Interested in learning more about security?

SANS Institute

Security Consensus Operational Readiness Evaluation

This checklist is from the SCORE Checklist Project. Reposting is not permited without express, written permission.

HP-UX 10.20 Security for DSS Requirements Checklist

Copyright SANS Institute
Author Retains Full Rights

HP-UX 10.20 Security for DSS requirements.

Originally written by: Darren Bennett 11/05/03

Updated/Edited: Darren Bennett 11/14/03

Updated/Edited: Darren Bennett 08/13/04

I. Configure Login Banners:

There are two scenarios regarding Login Banners, the first assumes that you previously edited and saved the files to a DOS formatted floppy. The second scenario explains how to modify/create the files yourself.

A. If you **have** pre-saved the Banner files on a floppy:
** Be sure it is write protected and virus free**

Perform the following as root to mount the floppy and then copy the files to the locations specified in step 2:

1. To transfer a file from a PC floppy to the UNIX system:
doscp /dev/rfloppy/c0t1d0:<DOS-Filename> <UNIX-Filename and Path>
2. Copy Xresources to /etc/dt/config/C/Xresources and copy issue to /etc/issue
3. Skip ahead to part II.

Additional transfer notes:
To view the contents of a DOS floppy: type “dosls -a /dev/rfloppy/c0t1d0:”
To view the contents of a UNIX directory type “ls –al </path/to/the/directory>”
To view the contents of a UNIX file type “more </path/to/filename>”

B. If you **do not have** pre-saved copies of the Xresources and issue files:

Step 1:

Copy the example Xresources file from /usr/dt/config/C/Xresources to /etc/dt/config/C/Xresources and edit it to match the following (Changes made to the default file have been highlighted), or create a new file containing the following and save it to /etc/dt/config/C/Xresources:

