Practical Solaris Security Administration

Roy Gertig

SCSA Security+ IAM CISSP

A+ N+ I-Net+ IT-Project+ CIW-A TCC

08/05/04

Science Applications International Corporation
An Employee-Owned Company

Presenter

NEbraskaCERT

- Roy Gertig
- Affiliations: (ISC)^2, Infragard, NEbraskaCert, CompTIA, etc.
- Contact:
  - gertigr@stratcom.mil
  - (402) 232-6159
- Style: Ad hoc

What this presentation won't do

NEbraskaCERT

- Won't make you an expert on Solaris Security
  - Won't make me one either
- Won't cover EVERYTHING about Solaris Security
- Won't guarantee that if you try any of the suggestions that difficulties will not happen
  - Standard DISCLAIMER so I can keep my house
  - Backup your system and/or have a test/dev system
- Won't make your system 100% secure

What presentation was designed to do

NEbraskaCERT

- Impart some knowledge on solaris security
  - Info you may not have thought about
  - Have some fun during the session
- Present basic suggestions for securing solaris
- Present some info on tools for testing
- Let's start from the beginning

Scenario

NEbraskaCERT

- You are the CIO of a service corporation
  - It's morning –
- Chief of the DBA shop rushes in and disturbs your serenity
- You're lucky day! The CFO just happens to come into your office

Let's Talk Security

NEbraskaCERT

- Earlier referred to "100% secure"

Terms

- SLE * ARO = ALE
- SLE = Single Loss Expectancy
- ARO = Annualized Rate of Occurrence
- ALE = Annualized Loss Expectancy
- SLE = Asset Value * Exposure Factor
- Exposure Factor = 0 to 100% Loss

Let's Talk Security Policy

NEbraskaCERT

- Security is a compromise – not an absolute
- How much are you willing to risk?
- Whatever the risk - Your security policy must be supported from the top down.

How Much is Enough?

NEbraskaCERT

- What is the minimum installation cluster you can install and still function?
  - Core - 62 pkgs
  - End User – 313 pkgs
  - Developer – 390 pkgs
  - Entire Distribution + OEM – 459 pkgs

- According to Noordergraaf, he installed a functional secure server with less than 20 pkgs – 36MB

