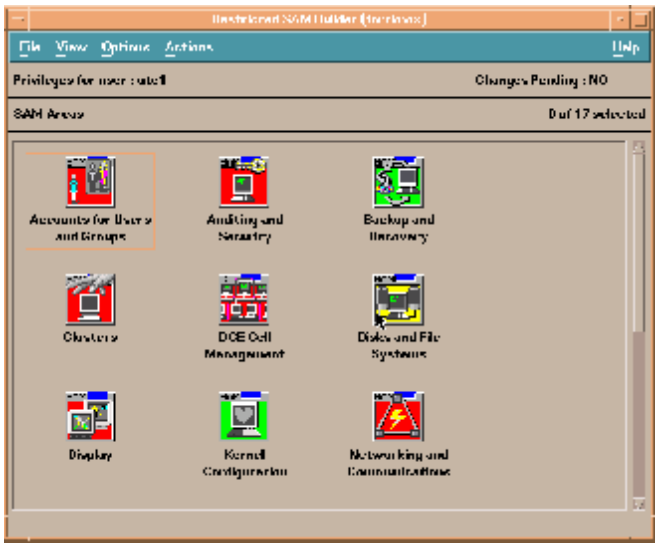
5

Restricted SAM



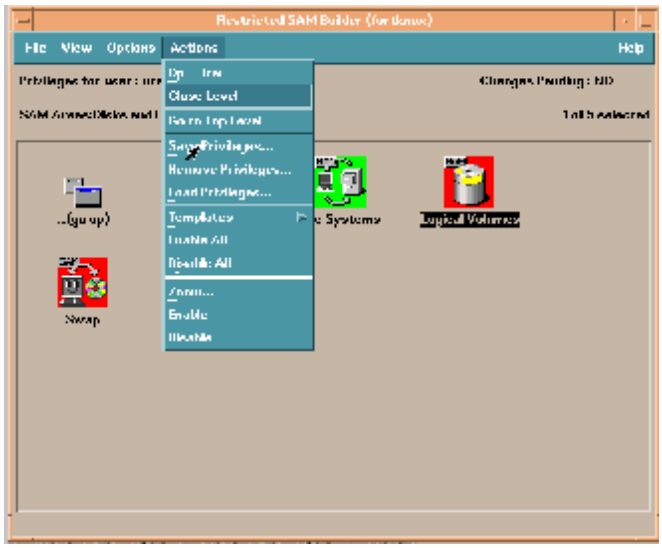
6

Restricted SAM



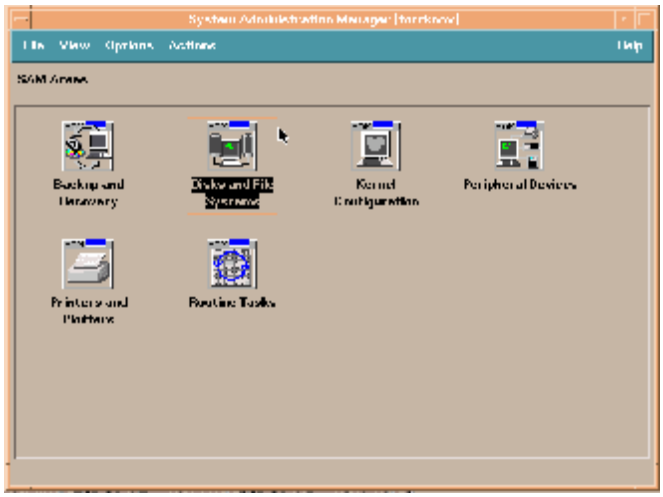
7

Restricted SAM



8

Restricted SAM (User Sicht)



9

Stack Buffer Overflow

- HP-UX 11i bietet einen neuen Kernel-Parameter: executable_stack
- Einstellungen:
  - 0: Stack nicht ausführbar
  - 1: (default) Stack wie bisher ausführbar
  - 2: wie 1, jedoch mit Protokollierung
- Spezielle Konfigurationen für einzelne Programme werden mit dem “chatr”-Kommando vorgenommen.