-- Begin Copying for Xresources file **Below This Line --**

```
!!#############################################################################
!!
!!   Xresources
!!
!!   Common Desktop Environment
!!
!!   Configuration file for the Login Manager
!!
```

```
!!   (c) Copyright 1993, 1994 Hewlett-Packard Company
!!   (c) Copyright 1993, 1994 International Business Machines Corp.
!!   (c) Copyright 1993, 1994 Sun Microsystems, Inc.
!!   (c) Copyright 1993, 1994 Novell, Inc.
!!
!!       ************** DO NOT EDIT THIS FILE **************
!!
!!   /usr/dt/config/Xresources is a factory-default file and will
!!   be unconditionally overwritten upon subsequent installation.
!!   Before making changes to the file, copy it to the configuration
!!   directory, /etc/dt/config. You must also update the resources
!!   resource in /etc/dt/config/Xconfig.
!!
!!   $Revision: 1.1 $
!!
!!#########################################################################
!!
!!
!!  This file contains appearance and behaviour resources for the
Dtlogin
!!  login screen.  These are designed to be read into the root window
!!  property via the 'xrdb' program.  Dtlogin will do this automatically
!!  after the server is reset and will remove them before the session
!!  starts.
!!
!!  Dtlogin contains internal default values for all resources.  To
!!  override a default value, uncomment the appropriate line below and
!!  supply the desired value.
!!
!!  Customization hints are included at the end of this file.
!!
!!


!!#########################################################################
!!
!!  Motif visuals
!!

*XmCascadeButton*shadowThickness:       1
*XmDrawnButton*shadowThickness: 1
*XmPushButton*shadowThickness:  1
*XmPushButtonGadget*shadowThickness:    1
*XmText*shadowThickness:        1
*XmTextField*shadowThickness:   1
*enableButtonTab:       True
*enableDefaultButton:   True
*enableEtchedInMenu:    True
*enableMenuInCascade:   True
*enableMultiKeyBindings:        True
*enableToggleColor:     True
*enableToggleVisual:    True
*highlightThickness:    1

!!#########################################################################
!!
```

```
!!  COLORS
!!
!!      #a8a8a8 = lightgray
!!      #7e7e7e = gray (darker shade)
!!      #ef506f = burgundy
!!

!! Dtlogin*foreground:                          black

#ifdef COLOR
!! Dtlogin*background:                          #a8a8a8
!! Dtlogin*highlightColor:                      #ef506f
!! Dtlogin*logo*Background:                     #ef506f
#else
!! Dtlogin*background:                          white
#endif

!!#########################################################################
!!
!!  FONTS
!!
!!      labelFont               button and label text
!!      textFont                help and error dialog text
!!

#if WIDTH < 1024
Dtlogin*labelFont:     -dt-interface system-medium-r-normal-l*-*-*-*-*-
*-*-*-*:
Dtlogin*textFont:      -dt-interface user-medium-r-normal-l*-*-*-*-*-*-
*-*-*:
Dtlogin*greeting.fontList:  -dt-interface system-medium-r-normal-l*-*-
*-*-*-*-*-*-*:
#else
Dtlogin*labelFont:     -dt-interface system-medium-r-normal-l*-*-*-*-*-
*-*-*-*:
Dtlogin*textFont:      -dt-interface user-medium-r-normal-l*-*-*-*-*-*-
*-*-*:
Dtlogin*greeting.fontList: -dt-interface system-medium-r-normal-l*-*-*-
*-*-*-*-*-*:
#endif

!!#########################################################################
!!
!!  CURSOR
!!
!!      False = The MIT "X" cursor (default)
!!      True  = The left pointer cursor

Dtlogin*workspaceCursor:     True

!!#########################################################################
!!
!!  GREETING
!!
```

```
!! Dtlogin*greeting.foreground:        black
!! Dtlogin*greeting.background:        #a8a8a8
Dtlogin*greeting.labelString:       **DoD Warning Banner** \
\n Use of this or any other DoD interest computer system constitutes a
consent \
\n to monitoring at all times. This is a DoD interest computer system.
All DoD \
\n interest computer systems and related equipment are intended for the
\
\n communication, transmission, processing, and storage of official
U.S. \
\n Government or other authorized information only. All DoD interest
computer \
\n systems are subject to monitoring at all times to ensure proper
functioning \
\n of equipment and systems including security devices and systems, to
prevent \
\n unauthorized use and violations of statutes and security
regulations, to \
\n deter criminal activity, and for other similar purposes. Any user of
a DoD \
\n interest computer system should be aware that any information placed
in the \
\n system is subject to monitoring and is not subject to any
expectation of \
\n privacy. If monitoring of this or any other DoD interest computer
system \
\n reveals possible evidence of violation of criminal statutes, this
evidence \
\n and any other related information, including identification
information \
\n about the user, may be provided to law enforcement officials. If
monitoring \
\n of this or any other DoD interest computer systems reveals
violations of \
\n security regulations or unauthorized use, employees who violate
security \
\n regulations or make unauthorized use of DoD interest computer
systems are \
\n subject to appropriate disciplinary action. Use of this or any other
DoD \
\n interest computer system constitutes a consent to monitoring at all
times.

Dtlogin*greeting.persLabelString:   Hello %s
!! Dtlogin*greeting.alignment:         ALIGNMENT_CENTER

!!#####################################################################
!!
!!  Size of Text Input Area
!!

Dtlogin*login_text.columns:  20
Dtlogin*passwd_text.columns: 20
```

```
!!#############################################################################
!!
!!  MISC
!!

Dtlogin*logo*bitmapFile:           /etc/dt/config/C/logo.xpm

Dtlogin*preeditType:

!!#############################################################################
!!
!!  LANGUAGE MENU NAME MAPPINGS

#undef C
Dtlogin*C.languageName:                    C
Dtlogin*C.iso88591.languageName:           C.ISO8859-1
Dtlogin*POSIX.languageName:                POSIX
Dtlogin*arabic-w.languageName:             Algerian.Arabic8
Dtlogin*arabic.languageName:               Arabic.Arabic8
Dtlogin*arabic.iso88596.languageName:      Arabic.ISO8859-6
Dtlogin*bulgarian.languageName:            Bulgarian.ISO8859-5
Dtlogin*czech.languageName:                Czech.ISO8859-2
Dtlogin*danish.iso88591.languageName:      Danish.ISO8859-1
Dtlogin*danish.languageName:               Danish.Roman8
Dtlogin*german.iso88591.languageName:      German.ISO8859-1
Dtlogin*german.languageName:               German.Roman8
Dtlogin*greek.languageName:                Greek.Greek8
Dtlogin*greek.iso88597.languageName:       Greek.ISO8859-7
Dtlogin*english.iso88591.languageName:     English-UK.ISO8859-1
Dtlogin*english.languageName:              English-UK.Roman8
Dtlogin*american.iso88591.languageName:    English-US.ISO8859-1
Dtlogin*american.languageName:             English-US.Roman8
Dtlogin*spanish.iso88591.languageName:     Spanish.ISO8859-1
Dtlogin*spanish.languageName:              Spanish.Roman8
Dtlogin*finnish.iso88591.languageName:     Finnish.ISO8859-1
Dtlogin*finnish.languageName:              Finnish.Roman8
Dtlogin*c-french.iso88591.languageName:    French-Canadian.ISO8859-1
Dtlogin*c-french.languageName:             French-Canadian.Roman8
Dtlogin*french.iso88591.languageName:      French.ISO8859-1
Dtlogin*french.languageName:               French.Roman8
Dtlogin*serbocroatian.languageName:        Croatian.ISO8859-2
Dtlogin*hungarian.languageName:            Hungarian.ISO8859-2
Dtlogin*icelandic.iso88591.languageName:   Icelandic.ISO8859-1
Dtlogin*icelandic.languageName:            Icelandic.Roman8
Dtlogin*italian.iso88591.languageName:     Italian.ISO8859-1
Dtlogin*italian.languageName:              Italian.Roman8
Dtlogin*hebrew.languageName:               Hebrew.Hebrew8
Dtlogin*hebrew.iso88598.languageName:      Hebrew.ISO8859-8
Dtlogin*japanese.languageName:             Japanese.SJIS
Dtlogin*japanese.euc.languageName:         Japanese.EUC
Dtlogin*katakana.languageName:             Japanese.KANA8
Dtlogin*korean.languageName:               Korean.EUC
Dtlogin*dutch.iso88591.languageName:       Dutch.ISO8859-1
Dtlogin*dutch.languageName:                Dutch.Roman8
Dtlogin*norwegian.iso88591.languageName:   Norwegian.ISO8859-1
```

```
Dtlogin*norwegian.languageName:           Norwegian.Roman8
Dtlogin*polish.languageName:              Polish.ISO8859-2
Dtlogin*portuguese.iso88591.languageName: Portuguese.ISO8859-1
Dtlogin*portuguese.languageName:          Portuguese.Roman8
Dtlogin*rumanian.languageName:            Rumanian.ISO8859-2
Dtlogin*russian.languageName:             Russian.ISO8859-5
Dtlogin*slovak.languageName:              Slovak.ISO8859-2
Dtlogin*slovene.languageName:             Slovene.ISO8859-2
Dtlogin*swedish.iso88591.languageName:    Swedish.ISO8859-1
Dtlogin*swedish.languageName:             Swedish.Roman8
Dtlogin*thai.languageName:                Thai.TIS620
Dtlogin*turkish.iso88599.languageName:    Turkish.ISO8859-9
Dtlogin*turkish.languageName:             Turkish.Turkish8
Dtlogin*chinese-s.languageName:           Chinese-s.HP15
Dtlogin*chinese-t.big5.languageName:      Chinese-t.BIG5
Dtlogin*chinese-t.languageName:           Chinese-t.CCDC

!!#########################################################################
!!
!!  CHOOSER
!!
dtchooser*chlistFont:         -dt-interface user-medium-r-normal-s*-*-*-
*-*-*-*-*-*:
dtchooser*visibleItemCount:   10

!!*************************************************************************
*******
!!
!!                       CUSTOMIZATION HINTS
!!
!!
!!  The login screen was designed to be easy to customize for a variety
of
!!  attributes. These include...
!!
!!      1. custom logo bitmap
!!      2. custom greeting message
!!      3. colors
!!      4. fonts
!!
!!  Users may replace the default logo with a custom one of their
choice.
!!
!!  Colors and fonts can be changed using the standard Motif resources
for
!!  the appropriate widget and/or class.

**-- End Copying for Xresources File Above This Line --**
```

Step 2:

Create a file /etc/issue and place the following in it:

-- Begin Copying for issue File Below This Line --

DoD Warning Banner
Use of this or any other DoD interest computer system constitutes consent to monitoring at all times. This is a DoD interest computer system. All DoD interest computer systems and related equipment are intended for the communication, transmission, processing, and storage of official U.S. Government or other authorized information only. All DoD interest computer systems are subject to monitoring at all times to ensure proper functioning of equipment and systems including security devices and systems, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for other similar purposes. Any user of a DoD interest computer system should be aware that any information placed in the system is subject to monitoring and is not subject to any expectation of privacy. If monitoring of this or any other DoD interest computer system reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of this or any other DoD interest computer systems reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of DoD interest computer systems are subject to appropriate disciplinary action. Use of this or any other DoD interest computer system constitutes a consent to monitoring at all times.