Patch Management

NEbraskaCERT

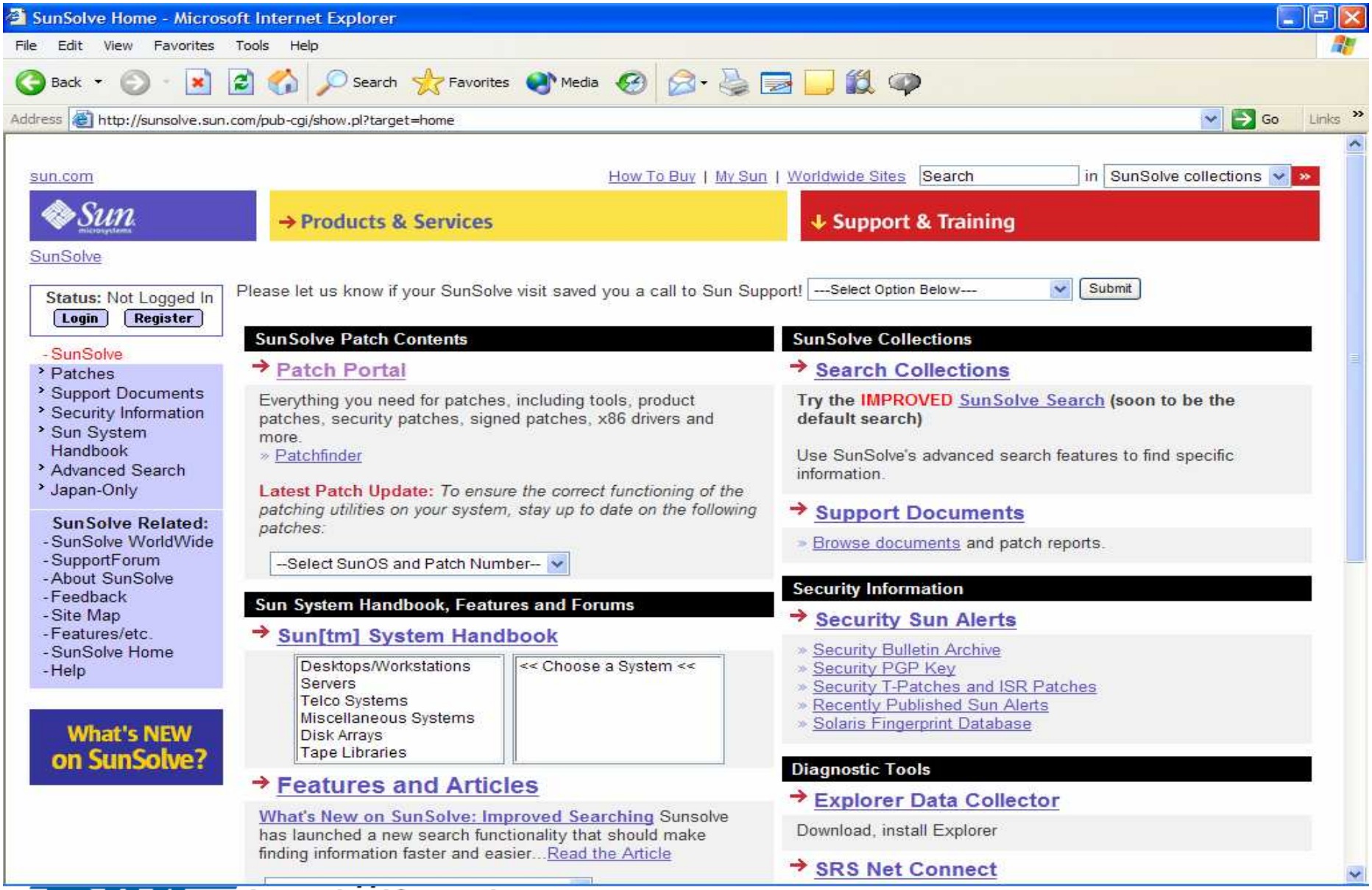
- <Patch Portal for Solaris>

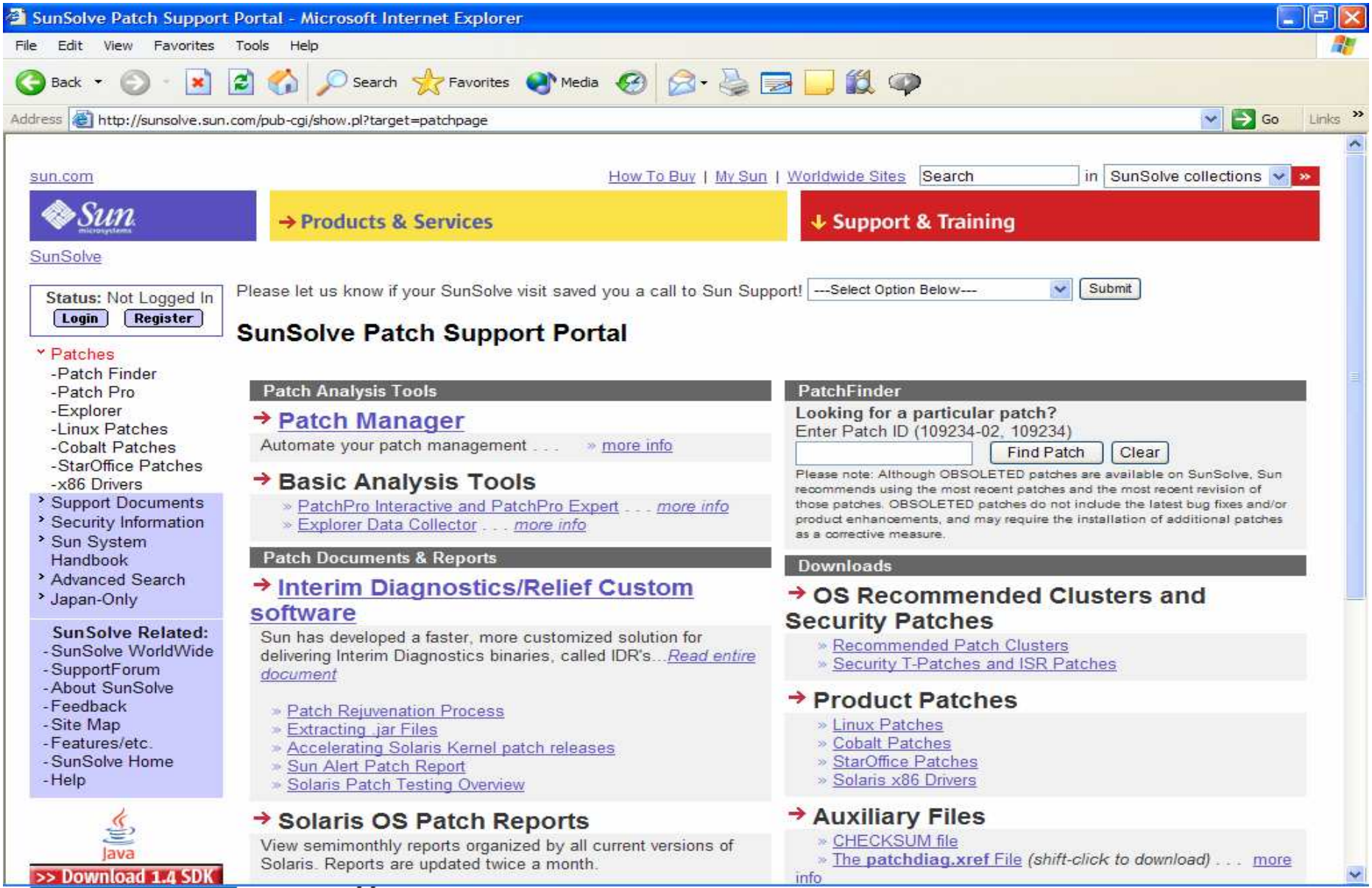
http://sunsolve.sun.com/pub-cgi/show.pl?target=home

- Download and install recommended OS and security patch clusters
  - Read patchinfo as a reboot may be required
- Check system and remove and unneeded pkgs Run Tripwire against it and get a good "snapshot"
- Bring system down to the "OK" prompt

sunsolve.sun.com

NEbraskaCERT




SunSolve Patch Support Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage
Go Links
sun.com
How To Buy | My Sun | Worldwide Sites
Search in SunSolve collections
Products & Services
Support & Training
SunSolve
Status: Not Logged In
Login Register
Please let us know if your SunSolve visit saved you a call to Sun Support!
---Select Option Below---
Submit
SunSolve Patch Support Portal
Patches
-Patch Finder
-Patch Pro
-Explorer
-Linux Patches
-Cobalt Patches
-StarOffice Patches
-x86 Drivers
Support Documents
Security Information
Sun System Handbook
Advanced Search
Japan-Only
SunSolve Related:
-SunSolve WorldWide
-SupportForum
-About SunSolve
-Feedback
-Site Map
-Features/etc.
-SunSolve Home
-Help
Java
>> Download 1.4 SDK
Patch Analysis Tools
Patch Manager
Automate your patch management . . . » more info
Basic Analysis Tools
» PatchPro Interactive and PatchPro Expert . . . more info
» Explorer Data Collector . . . more info
Patch Documents & Reports
Interim Diagnostics/Relief Custom software
Sun has developed a faster, more customized solution for delivering Interim Diagnostics binaries, called IDR's...Read entire document
» Patch Rejuvenation Process
» Extracting .jar Files
» Accelerating Solaris Kernel patch releases
» Sun Alert Patch Report
» Solaris Patch Testing Overview
Solaris OS Patch Reports
View semimonthly reports organized by all current versions of Solaris. Reports are updated twice a month.
PatchFinder
Looking for a particular patch?
Enter Patch ID (109234-02, 109234)
Find Patch Clear
Please note: Although OBSOLETED patches are available on SunSolve, Sun recommends using the most recent patches and the most recent revision of those patches. OBSOLETED patches do not include the latest bug fixes and/or product enhancements, and may require the installation of additional patches as a corrective measure.
Downloads
OS Recommended Clusters and Security Patches
» Recommended Patch Clusters
» Security T-Patches and ISR Patches
Product Patches
» Linux Patches
» Cobalt Patches
» StarOffice Patches
» Solaris x86 Drivers
Auxiliary Files
» CHECKSUM file
» The patchdiag.xref File (shift-click to download) . . . more info

Open Boot Prom (OBP)