10

/etc/default/security

- In dieser Datei können eine ganze Reihe von sicherheitsrelevanten Einstellungen systemweit vorgenommen werden:

```
#File:  /etc/default/security
ABORT_LOGIN_ON_MISSING_HOMEDIR=1
MIN_PASSWORD_LENGTH=7
#PASSWORD_MIN_UPPER_CASE_CHARS=0
#PASSWORD_MIN_LOWER_CASE_CHARS=1
#PASSWORD_MIN_DIGIT_CHARS=0
#PASSWORD_MIN_SPECIAL_CHARS=1
NOLOGIN=1
NUMBER_OF_LOGINS_ALLOWED=2
PASSWORD_HISTORY=3
SU_ROOT_GROUP=rootusr
SU_DEFAULT_PATH=/sbin:/usr/sbin:/usr/bin
SU_KEEP_ENV_VARS=SHLIB_PATH,LD_LIBRARY_PATH
```

11

Syslogd –N Schalter

- Mit Hilfe dieses neuen Schalters läßt sich die Möglichkeit des remote-Zugriffs auf den syslog-Daemon abschalten.

```
$ ps -ef| grep syslog
    root 23847     1  0 16:09:43 ?        0:00 /usr/sbin/syslogd -D -N

$ cat /etc/syslog.conf
# @(#) $Revision: 74.1 $
#
# syslogd configuration file.
#
# See syslogd(1M) for information about the format of this file.
#
mail.debug              /var/adm/syslog/mail.log
*.debug                 /var/adm/syslog/debug.log
*.info;mail.none        var/adm/syslog/syslog.log,@sysadmin.hp.com
*.alert                 /dev/console
*.alert                 root
*.emerg                 *
*.info                  @sysadmin.hp.com
```

12

HIDS/9000 & IPSec/9000

- HIDS/9000
  - HIDS ist ein host-based "Intrusion Detections System", das ein System durch permanentes Überwachen
    - der verwendeten Systemcalls (im Kernel) und
    - bestimmter System-Logdateien

    schützt.
- IPSec/9000
  - Mit IPSec ist eine host-to-host VPN verfügbar, die Datenverschlüsselung und –integrität sicherstellt.

13

IPFilter/9000

- IPFilter ist eine packetfiltering Firewall, die es erlaubt, anhand von Regeln, den Zugriff auf bestimmte Services oder von bzw. zu dedizierten Rechnern oder Netzwerken einzuschränken.

```
$ cat /etc/opt/ipf/ipf.conf
block return-rst in log quick proto tcp from 15.140.10.113/32 to any
block return-icmp(port-unr) in log quick proto udp from any to any port = 53
block return-icmp-as-dest(port-unr) in log quick proto udp from
15.140.10.113/32 to any
pass out quick on lan0 proto udp from any to any port = 53 keep state
pass in all
pass out all
```

14

Security Patch Check

- Mit diesem Tool kann ein System auf fehlende Security-Patches untersucht werden.

Laden der Referenz-Patch-Liste:

```
$ export ftp_proxy=http://web_proxy.mycompany.com:8088
$ /opt/sec_mgmt/spc/bin/security_patch_check -r
```

Ausführen des Security Patch Check:

```
$ /opt/sec_mgmt/spc/bin/security_patch_check
```

Untersuchen anhand einer gespeicherten swlist-Ausgabe:

```
$ swlist -l fileset -a supersedes -a revision \
  -a software_spec -a state > swlist.patches
$ security_patch_check -f swlist.patches
```

Überprüfen eines Remote-Systems:

```
$ security_patch_check -h <remote host>
```

15

Security Patch Check (manueller ftp-Download)

```
$ /opt/socks/bin/ftp ftp.itrc.hp.com
User:       ftp
Password:   <your-email-address>
cd export/patches
get security_catalog.gz
get security_catalog.sync
bye
cat security_catalog.sync
cksum security_catalog.gz
gunzip security_catalog.gz
```