-- End Copying for issue File Above This Line --

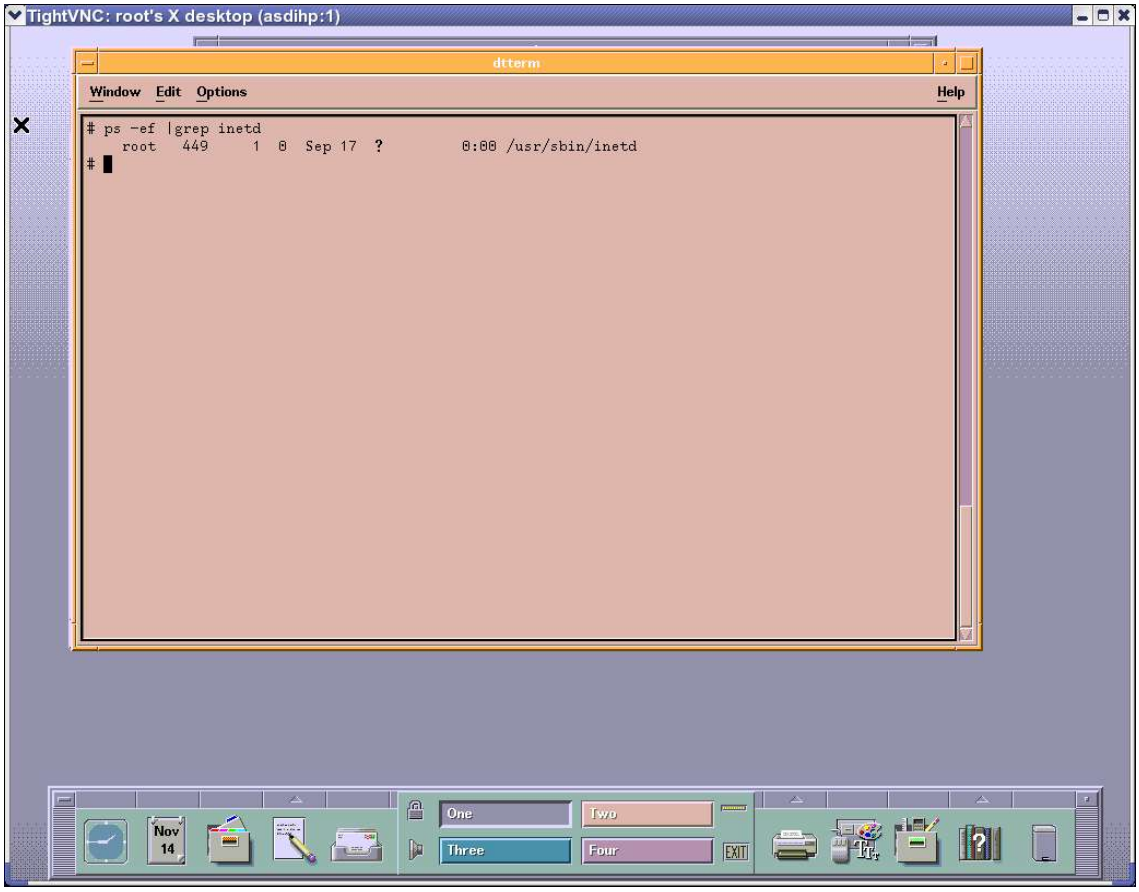
Step 3:

Enable banners for telnet access to the system:

a. Edit /etc/inetd.conf
b. Append "-b /etc/issue" to the "telnet" entry.
(the line should end with "telnetd -b /etc/issue")

c. From the command line, determine the Process ID (PID) for inetd:

Type "ps -ef |grep inetd”. (The PID is the first number from the right. In the example below, it is 449)



d. Restart inetd to load your changes:

Type “kill -HUP <PID of inetd>"

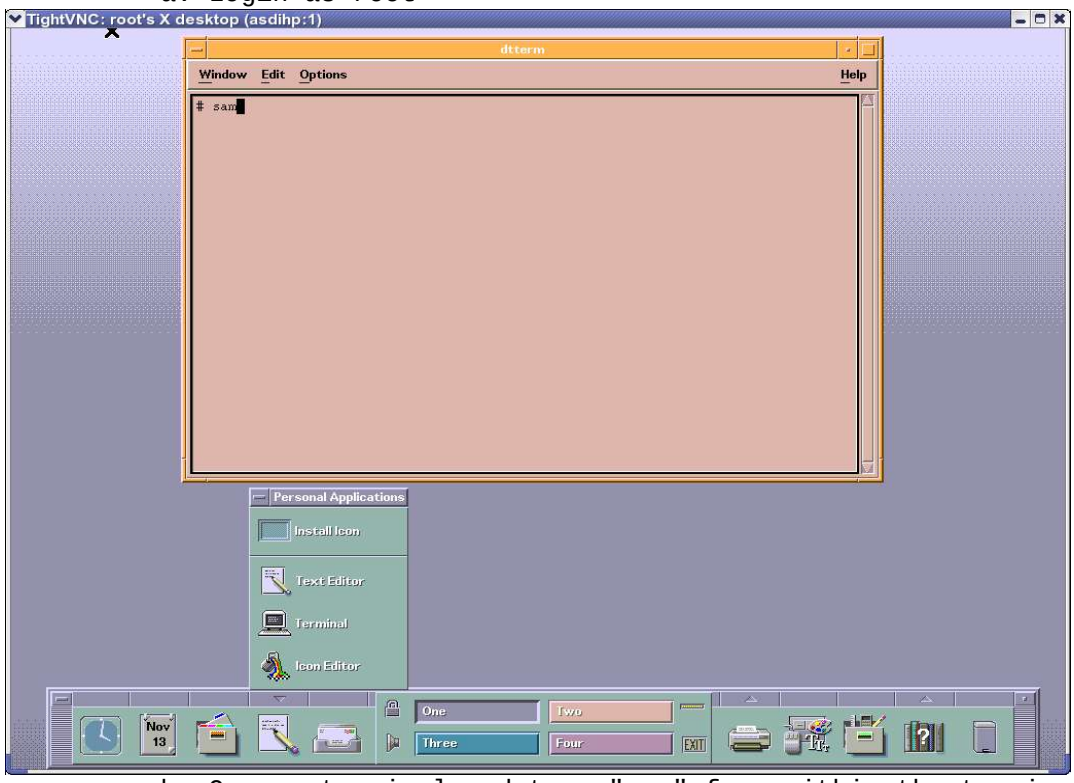
II. Disable access to the system PROM

a. Reboot the system via the "reboot" command (you must be root to do this)
b. During the boot process, you will be prompted with "to discontinue, press any key within 10 seconds" (press a key)
c. Type "CO" (for the Configuration Menu)
d. Type "SEC ON" (to enable secure boot mode)
e. Type "BIN"
- Verify that both Primary and Secondary boot devices have the same SCSI ID.
- Check that the Secure flag is set to ON and auto search is OFF
f. Type “RESET” to reboot the system with your changes enabled.