NEbraskaCERT

```
# eeprom
tpe-link-test?=true
scsi-initiator-id=7
keyboard-click?=false
keymap: data not available.
ttyb-rts-dtr-off=false
ttyb-ignore-cd=true
ttya-rts-dtr-off=false
ttya-ignore-cd=true
ttyb-mode=9600,8,n,1,-
ttya-mode=9600,8,n,1,-
pcia-probe-list=1,2,3,4
pcib-probe-list=1,2,3
mfg-mode=off
diag-level=min
#power-cycles=44
system-board-serial#: data not available.
system-board-date=
fcode-debug?=false
output-device=screen
input-device=keyboard
load-base=16384
boot-command=boot
auto-boot?=false
watchdog-reboot?=false
diag-file: data not available.
diag-device=net
boot-file: data not available.
boot-device=disk:a disk
local-mac-address?=false
ansi-terminal?=true
screen-#columns=80
screen-#rows=34
silent-mode?=false
use-nvramrc?=false
nvramrc: data not available.
security-mode=command
security-password: data not available.
security-#badlogins=10
oem-logo: data not available.
oem-logo?=false
oem-banner: data not available.
oem-banner?=false
hardware-revision: data not available.
last-hardware-update: data not available.
diag-switch?=false
```

OPB

diag-switch?=false

security-#badlogins

OPB Security is the First Line

security-mode?=

none, command, full

security-password

Can be set in OBP mode or in run levels using eeprom

/etc files

NEbraskaCERT

- /etc/inittab
- /etc/rcX.d
- /etc/system
- /etc/passwd
- /etc/shadow
- /etc/default/login
- /etc/default/passwd
- /etc/default/kbd
- /etc/default/su
- /etc/inet/inetd.conf
- /etc/hosts.allow
- /etc/hosts.deny
- /etc/hosts.equiv
- .rhosts file

System Startup

/etc/inittab

NEbraskaCERT

```
# cat /etc/inittab
ap::sysinit:/sbin/autopush -f /etc/iu.ap
ap::sysinit:/sbin/soconfig -f /etc/sock2path
fs::sysinit:/sbin/rcS sysinit          >/dev/msglog 2<>/dev/msglog </dev/console
is:3:initdefault:
p3:s1234:powerfail:/usr/sbin/shutdown -y -i5 -g0 >/dev/msglog 2<>/dev/msglog
sS:s:wait:/sbin/rcS                    >/dev/msglog 2<>/dev/msglog </dev/console
s0:0:wait:/sbin/rc0                    >/dev/msglog 2<>/dev/msglog </dev/console
s1:1:respawn:/sbin/rc1                 >/dev/msglog 2<>/dev/msglog </dev/console
s2:23:wait:/sbin/rc2                   >/dev/msglog 2<>/dev/msglog </dev/console
s3:3:wait:/sbin/rc3                    >/dev/msglog 2<>/dev/msglog </dev/console
s5:5:wait:/sbin/rc5                    >/dev/msglog 2<>/dev/msglog </dev/console
s6:6:wait:/sbin/rc6                    >/dev/msglog 2<>/dev/msglog </dev/console
fw:0:wait:/sbin/uadmin 2 0             >/dev/msglog 2<>/dev/msglog </dev/console
of:5:wait:/sbin/uadmin 2 6             >/dev/msglog 2<>/dev/msglog </dev/console
rb:6:wait:/sbin/uadmin 2 1             >/dev/msglog 2<>/dev/msglog </dev/console
sc:234:respawn:/usr/lib/saf/sac -t 300
co:234:respawn:/usr/lib/saf/ttymon -g -h -p "`uname -n` console login: " -T sun -d
dev/console -l console -m ldterm,ttcompat
#
```

/etc/rc scripts

NEbraskaCERT

- /etc/inittab starts /sbin/rcX which fire off the pertinent rc scripts in the /etc/rcX.d directory
  - Key here is to disable unneeded services by changing the name of the script name, ie, mv S71rpc s71rpc. If the "capital S" or "capital K" is not seen, script will not start.

/etc/rc2.d file

NEbraskaCERT

- K07dmi
- S70uucp
- S75cron
- S91afbinit
- K07snmpdx
- S71ldap.client
- S75flashprom
- S91ifbinit
- K28nfs.server
- S71rpc
- S75savecore
- S92volmgt
- S71sysid.sys
- S76nscd
- S93cacheos.finish
- S01MOUNTFSYS
- S72autoinstall
- S80PRESERVE
- S94ncalogd
- S05RMTMPFILES
- S72inetsvc
- S80lp
- S95IIim
- S20sysetup
- S72slpd
- S80spc
- S95amiserv
- S21perf
- S73cachefs.daemon
- S85power
- S95ocfserv
- S30sysid.net
- S73nfs.client
- S88sendmail
- S99audit
- S40llc2
- S74autofs
- S88utmpd
- S99dtlogin
- S47asppp
- S74syslog
- S89bdconfig
- S69inet
- S74xntpd
- S90wbem

/etc/passwd and shadow

NEbraskaCERT

```
# ls -l /etc/passwd
-r--r--r--   1 root     sys          488 Oct  8  2002 /etc/passwd
# more /etc/passwd
root:x:0:1:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
gertigr:x:1001:14:Roy Gertig, BJ-2/4, 2-6159:/export/home/gertigr:/bin/sh
# ls -l /etc/shadow
-r--------   1 root     sys          280 Oct  8  2002 /etc/shadow
# more /etc/shadow
root:n9PndAcwEx5NI:6445::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
lp:NP:6445::::::
uucp:NP:6445::::::
nuucp:NP:6445::::::
listen:*LK*:::::::
nobody:NP:6445::::::
noaccess:NP:6445::::::
nobody4:NP:6445::::::
gertigr:ST04RoW2By8JE:11968::::::
```

/etc/passwd (cont'd)

NEbraskaCERT

- # passwd –l <user> to lock an account
- # passwd –n 10 -x 7 to lock a passwd
  - Keep users from changing by setting minimum greater than maximum
- # passwd –f <user> to change passwd next login
- # passwd –n 30 <user> to change passwd every 30 days
- usermod to modify the file
- userdel to delete an account
- pwconv to clean up passwd / shadow files

/etc/default/login (1)