16

Security Patch Check (Report)

```
*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl, run as root
Analyzed localhost (HP-UX 11.00) from fortknox
Security catalog: ./security_catalog
Security catalog created on: Fri Sep 13 05:36:01 2002
Time of analysis: Mon Sep 16 08:52:19 2002
List of recommended patches for most secure system:
#  Recommended  Bull(s) Spec? Reboot? PDep? Description
-------------------------------------------------------------------------------
1  PHCO_22665   135     No    No      No    kermit(1)
2  PHCO_22766   167     No    No      No    cu(1) cumulative
3  PHCO_22767   146     No    No      No    cumulative crontab/at/cron
4  PHCO_23088   138     No    No      No    man(1)
5  PHCO_23117   127     No    No      No    bdf(1M) cumulative
6  PHCO_23118   127     No    No      Yes   df(1M) cumulative
7  PHCO_25342   153     No    No      No    Kernel configuration commands
8  PHCO_25527   191     Yes   No      Yes   libpam and libpam_unix cumulative
...
21 PHSS_26490   175     Yes   No      Yes   CDE Runtime Periodic
22 PHSS_27570   208     Yes   No      Yes OV EMANATE14.2 snmpModules of SNMPv2 MIB
-------------------------------------------------------------------------------
*** END OF REPORT ***
NOTE: Security bulletins can be found ordered by number at
http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin
```

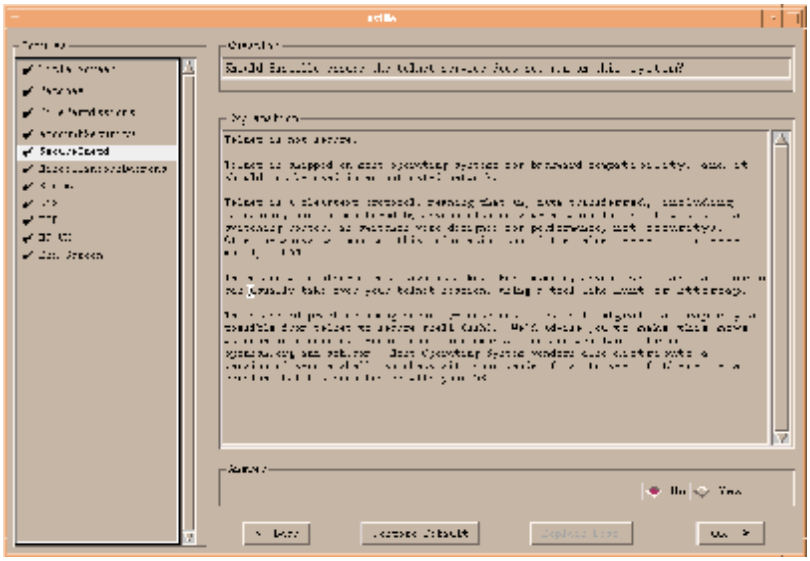
17

Bastille

- Bastille unterstützt die Umsetzung des White-Papers “Building a Bastion Host”.
- Bastille ist verfügbar für HP-UX 11.0 und 11i (11.11 und 11.23) – ab 11.23 - Sept. 2004 wird es direkt mit dem Betriebssystem installiert
- Die zu konfigurierenden Einstellungen werden mit einer graphischen Oberfläche abgefragt.

18

Bastille (Konfiguration)



19

Bastille

- Der User kann anschließend die gemachten Einstellungen automatisch umsetzen lassen.

- Vorschläge zu manuellen Änderungen werden in */var/opt/sec_mgmt/bastille/TODO.txt* abgelegt

20

WuFTP

- Der neue FTP-Daemon erlaubt eine erweiterte Protokollierung, sowie das Einrichten zusätzlicher FTP-User, die den selben Beschränkungen (change-root) unterliegen, wie der Anonymous-FTP User.

Optionen:

```
$ ftpd -L -K -a /etc/ftpd/ftpaccess
```

Change-Root:

```
$ grep ftp /etc/passwd
ftptest:*:102:30:FTP-Test
  User,,,:/home/ftptest/./:/usr/bin/ftponly

$ grep 30 /etc/group
ftpgroup:*:30:ftptest

$ grep guestgroup /etc/ftpd/ftpaccess
guestgroup ftpgroup
```

21

FTP (ftpaccess)

```
class   local   real,guest,anonymous *.domain 0.0.0.0
class   remote  real,guest,anonymous *

limit   local   20  Any                 /etc/msgs/msg.toomany
limit   remote  100 SaSu|Any1800-0600   /etc/msgs/msg.toomany
limit   remote  60  Any                 /etc/msgs/msg.toomany
...
log commands real
log transfers anonymous,real inbound,outbound

# all the following default to "yes" for everybody
delete       no   guest,anonymous        # delete permission?
overwrite    no   guest,anonymous        # overwrite permission?
rename       no   guest,anonymous        # rename permission?
chmod        no   anonymous              # chmod permission?
umask        no   anonymous              # umask permission?
...
# deny to retrieve the following files
noretrieve /etc/passwd /etc/group core
```