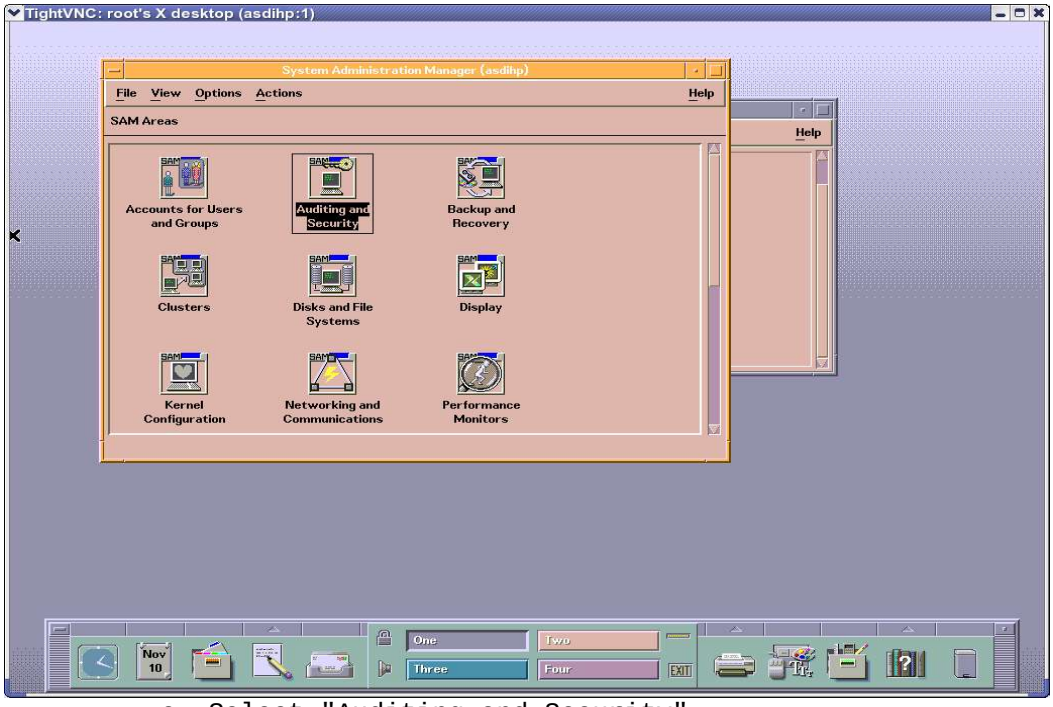
To re-enable PROM access at a later time, shutdown the system and remove the hard disks. Re-boot the system and disable the “SEC OFF” command using the same steps as above, shut down the system again, replace the drives and restart the system

III. Configure Auditing

a. Login as root



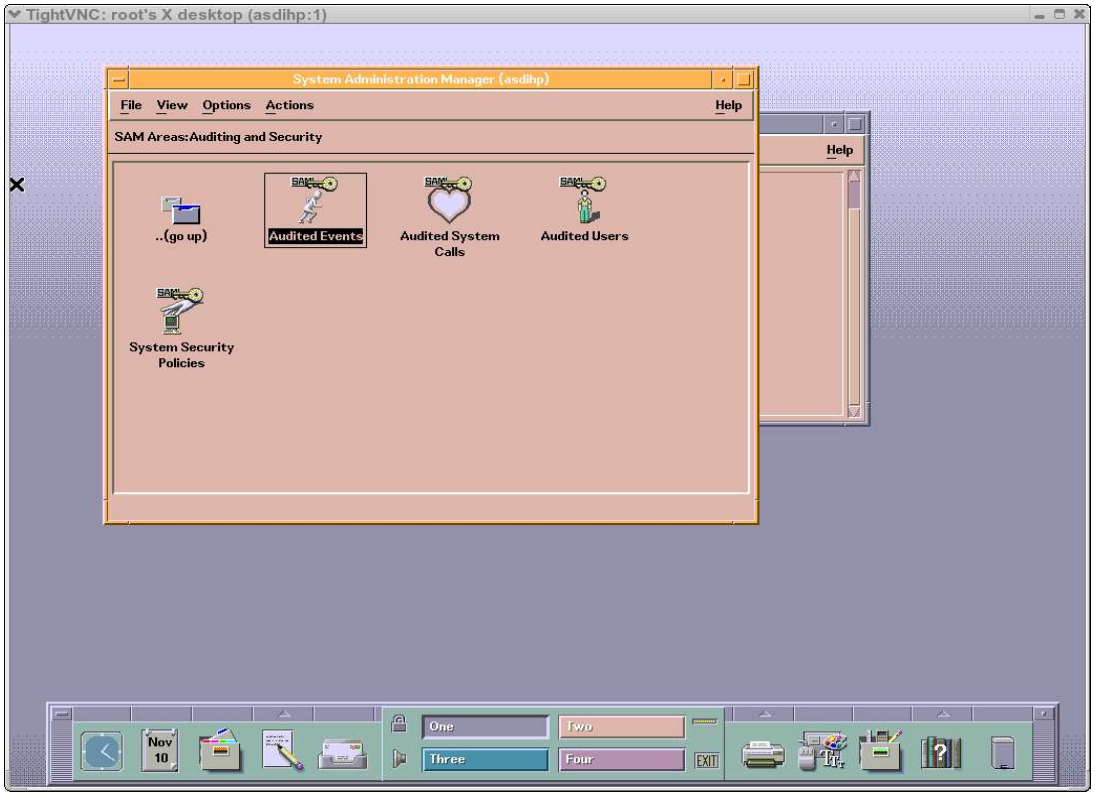
b. Open a terminal and type "sam" from within the terminal



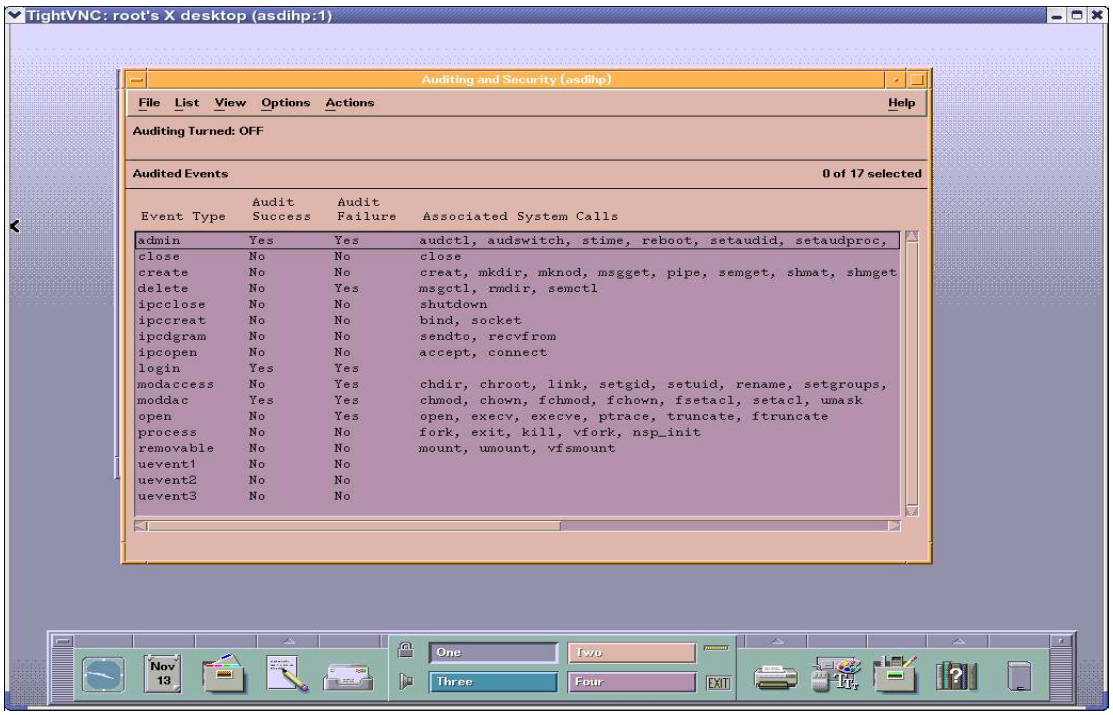
c. Select "Auditing and Security"