NEbraskaCERT

```
# more login
#ident  "@(#)login.dfl  1.10    99/08/04 SMI"   /* SVr4.0 1.1.1.1       */

# Set the TZ environment variable of the shell.
#
#TIMEZONE=EST5EDT

# ULIMIT sets the file size limit for the login.  Units are disk blocks.
# The default of zero means no limit.
#
#ULIMIT=0

# If CONSOLE is set, root can only login on that device.
# Comment this line out to allow remote login by root.
#
CONSOLE=/dev/console

# PASSREQ determines if login requires a password.
#
PASSREQ=YES

# ALTSHELL determines if the SHELL environment variable should be set
#
ALTSHELL=YES

# PATH sets the initial shell PATH variable
#
#PATH=/usr/bin:

# SUPATH sets the initial shell PATH variable for root
#
#SUPATH=/usr/sbin:/usr/bin

# TIMEOUT sets the number of seconds (between 0 and 900) to wait before
# abandoning a login session.
#
#TIMEOUT=300

# UMASK sets the initial shell file creation mode mask.  See umask(1).
#
#UMASK=022
```

/etc/default/login (2)

NEbraskaCERT

```
# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
# to log all root logins at level LOG_NOTICE and multiple failed login
# attempts at LOG_CRIT.
#
SYSLOG=YES

# SLEEPTIME controls the number of seconds that the command should
# wait before printing the "login incorrect" message when a
# bad password is provided.  The range is limited from
# 0 to 5 seconds.
#
#SLEEPTIME=4

# RETRIES determines the number of failed logins that will be
# allowed before login exits.
#
#RETRIES=5
#
# The SYSLOG_FAILED_LOGINS variable is used to determine how many failed
# login attempts will be allowed by the system before a failed login
# message is logged, using the syslog(3) LOG_NOTICE facility.  For example,
# if the variable is set to 0, login will log -all- failed login attempts.
#
#SYSLOG_FAILED_LOGINS=5
```

- touch /var/adm/loginlog
- chmod 600 /var/adm/loginlog
- chgrp sys /var/adm/loginlog

/etc/default/passwd & kbd

NEbraskaCERT

```
# more passwd
#ident  "@(#)passwd.dfl 1.3     92/07/14 SMI"
MAXWEEKS=
MINWEEKS=
PASSLENGTH=6
# more kbd
#pragma ident   "@(#)kbd.dfl    1.3     99/05/04 SMI"
#
# Copyright 1996, 1999 by Sun Microsystems, Inc.
# All Rights Reserved.
#
# /etc/default/kbd
#
# kbd default settings processed via kbd(1).
#
# KEYBOARD_ABORT affects the default behavior of the keyboard abort
# sequence, see kbd(1) for details.  The default value is "enable". The
# optional values are "disable" or "alternate". Any other value is ignored.
# If you choose "alternate" it will affect the serial console drivers  ONLY.
# The keyboard BREAK (sequence and plug/unplug) won't be affected by this.
# If "alternate" is in effect any protocol (PPP, SLIP... etc) should not be
# run over the serial console port.
#
# KEYCLICK affects the default keyclick behavior. Possible values are
# 'on' and 'off'.  Any other value is ignored. The default behavior is
# to leave the current keyclick setting unchanged.
#
# Uncomment the following line to disable keyboard or serial device
# abort sequences:
#KEYBOARD_ABORT=disable

# Uncomment the following line to enable a non-BREAK alternate
# serial input device abort sequence:
#KEYBOARD_ABORT=alternate

# Uncomment the following line to change the keyclick behavior:
#KEYCLICK=off
```

/etc/default/su

NEbraskaCERT

```
# cat su
#ident  "@(#)su.dfl     1.6     93/08/14 SMI"   /* SVr4.0 1.2   */

# SULOG determines the location of the file used to log all su attempts
#
SULOG=/var/adm/sulog

# CONSOLE determines whether attempts to su to root should be logged
# to the named device
#
#CONSOLE=/dev/console

# PATH sets the initial shell PATH variable
#
#PATH=/usr/bin:

# SUPATH sets the initial shell PATH variable for root
#
#SUPATH=/usr/sbin:/usr/bin

# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
# to log all su attempts.  LOG_NOTICE messages are generated for su's to
# root, LOG_INFO messages are generated for su's to other users, and LOG_CRIT
# messages are generated for failed su attempts.
#
SYSLOG=YES
```

Directory and File Level Security

NEbraskaCERT

- Directories so far should be owned by root
  - root should read, write, exec; group and others maybe read
- Check for proper SUID, SGID, and "sticky bit"
  - # find / -type f \ (-perm -u+s -o -perm -g+s \) -ls
- fix-modes file
  - http://jsecom16b.sun.com/ECom/EComActionServlet?StoreId=8&PartDetailId=817-0074-10&TransactionId=try&LMLoadBalanced=
    - Requires Login ID and password
- Use "Directory Shadowing"
- Access Control Lists (ACLs) for finer access tuning
  - getfacl
  - setfacl

File System Security

NEbraskaCERT

- Some file systems in the /etc/vfstab file can have options to mount with nosuid, ro.
  - Before doing, make sure no Directories or Files need nosuid, ro.

Network Security

/etc/inet/inetd.conf (1)

NEbraskaCERT

```
# more inetd.conf
#
#ident  "@(#)inetd.conf 1.44    99/11/25 SMI"   /* SVr4.0 1.5   */
#
#
# Configuration file for inetd(1M).  See inetd.conf(4).
#
# To re-configure the running inetd process, edit this file, then
# send the inetd process a SIGHUP.
#
# Syntax for socket-based Internet services:
#  <service_name> <socket_type> <proto> <flags> <user> <server_pathname> <args>
#
# Syntax for TLI-based Internet services:
#
#  <service_name> tli <proto> <flags> <user> <server_pathname> <args>
#
# IPv6 and inetd.conf
# By specifying a <proto> value of tcp6 or udp6 for a service, inetd will
# pass the given daemon an AF_INET6 socket.  The following daemons have
# been modified to be able to accept AF_INET6 sockets
#
#       ftp telnet shell login exec tftp finger printer
#
# and service connection requests coming from either IPv4 or IPv6-based
# transports.  Such modified services do not normally require separate
# configuration lines for tcp or udp.  For documentation on how to do this
# for other services, see the Solaris System Administration Guide.
#
# You must verify that a service supports IPv6 before specifying <proto> as
# tcp6 or udp6.  Also, all inetd built-in commands (time, echo, discard,
# daytime, chargen) require the specification of <proto> as tcp6 or udp6
#
# The remote shell server (shell) and the remote execution server
# (exec) must have an entry for both the "tcp" and "tcp6" <proto> values.
#
# Ftp and telnet are standard Internet services.
#
ftp     stream  tcp6    nowait  root    /usr/sbin/in.ftpd       in.ftpd
telnet  stream  tcp6    nowait  root    /usr/sbin/in.telnetd    in.telnetd
#
```