22

Sendmail 8.11.1

- In der Version 8.11.1 sind eine ganze Anzahl zusätzlicher Security-Funktionen implementiert; z.B.:
  - die Verwendung einer Zugriffsdatenbank (8.9.3)
  - ein standardmäßig abgeschaltetes Relaying (8.9.3)
  - Unterstützung von SASL – Simple Authentication and Security Layer (8.11.1)

23

Sendmail 8.11.1 (Konfiguration)

```
$ /usr/newconfig/etc/mail/cf/cf> ./gen_cf tmp.cf

Select the options below with space   as the separator

1:  generate sendmail.cf with Relay ON [ Includes 9 10 13 options ]
2:  generate sendmail.cf with Relay OFF [ Default sendmail.cf file ]
3:  generate sendmail.cf with Relay_entire_domain
4:  generate sendmail.cf with Relay_based_on_MX
5:  generate sendmail.cf with Relay_hosts_only
6:  generate sendmail.cf with Access_db
7:  generate sendmail.cf with Relay_local_from
8:  generate sendmail.cf with Blacklist_recipients
9:  generate sendmail.cf with Accept_unresolvable_domains
10: generate sendmail.cf with Accept_unqualified_senders
11: generate sendmail.cf with Realtime Blackhole List
12: generate sendmail.cf with Loose_relay_check
13: generate sendmail.cf with Promiscuous_relay

h:  Help [ Number ] [all]
x:  Exit from selection
```

24

Bind 9

- Es handelt sich hierbei um einen komplett neugeschriebenen Nameserver, der zusätzliche Protokolle wie DNSSEC, TSIG und TKEY beinhaltet.

DNSSEC	- RFC2535 cryptographische Authentifizierung und Sicherstellung der Datenintegrität
TKEY	- Protokoll zur Verteilung von pre-shared Keys
Split DNS	- Aufteilung des Namensbereiches in "public" und "private"
Dynamic DNS	- Änderung der Einträge zur Laufzeit
TSIG	- Sicherstellung der Datenintegrität zwischen Resolver und Nameserver

25

TCPWrapper

- Erlaubt die Verwendung von /etc/hosts.deny oder /etc/hosts.allow zur Einschränkung des Zugriffs auf die verfügbaren Services

```
$ cat /etc/hosts.allow
##
# @(#)hosts.allow $Revision: 1.001 $ $Date: 01/08/08 14:50:49 $
#
# The lines in the file contain the service daemon list and
# the Internet addresses or names of the hosts and/or networks
# allowed to use those services.
# The form for each entry in this file is:
# <daemon list> : <client list> [: <option> [: <option> ...] ]
# See the hosts_access(5) and hosts_options(5) manual pages for
# more information.
##
ftpd : otto123@rem_host
ALL: LOCAL @some_netgroup
ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
```

26

JFS 3.3

- Mit JFS 3.3 und HFS stehen ACLs (Access Control Lists) zur Verfügung, mit denen der Zugriff auf Dateien und Verzeichnisse geregelt werden kann.

```
$ ll bsp.txt
-rw-------   1 root   sys             5 Sep 16 13:33 bsp.txt

$ setacl -m g:users:rw bsp.txt

$ ll bsp.txt
-rw-rw----+  1 root   sys             5 Sep 16 13:33
  bsp.txt8

$ getacl bsp.txt
# file: bsp.txt, owner: root, group: sys
user::rw-
group::---
group:users:rw-
class:rw-
other:---
```

27

SSL & HP-UX MD5 Secure Checksum

- SSL (Secure Socket Layer) Libraries
  - Ist die grundlegende Technologie zur Verschlüsselung von Daten im Bereich von Web-Applikationen.
- HP-UX MD5 Secure Checksum
  - Erlaubt ähnlich wie das cksum Kommando die Erzeugung von Check-Summen, z.B. zur Sicherstellung der Datenintegrität.
  - Dabei kommt ein besserer Algorythmus zum Einsatz

28

SSH

- Bietet verschlüsselte Verbindungen mit ähnlichen Funktionen wie telnet, rlogin und ftp, sowie die Möglichkeit andere TCP-Verbindungen zu tunneln.