d. Select "Audited Events"

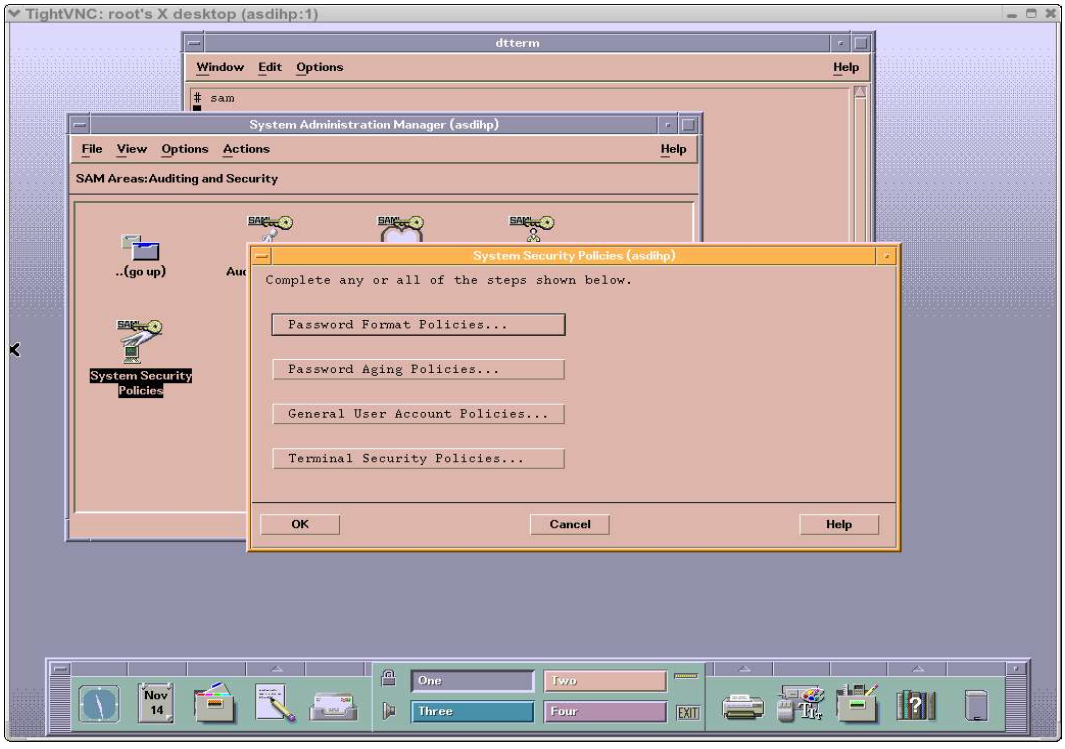
If this is the first time you have done this or the “audnames” file does not exist, you will first be prompted if one should be created (select yes)



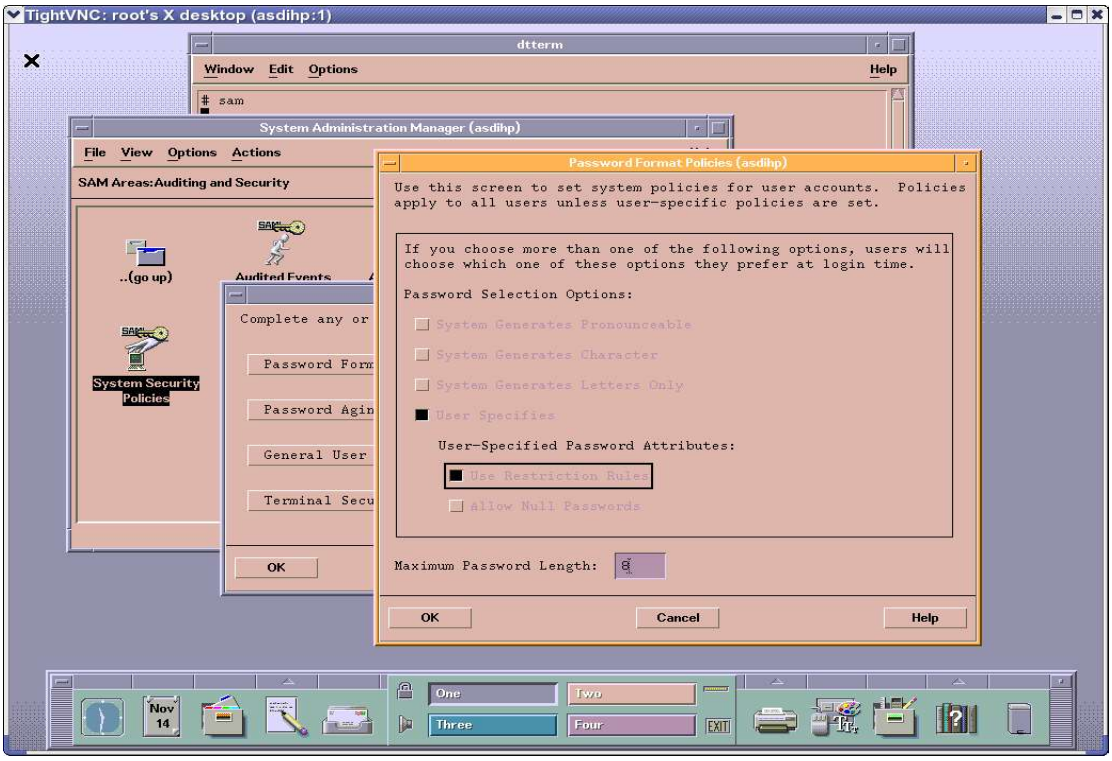
e. Make sure the following items are selected for auditing: (“Right Click” on the item to change its status)