/etc/inet/inetd.conf (2)

NEbraskaCERT

```
# Tnamed serves the obsolete IEN-116 name server protocol.
#
name    dgram   udp     wait    root    /usr/sbin/in.tnamed     in.tnamed
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
shell   stream  tcp     nowait  root    /usr/sbin/in.rshd       in.rshd
shell   stream  tcp6    nowait  root    /usr/sbin/in.rshd       in.rshd
login   stream  tcp6    nowait  root    /usr/sbin/in.rlogind    in.rlogind
exec    stream  tcp     nowait  root    /usr/sbin/in.rexecd     in.rexecd
exec    stream  tcp6    nowait  root    /usr/sbin/in.rexecd     in.rexecd
comsat  dgram   udp     wait    root    /usr/sbin/in.comsat     in.comsat
talk    dgram   udp     wait    root    /usr/sbin/in.talkd      in.talkd
#
# Must run as root (to read /etc/shadow); "-n" turns off logging in utmp/wtmp.
#
uucp    stream  tcp     nowait  root    /usr/sbin/in.uucpd      in.uucpd
#
# Tftp service is provided primarily for booting.  Most sites run this
# only on machines acting as "boot servers."
#
#tftp   dgram   udp6    wait    root    /usr/sbin/in.tftpd      in.tftpd -s /tftpboot
```

/etc/inet/inetd.conf (3)

NEbraskaCERT

```
#tftp   dgram   udp6    wait    root    /usr/sbin/in.tftpd      in.tftpd -s /tftpboot
#
# Finger, systat and netstat give out user information which may be
# valuable to potential "system crackers."  Many sites choose to disable
# some or all of these services to improve security.
#
finger  stream  tcp6    nowait  nobody  /usr/sbin/in.fingerd    in.fingerd
#systat stream  tcp     nowait  root    /usr/bin/ps             ps -ef
#netstat        stream  tcp     nowait  root    /usr/bin/netstat        netstat -f inet
#
# Time service is used for clock synchronization.
#
time    stream  tcp6    nowait  root    internal
time    dgram   udp6    wait    root    internal
#
# Echo, discard, daytime, and chargen are used primarily for testing.
#
echo    stream  tcp6    nowait  root    internal
echo    dgram   udp6    wait    root    internal
discard stream  tcp6    nowait  root    internal
discard dgram   udp6    wait    root    internal
daytime stream  tcp6    nowait  root    internal
daytime dgram   udp6    wait    root    internal
chargen stream  tcp6    nowait  root    internal
chargen dgram   udp6    wait    root    internal
#
#
# RPC services syntax:
#  <rpc_prog>/<vers> <endpoint-type> rpc/<proto> <flags> <user> \
#  <pathname> <args>
#
# <endpoint-type> can be either "tli" or "stream" or "dgram".
# For "stream" and "dgram" assume that the endpoint is a socket descriptor.
# <proto> can be either a nettype or a netid or a "*". The value is
# first treated as a nettype. If it is not a valid nettype then it is
# treated as a netid. The "*" is a short-hand way of saying all the
# transports supported by this system, ie. it equates to the "visible"
# nettype. The syntax for <proto> is:
#       *|<nettype|netid>|<nettype|netid>{[,<nettype|netid>]}
# For example:
# dummy/1       tli     rpc/circuit_v,udp       wait    root    /tmp/test_svc   test_svc
#
# Solstice system and network administration class agent server
100232/10       tli     rpc/udp wait root /usr/sbin/sadmind     sadmind
```

/etc/inet/inetd.conf (4)

NEbraskaCERT

```
# Rquotad supports UFS disk quotas for NFS clients
#
rquotad/1       tli     rpc/datagram_v  wait root /usr/lib/nfs/rquotad  rquotad
#
# The rusers service gives out user information.  Sites concerned
# with security may choose to disable it.
#
rusersd/2-3     tli     rpc/datagram_v,circuit_v        wait root /usr/lib/netsvc/rusers/rpc.rusersd
usersd
#
# The spray server is used primarily for testing.
#
sprayd/1        tli     rpc/datagram_v  wait root /usr/lib/netsvc/spray/rpc.sprayd      rpc.sprayd
#
# The rwall server allows others to post messages to users on this machine.
#
walld/1         tli     rpc/datagram_v  wait root /usr/lib/netsvc/rwall/rpc.rwalld      rpc.rwalld
```

/etc/inet/inetd.conf (5)

NEbraskaCERT

```
# The rwall server allows others to post messages to users on this machine.
#
walld/1         tli     rpc/datagram_v  wait root /usr/lib/netsvc/rwall/rpc.rwalld      rpc.rwalld
#
# Rstatd is used by programs such as perfmeter.
#
rstatd/2-4      tli   rpc/datagram_v wait root /usr/lib/netsvc/rstat/rpc.rstatd rpc.rstatd
#
# The rexd server provides only minimal authentication and is often not run
#
#rexd/1          tli  rpc/tcp wait root /usr/sbin/rpc.rexd     rpc.rexd
#
# rpc.cmsd is a data base daemon which manages calendar data backed
# by files in /var/spool/calendar
#
#
# Sun ToolTalk Database Server
#
100083/1        tli     rpc/tcp wait root /usr/dt/bin/rpc.ttdbserverd rpc.ttdbserverd
#
# UFS-aware service daemon
#
#ufsd/1 tli     rpc/*   wait    root    /usr/lib/fs/ufs/ufsd    ufsd -p
#
# Sun KCMS Profile Server
#
100221/1        tli     rpc/tcp wait root /usr/openwin/bin/kcms_server  kcms_server
#
# Sun Font Server
#
fs              stream  tcp     wait nobody /usr/openwin/lib/fs.auto    fs
#
# CacheFS Daemon
#
100235/1 tli rpc/tcp wait root /usr/lib/fs/cachefs/cachefsd cachefsd
#
# Kerberos V5 Warning Message Daemon
#
100134/1        tli     rpc/ticotsord   wait    root    /usr/lib/krb5/ktkt_warnd ktkt_warnd
```

/etc/inet/inetd.conf (6)