  Paßwort-freie Zugriffe (sshd_config):

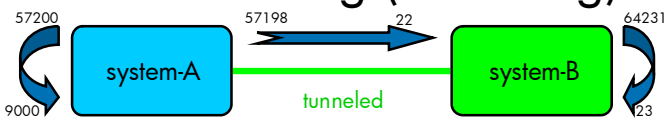
```
RSAAuthentication       yes
DSAAuthentication       yes
```

- SSH Port Forwarding (Tunneling)

```
$ ssh -n -N -L <local-port>:<remote-host>:<remote-port>
  <host> &
```

29

SSH Port Forwarding (Tunneling):



- Kommandos auf system-A:

```
$ ssh -n -N -L 9000:localhost:23 system-B &
$ telnet localhost 9000
```

- system-A - Verbindungen:

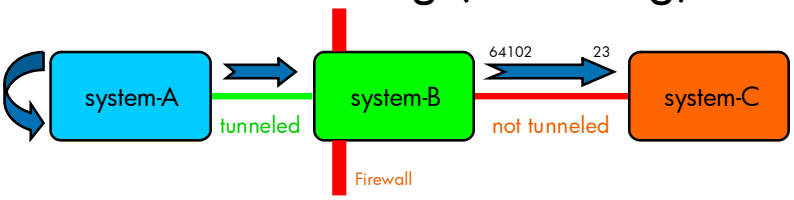
```
ssh  TCP  system-A:57198 -> system-B:22  (ESTABLISHED)
ssh  TCP  localhost:9000  (LISTEN)
ssh  TCP  localhost:9000 -> localhost:57200  (ESTABLISHED)
telnet  TCP  localhost:57200 -> localhost:9000  (ESTABLISHED)
```

- system-B - Verbindungen:

```
sshd TCP  system-B:22 -> system-A:57198  (ESTABLISHED)
sshd TCP  localhost:64231 -> localhost:telnet (ESTABLISHED)
```

30

SSH Port Forwarding (Tunneling):



- Kommandos auf system-A:

```
$ ssh -n -N -L 9000:system-C:23 system-B &
$ telnet localhost 9000
```

- system-A - Verbindungen:

```
ssh   TCP system-A:57119 -> system-B:22 (ESTABLISHED)
ssh   TCP localhost:9000 (LISTEN)
ssh   TCP localhost:9000 -> localhost:57119 (ESTABLISHED)
telnet TCP localhost:57119 -> localhost:9000 (ESTABLISHED)
```

- system-B - Verbindungen:

```
sshd  TCP system-B:22 -> system-A:57119 (ESTABLISHED)
sshd  TCP system-B:64102 -> system-C:telnet (ESTABLISHED)
```

- system-C – Verbindungen:

```
telnetd TCP system-C:23 -> system-B:64102(ESTABLISHED)
```

31

SSH X11 Forwarding:

Einträge in sshd_config
(auf dem <remote host>):

```
X11Forwarding       yes
X11DisplayOffset    10
```

Eintrag in der ssh_config:
(auf dem <client host>):

```
ForwardX11      yes
```

Beim Starten des Client:

```
$ ssh -X <user>@<host>
$ echo $DISPLAY <host>:10.0
```

Changeroot für SSH, SFTP und SCP:

- ab Version A.03.81 verfügbar für SSH und SFTP
- ab Version A.03.91 verfügbar für SCP
- die Konfiguration wird in den Release Notes beschrieben

32

HP-UX Strong Random Number Generator

- Zufallszahlen werden per Kernelmodul permanent generiert
- Durch die Implementierung im Kernel ist die Generierung der Zahlen zuverlässiger (ein Script könnte manipuliert werden) und schneller
- Das Tool stellt die Zufallszahlen über die Device Files /dev/random und /dev/urandom bereit
- Steht ab HP-UX 11.11 als Download zur Verfügung

33

Kerberos

- Kerberos stellt einen Mechanismus dar, bei dem sich ein Client bei einem Kerberos Server authentifiziert und dabei ein Ticket zurückbekommt. Dieses Ticket wird dann für die Nutzung der weiteren Service eingesetzt.

- Kerberos Server
- Kerberos Client
- SIS (Secure Internet Services)
  - Bietet Replacements für telnet, rlogin und ftp, die zur Authentifizierung anstelle von Klartextpaßworten den Kerberos-Mechanismus nutzen.

34

weitere Tools

- LDAP-UX Integration
  - Erlaubt die Nutzung eines LDAP-Servers zur Verwaltung der Unix-User – entweder über das NIS-LDAP-Gateway oder über den LDAP-UX Client.
- CIFS/9000 (Samba)
  - Ist ein Unix-basierender File-Server für Windows-Netzwerke.
  - Bietet die Möglichkeit, die Paßwortabfragen der Unix-User gegen einen NT-Server zu stellen.
- HP-UX AAA Server (Radius)
  - "Remote Authentication Dial In User Service" ist ein Standard-Dienst für Remote-Authentifizierung, gemäß RFC 2865/2866.

35

weitere Tools

- Boot Authenticator for Standard Mode of HP-UX (HP-UX 11.11)
  - Erlaubt das Setzen eines Boot-Passwortes, das eingegeben werden muss, bevor das System im Single-User-Mode genutzt werden kann.
  - Dazu muss kein Trusted System mehr konfiguriert werden.
- HP-UX Shadow Passwords
  - Implementiert die Verwendung der Datei /etc/shadow
  - Bietet die Möglichkeit, Shadow-Passworte zu nutzen ohne ein Trusted System zu konfigurieren.
- HP-UX Role-based Access Control (HP-UX 11.23)
  - Stellt derzeit eine ähnliche Funktionalität zur Verfügung wie "sudo".
  - Wird jedoch offiziell auf HP-UX supportet.

36

HP-UX Internet Express A.04.00

(ab HP-UX 11.11)

- enthält eine Vielzahl an Public-Domain-Tools enthält, die darin für HP-UX gesammelt wurden:

hpuxiexpress1 A.04.00-008
Axis A.04.00-1.1
Curl A.04.00-7.12.1.002
DanteSOCKS A.04.00-1.1.15
Fetchmail A.04.00-6.2.5
Horde A.04.00-2.2.7
IMP A.04.00-3.2.5
Jetty A.04.00-5.1.0
MySQL A.04.00-4.0.24
OpenJMS A.04.00-0.7.6.1
PAM_mkhomedir A.04.00-1.0
Pine A.04.00-4.61
ProFTPD A.04.00-1.2.10
Snort A.04.00-2.3.0
SSLDUMP-A.04.00-0.9b3
Tcpdump A.04.00-3.8.3
VOCAL A.04.00-1.5.0
Xinetd A.04.00-2.3.13

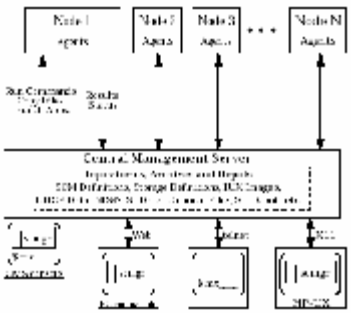
hpuxiexpress2 A.04.00-006
Calamaris A.04.00-2.59
Cyrus IMAP A.04.00-2.2.12
Eclipse A.04.00-3.0.004
FSH A.04.00-1.2
HSQLDB A.04.00-1.7.2.4
Jabber A.04.00-1.4.3.1
Libpcap A.04.00-0.8.3
Nessus A.04.00-2.0.12
OpenLDAP A.04.00-2.2.15.002
PAM_passwdqc A.04.00-0.7.5
PostgreSQL A.04.00-7.4.7
Qpopper A.04.00-4.0.5
SOAP A.04.00-2.3.1
Stunnel A.04.00-4.05
UDDI4J A.04.00-2.0.2
Xalan-C A.04.00-1.8.002

Ant A.04.00-1.6.2
Clam AntiVirus A.04.00-0.82
Cyrus SASL A.04.00-2.1.20
Ethereal A.04.00-0.10.10
Globus A.04.00-3.2.1
Hypermail A.04.00 2.1.8
JBoss A.04.00-4.0.0.002
Majordomo A.04.00-1.94.5
Net-SNMP A.04.00-5.1.2a
OpenSAML A.04.00-1.0
Perl-LDAP A.04.00 0.3202
ProcMail A.04.00-3.22
SmartFrog A.04.00-3.04.004
Squid A.04.00-2.59
Sudo A.04.00-1.6.8p4
UW-IMAP A.04.00-2004c
Xerces-C A.04.00-2.6.0.002

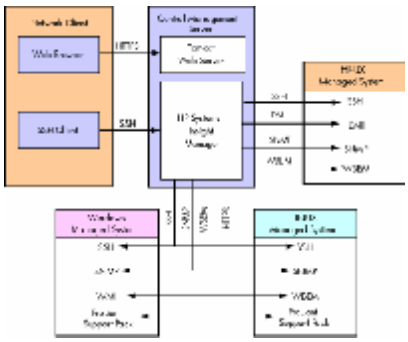
37

SCM (Service Control Manager) SIM (Systems Insight Manager)

- Bietet die Möglichkeit normalen Usern über eine Management-Station die Ausführung bestimmter Admin-Aufgaben auf festgelegten Rechnern im Netzwerk zu gestatten.



SCM



SIM

38

Schnittstellen

- PAM (Pluggable Authentication Module)
  - Erlaubt die Einbindung unterschiedlicher Authentifizierungs-mechanismen, wie NTLM, LDAP und DCE.

Libraries:

- libpam_unix.1 - Unix
- libpam_ldap.1 - LDAP Server
- libpam_ntlm.1 - NT-Server
- libpam_krb5.1 - Kerberos Server
- libpam_dce.1 - DCE (Integrated Login)

39

PAM

```
login  auth sufficient    /usr/lib/security/libpam_ntlm.1
login  auth required      /usr/lib/security/libpam_unix.1 try_first_pass
OTHER  auth sufficient    /usr/lib/security/libpam_ntlm.1
OTHER  auth required      /usr/lib/security/libpam_unix.1 try_first_pass

login  account sufficient /usr/lib/security/libpam_ntlm.1
login  account required   /usr/lib/security/libpam_unix.1
OTHER  account sufficient /usr/lib/security/libpam_ntlm.1
OTHER  account required   /usr/lib/security/libpam_unix.1

login  session required   /usr/lib/security/libpam_unix.1
OTHER  session required   /usr/lib/security/libpam_unix.1

login  password required  /usr/lib/security/libpam_ntlm.1
login  password required  /usr/lib/security/libpam_unix.1 use_first_pass
OTHER  password required  /usr/lib/security/libpam_ntlm.1
OTHER  password required  /usr/lib/security/libpam_unix.1 use_first_pass
```

40

Schnittstellen

- NSS (Name Service Switch)
  - Bietet die Möglichkeit verschiedene Dienste, wie DNS, NIS, LDAP oder lokale Dateien zur Namesauflösung zu verwenden.

```
$ cat /etc/nsswitch.conf
# File: nsswitch.conf
passwd:         files
group:          files
#hosts:         dns [TRYAGAIN=continue NOTFOUND=continue] files
hosts:          files [TRYAGAIN=continue NOTFOUND=continue] dns
services:       nis files
protocols:      files
networks:       files
rpc:            files
netgroup:       files
```

41

Schnittstellen

- GSS-API (Generic Security Services)
  - Eine RFC-2743 konforme Programmierschnittstelle für Securitymechanismen und –protokolle von Client-/Server-Anwendungen.
- CDSA (Common Data Security Architecture)
  - Es handelt sich hierbei um eine Programmierschnittstelle, deren Module zur Daten-Verschüsselung, Zertifikat-Verwaltung und Trustverwaltung genutzt werden können.

42

Literatur / Informationen

- Online-Literatur:
  - http://www.hp.com/security
  - http://docs.hp.com
- Literatur:
  - hp-ux 11i security
    Autor: Chris Wong
    ISBN 0-13-033062-0

- Software-Downloads:
  - http://software.hp.com
- Security-Bulletins:
  - http://itrc.hp.com
  - "search the technical knowledge base" (im Bereich "Maintenance und Support")
  - "Security Bulletin Archive" (ganz unten mittig, unter "Related Links")

43

invent

22