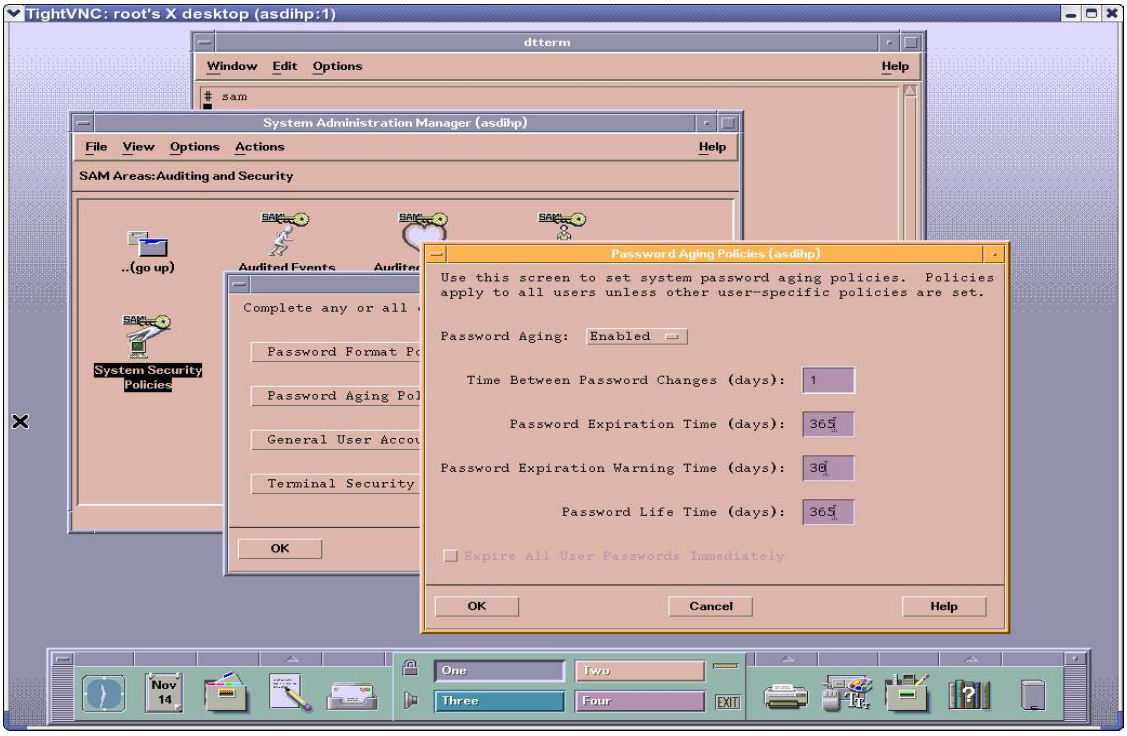


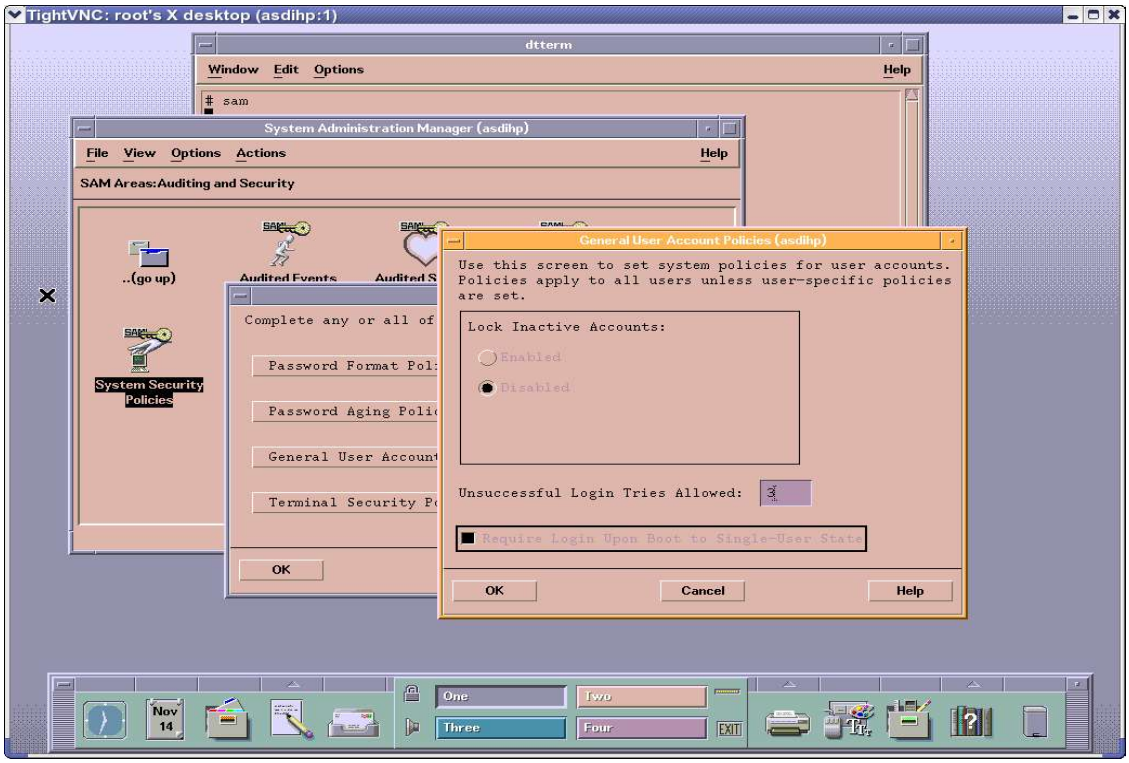
f. Select “System Security Policies” (Double Click)