NEbraskaCERT

```
# Print Protocol Adaptor - BSD listener
#
printer         stream  tcp6    nowait  root    /usr/lib/print/in.lpd   in.lpd
#
# GSS Daemon
#
100234/1        tli     rpc/ticotsord   wait    root    /usr/lib/gss/gssd gssd
#
# AMI Daemon
#
100146/1        tli     rpc/ticotsord   wait    root    /usr/lib/security/amiserv       amiserv
100147/1        tli     rpc/ticotsord   wait    root    /usr/lib/security/amiserv       amiserv
#
# OCF (Smart card) Daemon
#
100150/1        tli     rpc/ticotsord   wait    root    /usr/sbin/ocfserv       ocfserv
dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
100068/2-5 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd
sun-dr  stream  tcp6    wait    root    /usr/lib/dcs    dcs
300326/4        tli     rpc/tcp wait    root    /platform/SUNW,Ultra-Enterprise-10000/lib/dr_daemon     dr
emon
```

TCP Wrappers

NEbraskaCERT

- Wietse Venema's TCP Wrappers
  - ftp://ftp.porcupine.org/pub/security/index.html
  - http://www.cert.org/security-improvement/implementations/i041.07.html
- Must configure /etc/hosts.allow and hosts.deny
- Set /etc/syslog.conf for appropriate logging.

/etc/default/inetinit

NEbraskaCERT

- TCP_STRONG_ISS=1 to TCP_STRONG_ISS=2
- Or on the fly # ndd -set /dev/tcp tcp_strong_iss 2

Network Security Settings

NEbraskaCERT

- Using the ndd command to adjust kernel params
  - Commands to list current parameters
    - ndd –get /dev/ip \?
    - ndd –get /dev/tcp \?
    - ndd –get /dev/udp \?
    - ndd –get /dev/arp \?
    - ndd –get /dev/icmp \?
    - ndd –get /dev/hme \? (for host HBA interface)
    - ndd –get /dev/tcp tcp_rev_src_routes

SYN Flood Alleviation

NEbraskaCERT

- ndd -set /dev/tcp tcp_conn_req_max_q0 4096

Connection Exhaustion Attack

NEbraskaCERT

- ndd -set /dev/tcp tcp_conn_req_max_q 1024

Disable Source Routed Packets

NEbraskaCERT

- ndd -set /dev/ip ip_forward_src_routed 0

Disable IP Forwarding

NEbraskaCERT

- ndd -set /dev/ip ip_forwarding 0
- /etc/notrouter

Disable Directed Broadcasts

NEbraskaCERT

- ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
- ndd -set /dev/ip ip_respond_to_echo_broadcast 0
- ndd -set /dev/ip ip_respond_to_timestamp 0
- ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
- ndd -set /dev/ip ip_forward_directed_broadcasts 0

Disable ICMP Redirect

NEbraskaCERT

- ndd -set /dev/ip ip_ignore_redirect 1

Disable ARP Attacks

NEbraskaCERT

- ndd -set /dev/arp arp_cleanup_interval 60000

Disable Buffer Overflow

NEbraskaCERT

- set noexec_user_stack=1
  set noexec_user_stack_log=1

Auditing and Audit Logs

- As soon as bsmconv is run, the file /var/audit is created.
- /var/adm/messages
- /var/adm/sulog
- /var/adm/vold.log
- /var/adm/wtmpx
- /var/cron/log
- /var/adm/loginlog
- /var/log/syslog
- praudit, auditconfig, auditreduce

/var/adm/sulog

NEbraskaCERT

```
# more /var/adm/sulog
SU 09/27 10:22 + ??? root-uucp
SU 10/08 12:26 + pts/4 root-gertigr
SU 10/08 12:29 + pts/4 gertigr-root
SU 10/08 12:30 + pts/4 gertigr-root
SU 11/25 11:07 + console gertigr-root
SU 11/25 11:18 + pts/4 gertigr-root
SU 11/27 09:11 + pts/5 gertigr-root
SU 12/02 10:16 + pts/7 gertigr-root
SU 01/14 15:10 + pts/9 gertigr-root
SU 01/14 15:45 + pts/9 gertigr-root
SU 01/14 16:04 + pts/10 gertigr-root
SU 01/21 13:29 + pts/10 gertigr-root
SU 02/19 14:31 + pts/8 gertigr-root
SU 05/22 11:07 - pts/9 gertigr-root
SU 05/22 11:07 + pts/9 gertigr-root
SU 10/15 10:09 + pts/4 gertigr-root
SU 10/17 12:01 + pts/6 gertigr-root
SU 10/28 13:51 + pts/9 gertigr-root
SU 12/05 08:49 + pts/10 gertigr-root
SU 12/05 08:40 + pts/5 gertigr-root
SU 12/05 08:41 + pts/7 gertigr-root
SU 12/05 09:34 + pts/8 gertigr-root
SU 01/05 09:18 + pts/5 gertigr-root
SU 01/05 09:19 + pts/7 gertigr-root
SU 01/06 11:38 + pts/4 gertigr-root
SU 05/11 19:32 + pts/9 gertigr-root
SU 05/11 19:33 + console root-root
SU 05/11 19:40 - pts/4 gertigr-root
SU 05/11 19:41 + pts/4 gertigr-root
SU 05/11 19:43 + pts/4 gertigr-root
SU 05/11 19:47 + console gertigr-root
SU 05/11 20:00 + pts/4 gertigr-root
SU 05/11 20:10 + console gertigr-root
SU 05/12 14:07 + pts/4 gertigr-root
SU 05/12 16:20 + pts/5 gertigr-root
SU 05/18 14:20 + pts/6 gertigr-root
SU 05/18 14:35 + pts/7 gertigr-root
SU 05/18 14:42 + pts/8 gertigr-root
```

/var/adm

NEbraskaCERT

```
# ls
acct        lastlog     messages.0  messages.3  sm.bin      sulog       wtmpx
aculog      log         messages.1  passwd      spellhist   utmpx
exacct      messages    messages.2  sa          streams     vold.log
# pwd
/var/adm
```

logins

NEbraskaCERT

Solaris Advanced System Administrator's Guide, Second Edition:Understanding System Security - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://snap.nlc.dcccd.edu/reference/sysadmin/julian/ch18/418-421.html Go Links

Previous Table of Contents Next

The following example shows the output of the `logins` command, which is used with no arguments:

```
castle% su
Password:
# logins
root               0     other              1     Super-User
smtp               0     root               0     Mail Daemon User
daemon             1     other              1
bin                2     bin                2
sys                3     sys                3
adm                4     adm                4     Admin
uucp               5     uucp               5     uucp Admin
nuucp              9     nuucp              9     uucp Admin
listen            37     adm                4     Network Admin
lp                71     lp                 8     Line Printer Admin
winsor          1001     staff             10
ray             1002     staff             10
des             1003     staff             10
rob             1004     staff             10
nobody         60001     nobody         60001     Nobody
noaccess       60002     noaccess       60002     No Access User
nobody4        65534     nogroup        65534     SunOS 4.x Nobody
#
```

The following example displays an extended set of login status information for user `winsor`.

```
# logins -x -l winsor
winsor           1001  staff         10
                 /export/home/winsor
                 /bin/csh
                 PS 000000 -1 -1 -1
#
```

The following example shows a list of user accounts with no password.

RBAC

NEbraskaCERT

- RBAC is a way of giving users enough privileges in order for them to do their job. Comes with Solaris
  - sudo is a third party software that does much the same
- Uses four /etc files
  - /etc/user_attr
  - /etc/security/exec_attr
  - /etc/security/auth_attr
  - /etc/security/prof_attr
- Roles are added using roleadd

RBAC (Cont'd)

NEbraskaCERT

- Uses four /etc files
  - /etc/user_attr
    - user:qualifier:res1:res2:attr
  - /etc/security/prof_attr
    - profname:res1:res2;desc:attr
  - /etc/security/exec_attr
    - name:policy:type:res1:res2:id:attr
  - /etc/security/auth_attr
    - name::::type:profile

Secure Shell

NEbraskaCERT

- Third party addition
- Available with Solaris 9 distribution
- Use instead of "r" commands
  - All traffic is encrypted so passwords can't be "sniffed"
  - No need of .rhosts

Basic Security Module (BSM)

NEbraskaCERT

- Loadable kernel module - comes with solaris 8
- Intercepts system calls based on audit policy
- C2 security rating
- turn on as root in single-user mode /etc/security/bsmconv or bsmunconv to turn off
- first it turns off volume management by moving the S92volmgt script to another directory
- Performs full auditing of kernel and device allocation
- Disables "Stop-a" capability

BSM (cont'd)

NEbraskaCERT

- /etc/security/audit_control
- /etc/security/audit_event
- /etc/security/audit_user
- /etc/security/audit_startup script
  - auditconfig –conf
  - auditconfig –setpolicy none
  - auditconfig – setpolicy +cnt
- The last one keeps count of audited events, but doesn't log them if the file system is full

Pluggable Authentication Modules (PAM)

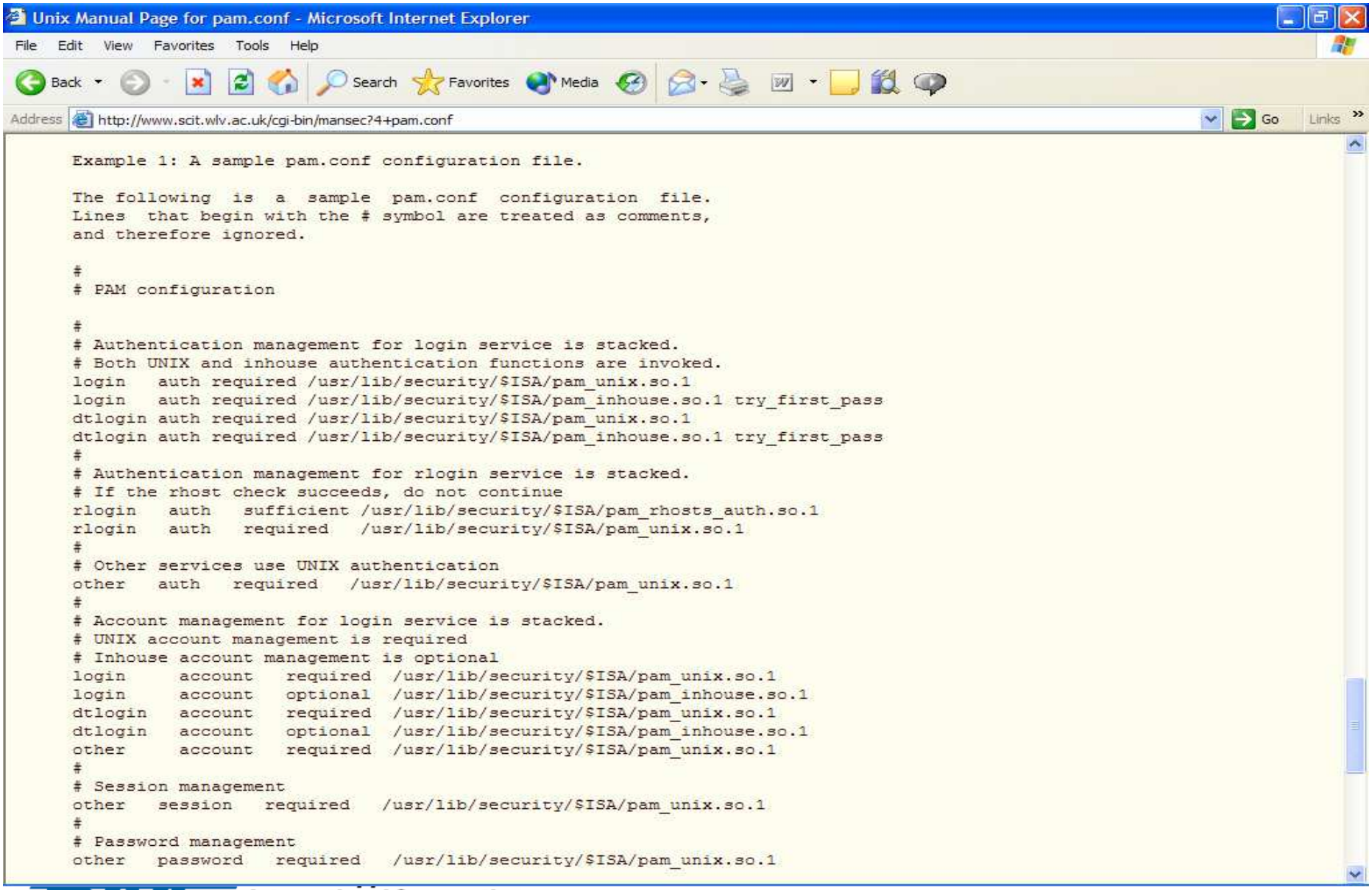
NEbraskaCERT

- Anytime you use telnet, you are using a PAM

- Add authentication technologies without adjusting login services. Can be used with:
  - RSA, DCE, Kerberos, S/Key, and smart card
  - policy driven in /etc/pam.conf (root readable)
  - unitary type login structure
    - If password is compromised, so are the multiple systems

/etc/pam.conf file

NEbraskaCERT




```
Example 1: A sample pam.conf configuration file.

The following is a sample pam.conf configuration file.
Lines that begin with the # symbol are treated as comments,
and therefore ignored.

#
# PAM configuration

#
# Authentication management for login service is stacked.
# Both UNIX and inhouse authentication functions are invoked.
login   auth required /usr/lib/security/$ISA/pam_unix.so.1
login   auth required /usr/lib/security/$ISA/pam_inhouse.so.1 try_first_pass
dtlogin auth required /usr/lib/security/$ISA/pam_unix.so.1
dtlogin auth required /usr/lib/security/$ISA/pam_inhouse.so.1 try_first_pass
#
# Authentication management for rlogin service is stacked.
# If the rhost check succeeds, do not continue
rlogin   auth   sufficient /usr/lib/security/$ISA/pam_rhosts_auth.so.1
rlogin   auth   required   /usr/lib/security/$ISA/pam_unix.so.1
#
# Other services use UNIX authentication
other   auth   required   /usr/lib/security/$ISA/pam_unix.so.1
#
# Account management for login service is stacked.
# UNIX account management is required
# Inhouse account management is optional
login     account   required  /usr/lib/security/$ISA/pam_unix.so.1
login     account   optional  /usr/lib/security/$ISA/pam_inhouse.so.1
dtlogin   account   required  /usr/lib/security/$ISA/pam_unix.so.1
dtlogin   account   optional  /usr/lib/security/$ISA/pam_inhouse.so.1
other     account   required  /usr/lib/security/$ISA/pam_unix.so.1
#
# Session management
other   session   required   /usr/lib/security/$ISA/pam_unix.so.1
#
# Password management
other   password   required   /usr/lib/security/$ISA/pam_unix.so.1
```

Security Tools

Some Tools

NEbraskaCERT

- Automated Security Enhancement Tool (ASET)
  - Checks setting in low/medium/high states
- find command
- System Administrator's Integrated Network Tool (SAINT)
  - http://www.wwdsi.com/saint/
  - http://www.cert.org/advisories
  - http://cve.mitre.org
    - Common vulnerabilities and exposure database
  - http://www.sans.org/topten.htm
  - http://ciac.llnl.gov/ciac/ToolsUnixNetMon.html#Courtney

Security Tools (cont'd)

NEbraskaCERT

- NMAP
- NESSUS
- Solaris Fingerprint Database
  - download and use MD5 to generate fingerprint to compare to one that lives on Sun's site
- Solaris Security Toolkit - JumpStart Architecture and Security Scripts (JASS)
- Tripwire

Bibliography

NEbraskaCERT

- Danielyan, Edgar, Solaris 8 Security, New York:New Riders Publishing, 2001.
- Gregory, Peter H., Solaris Security, Upper Saddle River:Prentice Hall PTR, 2000.
- Noordergraaf, Alex, et al., Enterprise Security: Solaris Operating Environment, Santa Clara: Sun Microsystems, Inc., 2002.
- Summers, Rita C., Secure Computing: Threats and Safeguards, New York:McGraw-Hill, 1997.

References (cont'd)

NEbraskaCERT

- <Building Open-SSH>
  http://www.sun.com/solutions/blueprints/404/817-6261.pdf
  <Making Login Services Independent of Authentication Technologies>
  http://java.sun.com/security/jaas/doc/pam.html#19776
- <General Security Site> http://www.securitydocs.com
- <Auditing in the Solaris 8 Operating Environment>
  http://downloads.securityfocus.com/library/audit_config.pdf
- <How Hackers Do It: Tricks, Tools, and Techniques>
  http://www.sun.com/solutions/blueprints/0502/816-4816-10.pdf
- <Configuring the Secure Shell Software>
  http://www.sun.com/blueprints/0403/817-2485.pdf
  <Public Key Infrastructure Overview>
  http://www.sun.com/blueprints/0801/publickey.pdf

References (cont'd)

NEbraskaCERT

- <Integrating the Secure Shell Software>
  http://www.sun.com/blueprints/0503/817-2821.pdf
- <Role Based Access Control and Secure Shell – A Closer Look at Two Solaris Operating Environment Security Features>
  http://www.sun.com/blueprints/0603/817-3062.pdf
- <IPSec in the Solaris 9 Operating Environment>
  http://wwws.sun.com/software/whitepapers/solaris9/ipsec.pdf
- <Trusted Solaris 8 Operating Environment>
  http://wwws.sun.com/software/whitepapers/wp-ts8/ts8-wp.pdf
- <Auditing in the Solaris 8 Operating Environment>
  http://www.sun.com/blueprints/0201/audit_config.pdf
- <Minimizing the Solaris Operating Environment for Security>
  http://www.sun.com/blueprints/1102/816-5241.pdf
- <Solaris Operating Environment Network Settings for Security>

(Link temporarily not available for Solaris 9)
http://www.sun.com/blueprints/1200/network-updt1.pdf

References (cont'd)

NEbraskaCERT

- <sun blueprints>

http://www.sun.com/blueprints/

- <sun blueprints scripts and tools>

http://www.sun.com/blueprints/tools

- <Patch Portal for Solaris>

http://sunsolve.sun.com/pub-cgi/show.pl?target=home

- <Deploying the Solaris OE Using a Solaris Security Toolkit CD>

http://www.sun.com/blueprints/0903/817-3592.pdf

- <Sun Product Documentation>

http://docs.sun.com

- <Securing Solaris Article>

http://www.netsys.com/cgi-bin/display_article.cgi?877

<Prentice Hall Technical Reference, Upgrade to Solaris 9>

http://www.phptr.com/articles/article.asp?p=101138&seqNum=1

Q & A

NEbraskaCERT

- You have questions
  I may have answers
  otherwise I'll research

Food for Thought

NEbraskaCERT

- Question
  - Why is Solaris like a tee-pee?
- Answer
  - No Gates
  - No Windows
  - Apache Inside