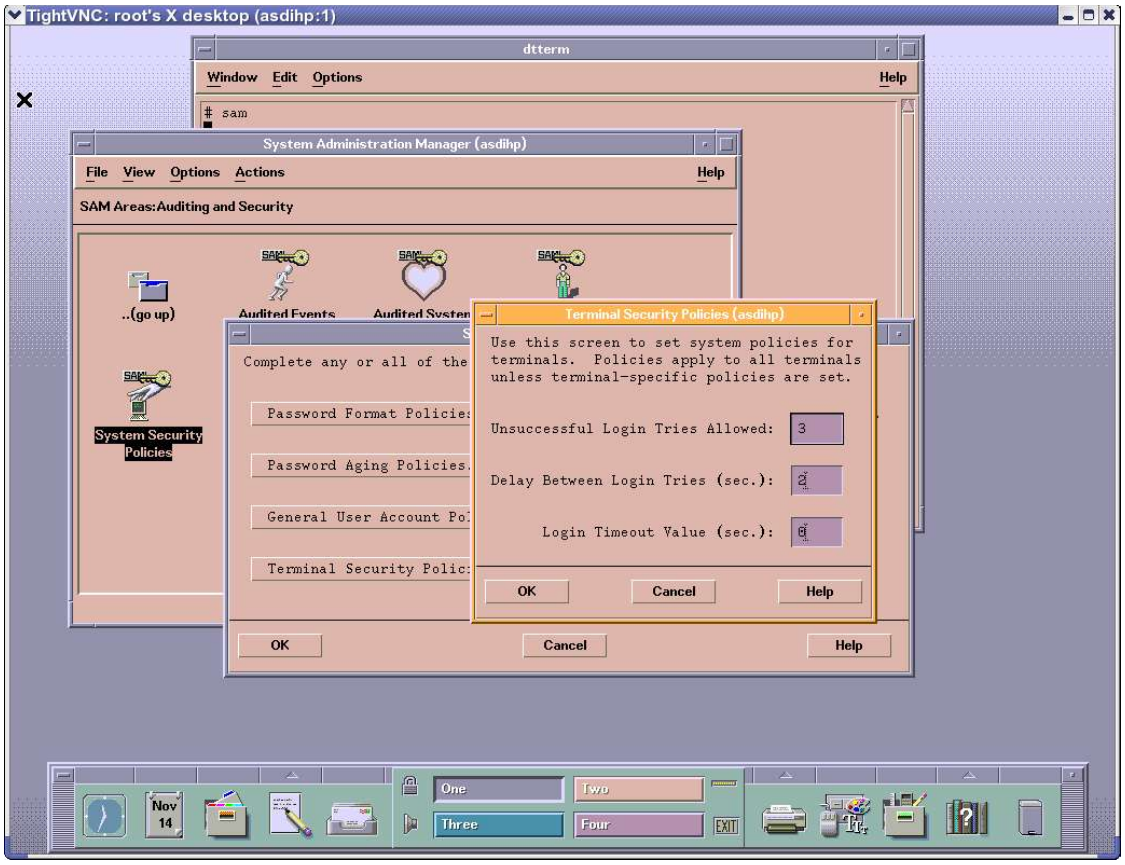


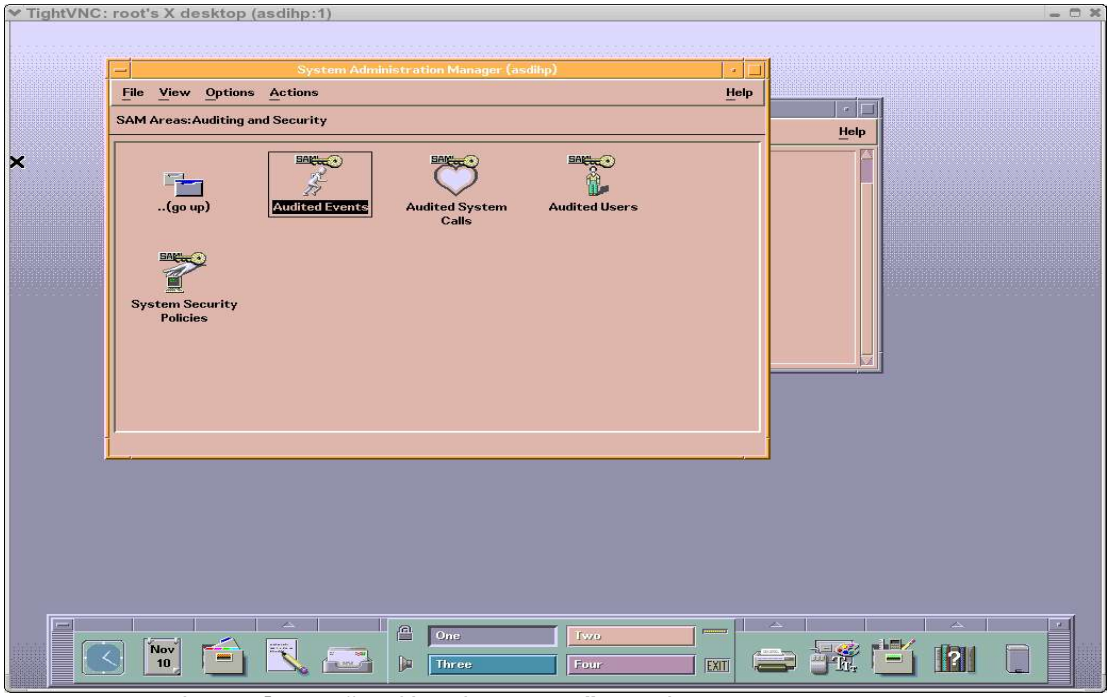
g. Select “Password Format Policies”, “Password Aging Policies”, “General User Account Policies”, and “Terminal Security Policies” and be sure they match the settings in the four images below:


TightVNC: root's X desktop (asdihp:1)
dtterm
Window Edit Options Help
sam
System Administration Manager (asdihp)
File View Options Actions
SAM Areas:Auditing and Security
..(go up)
Audited Events
System Security Policies
Complete any or
Password Form
Password Agin
General User
Terminal Secu
OK
Password Format Policies (asdihp)
Use this screen to set system policies for user accounts. Policies apply to all users unless user-specific policies are set.
If you choose more than one of the following options, users will choose which one of these options they prefer at login time.
Password Selection Options:
System Generates Pronounceable
System Generates Character
System Generates Letters Only
User Specifies
User-Specified Password Attributes:
Use Restriction Rules
Allow Null Passwords
Maximum Password Length: 8
OK
Cancel
Help
One
Two
Three
Four
EXIT
Nov 14


TightVNC: root's X desktop (asdihp:1)
dtterm
Window Edit Options Help
sam
System Administration Manager (asdihp)
File View Options Actions Help
SAM Areas:Auditing and Security
..(go up)
Audited Events
System Security Policies
Complete any or all
Password Format Po
Password Aging Pol
General User Accou
Terminal Security
OK
Password Aging Policies (asdihp)
Use this screen to set system password aging policies. Policies apply to all users unless other user-specific policies are set.
Password Aging: Enabled
Time Between Password Changes (days): 1
Password Expiration Time (days): 365
Password Expiration Warning Time (days): 30
Password Life Time (days): 365
Expire All User Passwords Immediately
OK
Cancel
Help
One
Two
Three
Four
EXIT
Nov 14

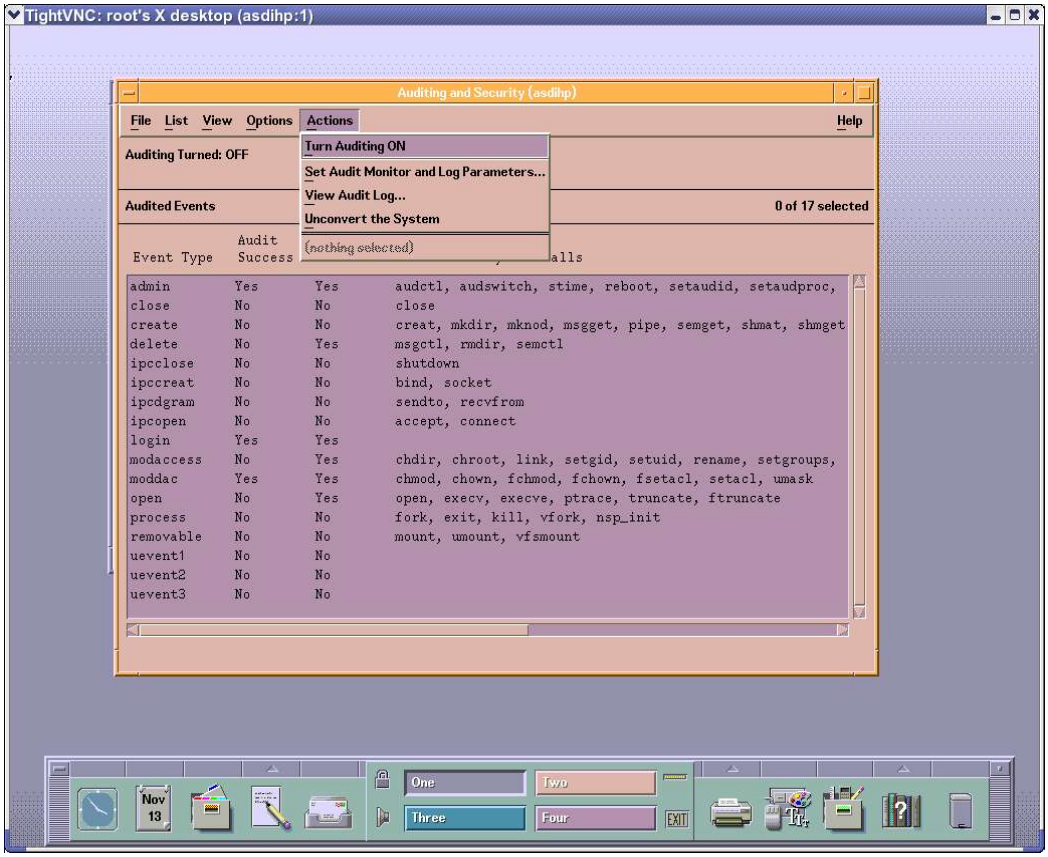

TightVNC: root's X desktop (asdihp:1)
dtterm
Window Edit Options Help
sam
System Administration Manager (asdihp)
File View Options Actions Help
SAM Areas:Auditing and Security
..(go up)
Audited Events
System Security Policies
Complete any or all of
Password Format Poli
Password Aging Polic
General User Account
Terminal Security Po
OK
General User Account Policies (asdihp)
Use this screen to set system policies for user accounts. Policies apply to all users unless user-specific policies are set.
Lock Inactive Accounts:
Enabled
Disabled
Unsuccessful Login Tries Allowed:
3
Require Login Upon Boot to Single-User State
OK
Cancel
Help
Nov 14
One
Two
Three
Four
EXIT





h. Select “Audited Events” Again

i. "Actions, Turn Auditing ON"



IV. Congratulations! You have finished.

Last Updated: April 17th, 2024

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Oslo April 2024	Oslo, NO	Apr 22, 2024 - Apr 27, 2024	Live Event
SANS Baltimore Spring 2024	Baltimore, MDUS	Apr 28, 2024 - May 03, 2024	Live Event
SANS Autumn Australia 2024	Sydney, NSW, AU	May 06, 2024 - May 11, 2024	Live Event
SANS Rome May 2024	Rome, IT	May 06, 2024 - May 11, 2024	Live Event
SANS Security West 2024	San Diego, CAUS	May 09, 2024 - May 14, 2024	Live Event
SANS Dubai May 2024	Dubai, AE	May 11, 2024 - May 16, 2024	Live Event
SANS ICS Europe 2024 Munich	Munich, DE	May 12, 2024 - May 18, 2024	Live Event
SANS Cloud Singapore 2024	Singapore, SG	May 13, 2024 - May 24, 2024	Live Event
SANS Doha May 2024	Doha, QA	May 18, 2024 - May 23, 2024	Live Event
SANS Amsterdam May 2024	Amsterdam, NL	May 20, 2024 - Jun 01, 2024	Live Event
SANS Leadership & Cloud Security - Crystal City 2024	Arlington, VAUS	May 20, 2024 - May 24, 2024	Live Event
SANS Philippines SEC504 2024	Manila, PH	May 27, 2024 - Jun 01, 2024	Live Event
SANS Cyber Defence Thailand 2024	Bangkok, TH	May 27, 2024 - Jun 01, 2024	Live Event
SANS SEC530 Canberra 2024	Canberra, ACT, AU	May 27, 2024 - Jun 01, 2024	Live Event
SANS Summer Dunes 2024	Riyadh, SA	Jun 01, 2024 - Jun 06, 2024	Live Event
SANS Muscat June 2024	Muscat, OM	Jun 01, 2024 - Jun 06, 2024	Live Event
SANS Munich June 2024	Munich, DE	Jun 03, 2024 - Jun 08, 2024	Live Event
SANS Miami 2024	Coral Gables, FLUS	Jun 03, 2024 - Jun 15, 2024	Live Event
SANS Paris June 2024	Paris, FR	Jun 10, 2024 - Jun 15, 2024	Live Event
SANS Madrid June 2024	Madrid, ES	Jun 10, 2024 - Jun 15, 2024	Live Event
SANS ICS Security Summit & Training 2024	Orlando, FLUS	Jun 16, 2024 - Jun 24, 2024	Live Event
SANS Tbilisi June 2024	Tbilisi, GE	Jun 17, 2024 - Jun 22, 2024	Live Event
SANS Rocky Mountain Summer 2024	Denver, COUS	Jun 17, 2024 - Jun 22, 2024	Live Event
SANS Warsaw June 2024	Warsaw, PL	Jun 17, 2024 - Jun 22, 2024	Live Event
SANS Cyber Defence Japan 2024	Tokyo, JP	Jun 17, 2024 - Jun 29, 2024	Live Event
SANS Cyber Defence Australia 2024	Canberra, ACT, AU	Jun 24, 2024 - Jul 06, 2024	Live Event
SANS Zurich June 2024	Zurich, CH	Jun 24, 2024 - Jun 29, 2024	Live Event
SANS San Antonio 2024	San Antonio, TXUS	Jun 24, 2024 - Jun 29, 2024	Live Event
SANS London July 2024	London, GB	Jul 01, 2024 - Jul 06, 2024	Live Event
SANSFIRE 2024	Washington, DCUS	Jul 15, 2024 - Jul 20, 2024	Live Event
SANS Amsterdam July 2024	Amsterdam, NL	Jul 15, 2024 - Jul 20, 2024	Live Event
SANS Pen Test Austin 2024	OnlineTXUS	Apr 22, 2024 - Apr 27, 2024	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced