CIS Benchmarks

CIS Oracle Solaris 11.4 Benchmark

v1.0.0 - 01-02-2020

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Overview

This document, CIS Oracle Solaris 11.4 Benchmark, provides prescriptive guidance for establishing a secure configuration posture for Oracle Solaris 11 on both x86 and SPARC platforms. This guide was tested against Oracle Solaris 11.4 SRU 12 (11.4.12.5.0/20-Aug-2019). As of the publication of this document, Solaris 11.4.12.5.0 is the latest available support update for the Solaris 11 OS. The recommendations included in this document may need to be adjusted for other Solaris 11 updates. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Oracle Solaris 11.4

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

The CIS community also extends thanks to those that contributed to previous versions of this Benchmark:
Adam Montville, Andrew Gilmore, Blake Frantz, Carole Fennelly, Chris Cook, Christopher Calabrese, Damian Southard, Dave Shackleford, David A. Kennel, David Pollard, Douglas J Schmidt, Filip Francis, Glenn Brunette, Hal Pomeranz, Hoang Truong Dinh, Ian J Hunt, Jason Mackanick, Jay Beale, Joe Wulf, Joel Kirch, John Banghart, John Jenkinson, John Traenkenschuh, Jonathan Klein, Keith Buck, Larry Cole, Mark Phillips, Mike Bamford, Nancy Whitney, Nelson Benitez, Ralph Durkee, Randy Young, Timothy Wood, Tom Maloy, Tom Rhodes, Vladimir Bogodist, Wilfred Artman, and Zack Yang

Contributor
David Pollard , NASA - National Aeronautics and Space Administration
Rael Daruszka , Center for Internet Security
Robert Thomas
Mark Hesse

Editor
Eric Pinnell

Recommendations

1 Software Installation and Updates

The Solaris 11 OS should be periodically updated to enable the support of new hardware platforms as well as enhance the security, reliability, and performance of the system.

1.1 Use the Latest Package Updates (Not Scored)

Profile Applicability:

- Level 1

Description:

The Solaris 11 OS should be periodically updated to install or upgrade software packages that will enhance the security, reliability, and performance of the system.

Rationale:

For the Solaris 11 OS, there will be no more software patches issued, but rather security and other improvements will be installed by updating one or more software packages.

Audit:

To verify that the system is operating with the latest software updates, perform the following and verify that the result is as shown:

```
# pkg update -n

No updates available for this image.
```

In addition, you can manually verify the update associated with the running system using the following command. The output of this command will indicate the operation system version and update number as well as the Software Repository Update (SRU) number.

```
pkg info entire
             Name: entire
          Summary: entire incorporation including Support Repository Update
                  (Oracle Solaris 11.4.12.5.0).
      Description: This package constrains system package versions to the
same build.
                   WARNING: Proper system update and correct package
selection depend
                   on the presence of this incorporation.  Removing this
package will
                   result in an unsupported system.  For more information
see:
                   https://support.oracle.com/rs?type=doc&id=2433412.1
         Category: Meta Packages/Incorporations
            State: Installed
        Publisher: solaris
          Version: 11.4 (Oracle Solaris 11.4.12.5.0)
           Branch: 11.4.12.0.1.5.0
   Packaging Date: August  9, 2019 at 10:06:39 PM
Last Install Time: August 29, 2019 at  8:47:28 PM
             Size: 2.52 kB
             FMRI: pkg://solaris/entire@11.4-11.4.12.0.1.5.0:20190809T220639Z

For more information, see the Oracle white paper titled "Packaging and
Delivering Software with the Image Packaging System in Oracle Solaris 11.4"
available from: https://docs.oracle.com/cd/E37838_01/html/E61051/index.html.
```

Remediation:

Run the following command to refresh the package catalog, download and apply any available updates:

```
# pkg update
```

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

2 Disable Unnecessary Services

While using the most up to date software packages will help to correct any known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to disable services that are not required for that particular system's intended operation or management. This helps to prevent the exploitation of vulnerabilities that may be discovered at a later date. The actions in this section of the document provide guidance on what services can be safely disabled and under which circumstances.

The Solaris 11 OS has implemented a "Secure by Default" (SBD) posture whereby many services that were once automatically enabled are now either disabled or configured to listen only for connections originating from the system itself. This default software configuration greatly simplifies many of the security hardening steps typically undertaken in previous versions of the operating system. As a result, this section will build upon this default configuration and focus specifically on those services that are enabled (local-only or otherwise) that organizations may want to disable.

As noted above, several services are not disabled, but rather are placed into a "local only" mode where they will accept connections originating only from the local system itself. This was done to strike a balance between security and out-of-the-box usability. If these services are not required, it is recommended that they be disabled to guard against potential future vulnerabilities that can be exploited by users and/or services that are operating locally on the system.

2.1 Configure TCP Wrappers (Not Scored)

Profile Applicability:

- Level 1

Description:

TCP Wrappers is a host-based access control system that allows administrators to control who has access to various network services based on the IP address of the remote end of the connection. TCP Wrappers also provide logging information via `syslog` about both successful and unsuccessful connections.

Rationale:

TCP Wrappers provides granular control over what services can be accessed over the network. Its logs show attempted access to services from non-authorized systems, which can help identify unauthorized access attempts.

Audit:

Perform the following and verify that the result is as shown:

```
# inetadm -p | grep tcp wrappers

tcp_wrappers=TRUE

# ls /etc/hosts.deny

/etc/hosts.deny

# ls /etc/hosts.allow

/etc/hosts.allow
```

The above command will check whether TCP Wrappers is enabled for all TCP-based services started by inetd. Individual inetd services may still be configured to use TCP Wrappers even if the global parameter (above) is set to FALSE. To check the status of individual inetd services, use the command:

```
# for svc in `inetadm | awk '/svc:\// { print $NF }'`; do
     val=`inetadm -l ${svc} | grep -c tcp_wrappers=TRUE`
     if [ ${val} -eq 1 ]; then
        echo "TCP Wrappers enabled for ${svc}"
     fi
done
```

Lastly, TCP Wrappers can be enabled for the RPC port mapping service. To determine if this is the case, use the command:

```
# svcprop -p config/enable_tcpwrappers rpc/bind

false
```

Remediation:

To enable TCP Wrappers, run the following commands:

1. Create and customize your policy in `/etc/hosts.allow`:

```
# echo "ALL: <net>/<mask>, <net/<mask>, …" > /etc/hosts.allow
```

where each / combination (for example, the Class C address block "`192.168.1.0/255.255.255.0`") can represent one network block in use by your organization that requires access to this system.

2. Create a default deny policy in `/etc/hosts.deny`:

```
# echo "ALL: ALL" >/etc/hosts.deny
```

3. Enable TCP Wrappers for all services started by `inetd`:

```
# inetadm -M tcp_wrappers=TRUE
```

To protect only specific `inetd`services, use the command:

```
# inetadm -m [FMRI] tcp_wrappers=TRUE
```

where [FMRI] is the service to protect.
To enable TCP Wrappers for the RPC port mapping service, use the commands:

```
# svccfg -s rpc/bind setprop config/enable_tcpwrappers=true

# svcadm refresh rpc/bind
```

To protect UDP and RPC-based services that are spawned from `inetd`, consider implementing a host-based firewall. Oracle Solaris PF firewall (a.k.a. PF) has replaced Solaris IP Filter (IPF) in Solaris 11.4. See `firewall(5)` for more information.

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

2.2 Disable Local-only Graphical Login Environment (Scored)

Profile Applicability:

- Level 1

Description:

The graphical login service provides the capability of logging into the system using an X-windows type interface from the console. If graphical login access for the console is required, leave the service in local-only mode.

Rationale:

This service should be disabled if it is not required.

Audit:

Perform the following and verify that the result is as shown:

```
# svcs -Ho state svc:/application/graphical-login/gdm:default

disabled
```

If the service is not installed, this will return an error, or no output. This is also considered a passing state.

Remediation:

To disable this service, run the following command:

```
# svcadm disable svc:/application/graphical-login/gdm:default
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.3 Configure sendmail Service for Local-Only Mode (Scored)

Profile Applicability:

- Level 1

Description:

In Solaris 11, the `sendmail` service is set to local only mode by default. This means that users on remote systems cannot connect to the `sendmail` service, eliminating the possibility of a remote exploit attack against some future `sendmail` vulnerability. Leaving `sendmail` in local-only mode permits mail to be sent out from the local system. If the local system will not be processing or sending any mail, this service can be disabled.

However, if `sendmail` is disabled completely, email messages sent to the `root` account (such as `cron` job output or audit service warnings) will fail to be delivered.

An alternative approach is to disable the `sendmail` service and create a `cron` job to process all mail that is queued on the local system, sending it to a relay host defined in the `sendmail.cf` file. It is recommended that `sendmail` be left in local-only mode unless there is a specific requirement to completely disable it.

Rationale:

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

Audit:

Perform the following command and make sure that the MTA is listening on the loopback address (127.0.0.1):

```
# netstat -an | grep LIST | grep ".25 "

127.0.0.1.25 *.* 0 0 256000 0 LISTEN
::1.25        *.*  0  0  128000  0  LISTEN

# netstat -an | grep LIST | grep ".587 "

127.0.0.1.587 *.* 0 0 256000 0 LISTEN
```

Remediation:

Run the following to set sendmail to listen only local interfaces:

```
# svccfg -v -s svc:/network/smtp:sendmail setprop config/local only=true

# svcadm refresh sendmail

# svcadm restart sendmail
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.4 Disable RPC Encryption Key (Scored)

Profile Applicability:

- Level 1

Description:

The `keyserv` service is only required for sites that are using the Secure RPC mechanism. The most common use for Secure RPC on Solaris machines is "secure NFS", which uses the Secure RPC mechanism to provide higher levels of security than the standard NFS protocols. ("Secure NFS" is unrelated to Kerberos authentication as a mechanism for providing higher levels of NFS security. "Kerberized" NFS does not require the `keyserv` service to be running.)

Rationale:

This service should be disabled if it is not required.

Audit:

Perform the following and verify that the result is as shown:

```
# svcs -Ho state svc:/network/rpc/keyserv

disabled
```

If the service is not installed, this will return an error, or no output. This is also considered a passing state.

Remediation:

To disable this service, run the following command:

```
# svcadm disable svc:/network/rpc/keyserv
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.5 Disable Generic Security Services (GSS) (Scored)

Profile Applicability:

- Level 1

Description:

The GSS API is a security abstraction layer that is designed to make it easier for developers to integrate with different authentication schemes. It is most commonly used in applications for sites that use Kerberos for network authentication, though it can also allow applications to interoperate with other authentication schemes.

Rationale:

GSS does not expose anything external to the system as it is configured to use TLI (protocol = `ticotsord`) by default. This service should be disabled if it is not required.

Audit:

Perform the following and verify that the result is as shown:

```
# svcs -Ho state svc:/network/rpc/gss

disabled | uninitialized
```

If the service is not installed, this will return an error, or no output. This is also considered a passing state. If inetd is disabled, the status will return as “uninitialized”.

Remediation:

To disable this service, run the following command:

```
# svcadm disable svc:/network/rpc/gss
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.6 Disable Apache Service (Scored)

Profile Applicability:

- Level 1

Description:

The Apache service provides an instance of the Apache web server.

Rationale:

This service should be disabled if it is not required.

Audit:

Perform the following and verify that the result is as shown:

```
# svcs -Ho state svc:/network/http:apache24

disabled
```

If the service is not installed, this will return an error, or no output. This is also considered a passing state.

Remediation:

To disable this service, run the following command:

```
# svcadm disable svc:/network/http:apache24
```

References:

1. Apache Benchmark and scoring tool from CIS, https://www.cisecurity.org/benchmark/apache_http_server/
2. Apache Foundation's "Security Tips" document http://httpd.apache.org/docs-2.0/misc/security_tips.html

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.7 Disable Kerberos TGT Expiration Warning (Scored)

Profile Applicability:

- Level 1

Description:

The Kerberos TGT warning service is used to warn users when their Kerberos tickets are about expire or to renew those tickets before they expire. This service is not used if Kerberos has not been configured. This service is configured to be "local only" by default.

Rationale:

This service should be disabled if it is not required.

Audit:

Perform the following and verify that the result is as shown:

```
# svcs -Ho state svc:/network/security/ktkt_warn

disabled | uninitialized
```

If the service is not installed, this will return an error, or no output. This is also considered a passing state. If inetd is disabled, the status will return as “uninitialized”.

Remediation:

To disable this service, run the following command:

```
# svcadm disable svc:/network/security/ktkt_warn
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.8 Disable NIS Client Services (Scored)

Profile Applicability:

- Level 1

Description:

If the local site is not using the NIS naming service to distribute system and user configuration information, this service may be disabled. This service is disabled by default unless the NIS service has been installed and configured on the system.

Rationale:

As RPC-based services such as NIS may use non-secure authentication and share sensitive network object information with systems and applications using RPC-based service, NIS client daemons should be disabled. Users are encouraged to use LDAP as a name service in place of NIS.

Audit:

Perform the following and verify that the result is as shown:

```
# svcs -Ho state svc:/network/nis/client

disabled
```

If LDAP is not in use check that nis/domain is also disabled:

```
# svcs -Ho state svc:/network/nis/domain

disabled
```

If the service is not installed, this will return an error, or no output. This is also considered a passing state.

Remediation:

To disable this service, run the following commands:

```
# svcadm disable svc:/network/nis/client
```

Check to see if LDAP Client is in use:

```
# svcs -a | grep ldap | awk -F" " '{if ($1 ~ /disabled/ && $3 ~ /client/)
print "LDAP Client is disabled - svc:/network/nfs/domain can be disabled.";}'
```

If LDAP is not in use also disable nis/domain:

```
# svcadm disable svc:/network/nis/domain
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.9 Disable NIS Server Services (Scored)

Profile Applicability:

- Level 1

Description:

The NIS server software is not installed by default and is only required on systems that are acting as an NIS server for the local site. Typically there are only a small number of NIS servers on any given network. These services are disabled by default unless the system has been previously configured to act as a NIS server.

Rationale:

As RPC-based services such as NIS may use non-secure authentication and share sensitive network object information with systems and applications using RPC-based services, this service should be disabled. Users are encouraged to use LDAP as a name service in place of NIS.

Audit:

Perform the following and verify that the result is as shown:

```
# svcs -Ho state svc:/network/nis/server

disabled
```

If LDAP is not in use check that nis/domain is also disabled:

```
# svcs -Ho state svc:/network/nis/domain

disabled
```

If the service is not installed, this will return an error, or no output. This is also considered a passing state.

Remediation:

To disable this service, run the following commands:

```
# svcadm disable svc:/network/nis/server
```

Check to see if LDAP Client is in use:

```
# svcs -a | grep ldap | awk -F" " '{if ($1 ~ /disabled/ && $3 ~ /client/)
print "LDAP Client is disabled - svc:/network/nfs/domain can be disabled.";}'
```

If LDAP is not in use also disable nis/domain:

```
# svcadm disable svc:/network/nis/domain
```

Notes:

It is possible that the `svc:/network/nis/server` package may not be installed by default on some systems. In this case, the above commands will indicate that the software is not installed.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.10 Disable Removable Volume Manager (Scored)

Profile Applicability:

- Level 1

Description:

The HAL-aware removable volume manager in the Solaris 11 OS automatically mounts external devices for users whenever the device is attached to the system. These devices include CD-R, CD-RW, floppies, DVD, USB and 1394 mass storage devices. See the `rmvolmgr`(1M) manual page for more details.

Rationale:

Allowing users to mount and access data from removable media devices makes it easier for malicious programs and data to be imported onto the network. It also introduces the risk that sensitive data may be transferred off the system without a log record. By adding rmvolmgr to the `.xinitrc` file, user-isolated instances of `rmvolmgr` can be run via a session startup script. In such cases, the `rmvolmgr` instance will not allow management of volumes that belong to other than the owner of the startup script. When a user logs onto the workstation console (`/dev/console`), any instance of user-initiated `rmvolmgr` will only own locally connected devices, such as CD-ROMs or flash memory hardware, locally connected to USB or FireWire ports.

Audit:

Perform the following and verify that the result is as shown:

```
# svcs -Ho state svc:/system/filesystem/rmvolmgr

disabled

# svcs -Ho state svc:/network/rpc/smserver

disabled
```

If the service is not installed, this will return an error, or no output. This is also considered a passing state.

Remediation:

To disable this service, run the following commands:

```
# svcadm disable svc:/system/filesystem/rmvolmgr

# svcadm disable svc:/network/rpc/smserver
```

Notes:

`rmformat` is a `rpc.smserverd` client. If you need to support this service, but still want to disable `rmvolmgr`, then do not disable `smserver` in the action above.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.11 Disable automount Service (Scored)

Profile Applicability:

- Level 1

Description:

The `automount` daemon is normally used to automatically mount NFS file systems from remote file servers when needed. However, the `automount` daemon can also be configured to mount local (loopback) file systems as well, which may include local user home directories, depending on the system configuration.

Rationale:

This service should be disabled if it is not required.

Audit:

Perform the following and verify that the result is as shown:

```
# svcs -Ho state svc:/system/filesystem/autofs

disabled
```

If the service is not installed, this will return an error, or no output. This is also considered a passing state.

Remediation:

To disable this service, run the following command:

```
# svcadm disable svc:/system/filesystem/autofs
```

Notes:

By default, the Solaris 11 OS uses the `automount` service for local user home directories, so it should not be disabled without adjusting the home directory setting of each local user.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.12 Disable Telnet Service (Scored)

Profile Applicability:

- Level 1

Description:

The `telnet` daemon, which accepts connections from users from other systems via the `telnet` protocol and can be used for remote shell access.

Rationale:

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow a user with access to sniff network traffic the ability to steal credentials. The `ssh protocol` provides an encrypted session and stronger security.

Audit:

Ensure `telnet` server is not enabled:

```
# svcs -Ho state svc:/network/telnet

disabled
```

If the service is not installed, this will return an error, or no output. This is also considered a passing state.

Remediation:

Disable `telnet` server if enabled:

```
# svcadm disable svc:/network/telnet
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3 Kernel Tuning

This section describes additional measures that may be taken to provide protection on the kernel level.

3.1 Disable Response to Broadcast ICMPv4 Echo Request (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether Solaris responds to broadcast ICMPv4 echo requests.

Rationale:

Reduce attack surface by restricting this vector used for host discovery and to prevent denial of service attacks.

Audit:

To verify this setting, use the commands:

```
# ipadm show-prop -p _respond_to_echo_broadcast -co current ip

0

# ipadm show-prop -p _respond_to_echo_broadcast -co persistent ip

0
```

Remediation:

To enforce this setting, use the command:

```
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.2 Disable Response to ICMP Broadcast Netmask Requests (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether Solaris will respond to ICMP broadcast netmask requests.

Rationale:

Reduce attack surface by restricting this vector used for host and network discovery and to prevent denial of service attacks.

Audit:

To verify this setting, use the commands:

```
# ipadm show-prop -p _respond_to_address_mask_broadcast -co current ip
0
# ipadm show-prop -p _respond_to_address_mask_broadcast -co persistent ip
0
```

Remediation:

To enforce this setting, use the command:

```
# ipadm set-prop -p _respond_to_address_mask_broadcast=0 ip
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.3 Enable Strong TCP Sequence Number Generation (Scored)

Profile Applicability:

- Level 1

Description:

The variable `TCP_STRONG_ISS` defines the mechanism used for TCP initial sequence number generation. If an attacker can predict the next sequence number, it is possible to inject fraudulent packets into the data stream to hijack the session.

Rationale:

The RFC 1948 method is widely accepted as the strongest mechanism for TCP packet generation. This makes remote session hijacking attacks more difficult, as well as any other network-based attack that relies on predicting TCP sequence number information. It is theoretically possible that there may be a small performance hit in connection setup time when this setting is used, but there are no publicly available benchmarks that establish this.

Audit:

To verify the setting is in effect in the `/etc/default/inetinit` file, use the command:

```
# grep "^TCP_STRONG_ISS=" /etc/default/inetinit

TCP_STRONG_ISS=2
```

To verify this setting is in effect on the running system, use the command:

```
# ipadm show-prop -p _strong_iss -co current tcp

2
```

Remediation:

Run the following commands to set the `TCP_STRONG_ISS` parameter to use RFC 1948 sequence number generation in the `/etc/default/inetinit` file:

```
# cd /etc/default

# awk '/TCP_STRONG_ISS=/ { $1 = "TCP_STRONG_ISS=2" }; { print }' inetinit >
inetinit.CIS

# mv inetinit.CIS inetinit
```

To set the `TCP_STRONG_ISS` parameter on a running system, use the command:

```
# ipadm set-prop -p _strong_iss=2 tcp
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.4 Disable Response to ICMP Broadcast Timestamp Requests (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether Solaris will respond to ICMP broadcast timestamp requests.

Rationale:

Reduce attack surface by restricting this vector used for host discovery and to prevent denial of service attacks.

Audit:

To verify this setting, use the commands:

```
# ipadm show-prop -p _respond_to_timestamp_broadcast -co current ip

0

# ipadm show-prop -p _respond_to_timestamp_broadcast -co persistent ip

0
```

Remediation:

To enforce this setting, use the command:

```
# ipadm set-prop -p _respond_to_timestamp_broadcast=0 ip
```

References:

1. http://capec.mitre.org/data/definitions/295.html

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.5 Disable Source Packet Forwarding (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether the IPv4 or IPv6 configuration will forward packets with IPv4 routing options or IPv6 routing headers.

Rationale:

Keep this parameter disabled to prevent denial of service attacks through spoofed packets.

Audit:

To verify this setting for IPv4 packets, use the commands:

```
# ipadm show-prop -p _forward_src_routed -co current ipv4
0
# ipadm show-prop -p _forward_src_routed -co persistent ipv4
0
```

To verify this setting for IPv6 packets, use the commands:

```
# ipadm show-prop -p _forward_src_routed -co current ipv6
0
# ipadm show-prop -p _forward_src_routed -co persistent ipv6
0
```

Remediation:

To enforce this setting for IPv4 packets, use the command:

```
# ipadm set-prop -p _forward_src_routed=0 ipv4
```

To enforce this setting for IPv6 packets, use the command:

```
# ipadm set-prop -p _forward_src_routed=0 ipv6
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.6 Disable Directed Broadcast Packet Forwarding (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether Solaris forwards broadcast packets for a specific network if it is directly connected to the machine.

Rationale:

Keep this parameter disabled to prevent denial of service attacks.

Audit:

To verify this setting, use the commands:

```
# ipadm show-prop -p _forward_directed_broadcasts -co current ip
0
# ipadm show-prop -p _forward_directed_broadcasts -co persistent ip
0
```

Remediation:

To enforce this setting, use the command:

```
# ipadm set-prop -p _forward_directed_broadcasts=0 ip
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.7 Enable Stack Protection (Scored)

Profile Applicability:

- Level 1

Description:

Buffer overflow exploits have been the basis for many highly publicized compromises and defacements of large numbers of Internet connected systems. Many of the automated tools in use by system attackers exploit well-known buffer overflow problems in vendor-supplied and third party software.

Rationale:

Enabling stack protection prevents certain classes of buffer overflow attacks and is a significant security enhancement. However, this does not protect against buffer overflow attacks that do not execute code on the stack (such as `return-to-libc` exploits). While most of the Solaris OS is already configured to employ a non-executable stack, this setting is still recommended to provide a more comprehensive solution for both Solaris and other software that may be installed.

Audit:

Perform the following and verify that the result is as shown:

```
# sxadm status -po extension,status,configuration nxheap,nxstack

nxheap:enabled.tagged-files:default.default
nxstack:enabled.all:default.default
```

Remediation:

To enable stack protection and block stack-smashing attacks, run the following:

```
# sxadm delcust nxheap

# sxadm delcust nxstack
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.8 Restrict Core Dumps to Protected Directory (Scored)

Profile Applicability:

- Level 1

Description:

The action described in this section creates a protected directory to store core dumps and also causes the system to create a log entry whenever a regular process dumps core.

Rationale:

Core dumps, particularly those from set-UID and set-GID processes, may contain sensitive data.

Audit:

Perform the following and verify that the result is as shown:

```
# coreadm

     global core file pattern:
     global core file content: default
     kernel zone core file pattern:
     init core file pattern: core
     init core file content: default
     global core dumps: disabled
     kernel zone core dumps: disabled
     per-process core dumps: enabled
     global setid core dumps: disabled
     per-process setid core dumps: disabled
     global core dump logging: disabled
     diagnostic core dumps: enabled
     retention policy: summary
     core diagnostic alert: enabled

# ls -ld /var/share/cores

drwx------   2 root     sys            2 Aug 20  2018 /var/share/cores
```

Remediation:

To implement the recommendation, run the commands:

```
# chmod 700 /var/share/cores

# coreadm -g /var/share/cores/core_%n_%f_%u_%g_%t_%p \
        -e log -e global -e global-setid \
        -d process -d proc-setid
```

If the local site chooses, dumping of core files can be completely disabled with the following command:

```
# coreadm -d global -d global-setid -d process -d proc-setid
```

CIS Controls:

Version 7

13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization

Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

3.9 Disable Response to ICMP Timestamp Requests (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether Solaris will respond to ICMP timestamp requests.

Rationale:

Reduce attack surface by restricting this vector used for host discovery.

Audit:

To verify this setting, use the commands:

```
# ipadm show-prop -p _respond_to_timestamp -co current ip
0
# ipadm show-prop -p _respond_to_timestamp -co persistent ip
0
```

Remediation:

To enforce this setting, use the command:

```
# ipadm set-prop -p _respond_to_timestamp=0 ip
```

References:

1. http://capec.mitre.org/data/definitions/295.html

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.10 Disable Response to Multicast Echo Request (Scored)

Profile Applicability:

- Level 1

Description:

These settings control whether Solaris responds to multicast IPv4 and IPv6 echo requests.

Rationale:

Reduce attack surface by restricting this vector used for host discovery and to prevent denial of service attacks.

Audit:

To verify this setting for IPv4 packets, use the commands:

```
# ipadm show-prop -p _respond_to_echo_multicast -co current ipv4
0
# ipadm show-prop -p _respond_to_echo_multicast -co persistent ipv4
0
```

To verify this setting for IPv6 packets, use the commands:

```
# ipadm show-prop -p _respond_to_echo_multicast -co current ipv6
0
# ipadm show-prop -p _respond_to_echo_multicast -co persistent ipv6
0
```

Remediation:

To enforce this setting for IPv4 packets, use the command:

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
```

To enforce this setting for IPv6 packets, use the command:

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv6
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.11 Ignore ICMP Redirect Messages (Scored)

Profile Applicability:

- Level 1

Description:

These settings control whether Solaris will ignore ICMP redirect messages.

Rationale:

IP redirects should not be necessary in a well-designed and maintained network. Set to a value of 1 if there is a high risk for a DoS attack. Otherwise, the default value of 0 is sufficient.

Audit:

To verify this setting for IPv4 packets, use the commands:

```
# ipadm show-prop -p _ignore_redirect -co current ipv4

1

# ipadm show-prop -p _ignore_redirect -co persistent ipv4

1
```

To verify this setting for IPv6 packets, use the commands:

```
# ipadm show-prop -p _ignore_redirect -co current ipv6

1

# ipadm show-prop -p _ignore_redirect -co persistent ipv6

1
```

Remediation:

To enforce this setting for IPv4 packets, use the command:

```
# ipadm set-prop -p _ignore_redirect=1 ipv4
```

To enforce this setting for IPv6 packets, use the command:

```
# ipadm set-prop -p _ignore_redirect=1 ipv6
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.12 Set Strict Multihoming (Scored)

Profile Applicability:

- Level 1

Description:

These settings control whether a packet arriving on a non-forwarding interface can be accepted for an IP address that is not explicitly configured on that interface.

Rationale:

Enable this setting for systems that have interfaces that cross strict networking domains (for example, a firewall or a VPN node).

Audit:

To verify this setting for IPv4 packets, use the commands:

```
# ipadm show-prop -p _strict_dst_multihoming -co current ipv4
1
# ipadm show-prop -p _strict_dst_multihoming -co persistent ipv4
1
```

To verify this setting for IPv6 packets, use the commands:

```
# ipadm show-prop -p _strict_dst_multihoming -co current ipv6
1
# ipadm show-prop -p _strict_dst_multihoming -co persistent ipv6
1
```

Remediation:

To enforce this setting for IPv4 packets, use the command:

```
# ipadm set-prop -p _strict_dst_multihoming=1 ipv4
```

To enforce this setting for IPv6 packets, use the command:

```
# ipadm set-prop -p _strict_dst_multihoming=1 ipv6
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.13 Disable ICMP Redirect Messages (Scored)

Profile Applicability:

- Level 1

Description:

These setting controls whether Solaris sends ICMPv4 and ICMPv6 redirect messages.

Rationale:

A malicious user can exploit the ability of the system to send ICMP redirects by continually sending packets to the system, forcing the system to respond with ICMP redirect messages, resulting in an adverse impact on the CPU performance of the system.

Audit:

To verify this setting for IPv4 packets, use the commands:

```
# ipadm show-prop -p send_redirects -co current ipv4

off

# ipadm show-prop -p send_redirects -co persistent ipv4

off
```

To verify this setting for IPv6 packets, use the commands:

```
# ipadm show-prop -p send_redirects -co current ipv6

off

# ipadm show-prop -p send_redirects -co persistent ipv6

off
```

Remediation:

To enforce this setting for IPv4 packets, use the command:

```
# ipadm set-prop -p send_redirects=off ipv4
```

To enforce this setting for IPv6 packets, use the command:

```
# ipadm set-prop -p send_redirects=off ipv6
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.14 Disable TCP Reverse IP Source Routing (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls whether TCP reverses the IP source routing option for incoming connections.

Rationale:

If IP source routing is needed for diagnostic purposes, enable it. Otherwise disable it.

Audit:

To verify this setting, use the commands:

```
# ipadm show-prop -p _rev_src_routes -co current tcp
0
# ipadm show-prop -p _rev_src_routes -co persistent tcp
0
```

Remediation:

To enforce this setting, use the command:

```
# ipadm set-prop -p _rev_src_routes=0 tcp
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.15 Set Maximum Number of Half-open TCP Connections (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls how many half-open connections can exist for a TCP port.

Rationale:

It is necessary to control the number of completed connections to the system to provide some protection against Denial of Service attacks. Note that the value of 4096 is a minimum to establish a good security posture for this setting. In environments where connections numbers are high, such as a busy webserver, this value may need to be increased.

Audit:

To verify this setting, use the commands:

```
# ipadm show-prop -p _conn_req_max_q0 -co current tcp

4096

# ipadm show-prop -p _conn_req_max_q0 -co persistent tcp

4096
```

Remediation:

To enforce this setting, use the command:

```
# ipadm set-prop -p _conn_req_max_q0=4096 tcp
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.16 Set Maximum Number of Incoming Connections (Scored)

Profile Applicability:

- Level 1

Description:

This setting controls the maximum number of incoming connections that can be accepted on a TCP port.

Rationale:

Note that the value of `1024` is a minimum to establish a good security posture for this setting. In environments where connections numbers are high, such as a busy webserver, this value may need to be increased.

Audit:

To verify this setting, use the commands:

```
# ipadm show-prop -p _conn_req_max_q -co current tcp

1024

# ipadm show-prop -p  conn req max q -co persistent tcp

1024
```

Remediation:

To enforce this setting, use the command:

```
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.17 Disable Network Routing (Scored)

Profile Applicability:

- Level 1

Description:

The network routing daemon, `in.routed`, manages network routing tables. If enabled, it periodically supplies copies of the system's routing tables to any directly connected hosts and networks and picks up routes supplied to it from other networks and hosts.

Rationale:

Routing Internet Protocol (RIP) is a legacy protocol with a number of security weaknesses including a lack of authentication, zoning, pruning, etc.

Audit:

To verify this setting for IPv4, use the command:

```
# routeadm -p | egrep "^ipv4-routing |^ipv4-forwarding " | awk '{printf("%s
%s\n", $1, $NF); }'

ipv4-routing current=disabled
ipv4-forwarding current=disabled
```

To verify this setting is persistent between reboots for IPv4, use the command:

```
# routeadm -p | egrep "^ipv4-routing |^ipv4-forwarding " | awk '{printf("%s
%s\n", $1, $2); }'

ipv4-routing persistent=disabled
ipv4-forwarding persistent=disabled
```

To verify this setting for IPv6, use the command:

```
# routeadm -p | egrep "^ipv6-routing |^ipv6-forwarding " | awk '{printf("%s
%s\n", $1, $NF); }'

ipv6-routing current=disabled
ipv6-forwarding current=disabled
```

To verify this setting is persistent between reboots for IPv6, use the command:

```
# routeadm -p | egrep "^ipv6-routing |^ipv6-forwarding " | awk '{printf("%s
%s\n", $1, $2); }'

ipv6-routing persistent=disabled
ipv6-forwarding persistent=disabled
```

Remediation:

To enforce this setting and disable IPv4 routing, use the command:

```
# routeadm -d ipv4-forwarding -d ipv4-routing
```

To enforce this setting and disable IPv6 routing, use the command:

```
# routeadm -d ipv6-forwarding -d ipv6-routing
```

To apply these changes to the running system, use the command:

```
# routeadm -u
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4 Auditing and Logging

With the release of the Solaris 11 OS, the Solaris Audit service is enabled by default. As a result, recommendations where audit and log information was typically configured and sent to the system log (`syslog`) facility have been modified to use the Solaris Audit service instead. Note that for sites that still require such information to be delivered over `syslog`, the Solaris Audit facility can be configured to deliver audit records to that service as well.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident), it is recommended that the time be synchronized among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices including Oracle Solaris 11. More information on NTP can be found at http://www.ntp.org.

4.1 Create CIS Audit Class (Scored)

Profile Applicability:

- Level 1

Description:

To group a set of related audit events, the Solaris Audit service provides the ability for sites to define their own audit classes that contain just those events that the site wants to audit.

Rationale:

To simplify administration, a CIS specific audit class should be created.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep ":CIS Solaris Benchmark" /etc/security/audit_class

0x0100000000000000:cis:CIS Solaris Benchmark
```

Remediation:

To create the CIS audit class, edit the `/etc/security/audit_class` file and add the following entry before the last line of the file:

```
0x0100000000000000:cis:CIS Solaris Benchmark
```

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

4.2 Enable Auditing of Incoming Network Connections (Scored)

Profile Applicability:

- Level 1

Description:

The Solaris Audit service can be configured to record incoming network connections to any listening service running on the system.

Rationale:

This recommendation will provide an audit trail that contains information related to incoming network connections. While this functionality can be enabled using service-specific mechanisms, using the Solaris Audit service provides a more centralized and complete window into incoming network activity.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "cis" /etc/security/audit_event | awk -F: '{ print $2 }'

[…]
AUE_ACCEPT
AUE_CONNECT
AUE_SOCKACCEPT
AUE_SOCKCONNECT
AUE_inetd_connect
[…]
```

Remediation:

To enforce this setting, use the commands to modify the `/etc/security/audit_event` file and add the `cis` audit class to the following audit events:

```
# cp /etc/security/audit_event /etc/security/audit_event.orig

# awk 'BEGIN{FS=":"; OFS=":"} {if ($2 ~
/AUE_ACCEPT|AUE_CONNECT|AUE_SOCKACCEPT|AUE_SOCKCONNECT|AUE_inetd_connect/)
$4=$4",cis";} {print} ' etc/security/audit_event >
/etc/security/audit_event.out

# cp /etc/security/audit_event.out /etc/security/audit_event
```

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.3 Enable Auditing of File Metadata Modification Events (Scored)

Profile Applicability:

- Level 1

Description:

The Solaris Audit service can be configured to record file metadata modification events for every process running on the system. This will allow the auditing service to determine when file ownership, permissions and related information is changed.

Rationale:

This recommendation will provide an audit trail that contains information related to changes of file metadata. The Solaris Audit service is used to provide a more centralized and complete window into activities such as these.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "cis" /etc/security/audit_event | awk -F: '{ print $2 }'

[…]
AUE_CHMOD
AUE_CHOWN
AUE_FCHOWN
AUE_FCHMOD
AUE_LCHOWN
AUE_ACLSET
AUE_FACLSET
[…]
```

The output of this command may include additional audit event names that had previously been assigned to the `cis` audit class.

Remediation:

To enforce this setting, use the commands to modify the `/etc/security/audit_event` file and add the `cis` audit class to the following audit events:

```
# awk 'BEGIN{FS=":"; OFS=":"} {if ($2 ~
/AUE_CHMOD|AUE_CHOWN|AUE_FCHOWN|AUE_FCHMOD|AUE_LCHOWN|AUE_ACLSET|AUE_FACLSET/
) $4=$4",cis";} {print} ' /etc/security/audit_event >
/etc/security/audit_event.CIS

# cp /etc/security/audit_event.CIS /etc/security/audit_event
```

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.4 Enable Auditing of Process and Privilege Events (Scored)

Profile Applicability:

- Level 1

Description:

The Solaris Audit service can be configured to record the use of privileges by processes running on the system. This will capture events such as the setting of UID and GID values, setting of privileges, as well as the use of functionality such as `chroot(2)`.

Rationale:

This recommendation will provide an audit trail that contains information related to the use of privileges by processes running on the system. The Solaris Audit service is used to provide a more centralized and complete window into activities such as these.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "cis" /etc/security/audit_event | awk -F: '{ print $2 }'

[…]
AUE_CHROOT
AUE_SETREUID
AUE_SETREGID
AUE_FCHROOT
AUE_PFEXEC
AUE_SETUID
AUE_NICE
AUE_SETGID
AUE_PRIOCNTLSYS
AUE_SETEGID
AUE_SETEUID
AUE_SETPPRIV
AUE_SETSID
AUE_SETPGID
[…]
```

The output of this command may include additional audit event names that had previously been assigned to the `cis`audit class.

Remediation:

To enforce this setting, use the commands to modify the `/etc/security/audit_event` file and add the `cis` audit class to the following audit events:

```
# awk 'BEGIN{FS=":"; OFS=":"} {if ($2 ~
/AUE_CHROOT|AUE_SETREUID|AUE_SETREGID|AUE_FCHROOT|AUE_PFEXEC|AUE_SETUID|AUE_N
ICE|AUE_SETGID|AUE_PRIOCNTLSYS|AUE_SETEGID|AUE_SETEUID|AUE_SETPPRIV|AUE_SETSI
D|AUE_SETPGID/) $4=$4",cis";} {print} ' /etc/security/audit_event >
/etc/security/audit_event.CIS

# cp /etc/security/audit_event.CIS /etc/security/audit_event
```

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.5 Configure Solaris Auditing (Scored)

Profile Applicability:

- Level 1

Description:

Solaris auditing service keeps a record of how a system is being used. Solaris auditing can be configured to record different classes of events based upon site policy. This recommendation will set and verify a consensus-developed auditing policy. That said, all organizations are encouraged to tailor this policy based upon their specific needs. For more information on the Solaris auditing service including how to filter and view events, see the Oracle Solaris product documentation.

The "`cis`" class is a "custom class" that CIS recommends creating that includes specifically those events that are of interest (defined in the sections above). In addition to those events, this recommendation also includes auditing of login and logout (`lo`) events, administrative (`ad`) events, file transfer (`ft`) events, and command execution (`ex`) events.

This recommendation also configures the Solaris auditing service to capture and report command line arguments (for command execution events) and the zone name in which a command was executed (for global and non-global zones). Further, this recommendation sets a disk utilization threshold of 1%. If this threshold is crossed (for the volume that includes `/var/shares/audit`), then a warning e-mail will be sent to advise the system administrators that audit events may be lost if the disk becomes full. Finally, this recommendation will also ensure that new audit trails are created at the start of each new day (to help keep the size of the files small to facilitate analysis).

Rationale:

The consensus settings described in this section are an effort to log interesting system events without consuming excessive amounts of resources logging significant but usually uninteresting system calls.

Audit:

Perform the following to determine if the system is configured as recommended:

```
# auditconfig -getcond

audit condition = auditing

# auditconfig -getpolicy

configured audit policies = argv,cnt,zonename
active audit policies = argv,cnt,zonename

# auditconfig -getflags

configured user default audit flags =
ad,ft,lo,ex,cis(0x1000000800f1080,0x1000000800f1080)
active user default audit flags =
ad,ft,lo,ex,cis(0x1000000800f1080,0x1000000800f1080)

# auditconfig -getnaflags

configured non-attributable audit flags = lo(0x1000,0x1000)
active non-attributable audit flags = lo(0x1000,0x1000)

# auditconfig -getplugin audit_binfile

Plugin: audit_binfile (active)
        Attributes:
p_age=0h;p_dir=/var/audit;p_flags=all;p_fsize=0;p_minfree=1

# userattr audit_flags root

lo,ad,ft,ex,cis:no

# ls -l /var/share/audit/*.not_terminated.*

[verify that the file size is not zero and is growing as events are audited]
```

Remediation:

To enforce this setting, use the commands:

```
# auditconfig -conf

# auditconfig -setflags lo,ad,ft,ex,cis

# auditconfig -setnaflags lo

# auditconfig -setpolicy cnt,argv,zonename

# auditconfig -setplugin audit_binfile active p_minfree=1

# audit -s

# rolemod -K audit_flags=lo,ad,ft,ex,cis:no root

# EDITOR=ed crontab -e root << END_CRON
$
a
0 0 * * * /usr/sbin/audit -n
.
w
q
END_CRON

# chown root:root /var/shares/audit

# chmod 750 /var/shares/audit
```

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

5 File/Directory Permissions/Access

File and directory permission control is one of the greatest challenges of secure system administration. This section provides guidance on how to secure system files and directories and set secure defaults for users. Guidance for monitoring user and system files on an on-going basis is provided in the System Maintenance section of this document.

5.1 Set Sticky Bit on World Writable Directories (Not Scored)

Profile Applicability:

- Level 1

Description:

When the so-called sticky bit (set with chmod +t) is set on a directory, then only the owner of a file may remove that file from the directory (as opposed to the usual behavior where anybody with write access to that directory may remove the file).

Rationale:

Files in directories that have had the 'sticky bit' set, can only be deleted by users that have both write permissions for the directory in which the file resides, as well as ownership of the file or directory, or has sufficient privilege. As this prevents users from overwriting each other's files, whether it be accidental or malicious, it is generally appropriate for most world-writable directories (e.g., `/tmp`). However, consult appropriate vendor documentation before blindly applying the sticky bit to any world writable directories found, in order to avoid breaking any application dependencies on a given directory.

Audit:

Perform the following to verify that the result is as recommended:

```
# find / \( -fstype nfs -o -fstype cachefs -o -fstype autofs -o -fstype ctfs
-o -fstype mntfs -o -fstype objfs -o -fstype proc \) -prune -o -type d \( -
perm -0002 -a ! -perm -1000 \) -ls
```

No output should be returned.

Remediation:

To set the sticky bit on a directory, run the following command:

```
# chmod +t [directory name]
```

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6 System Access, Authentication, and Authorization

The actions described in this section are just a few measures that can be taken at a system level to control access to the system and its services. It is strongly advised that organizations have a process in place to document, authorize, and validate access privileges and to revoke authorizations when they are no longer required.

6.1 Disable login: Services on Serial Ports (Scored)

Profile Applicability:

- Level 1

Description:

The `svccfg` command provides service administration for the lower level of the Service Access Facility hierarchy and can be used to disable the ability to login on a particular port.

Rationale:

Login services should not be enabled on any serial ports that are not strictly required to support the mission of the system. This action can be safely performed even when console access is provided using a serial port.

Audit:

Perform the following to verify that the result is as recommended:

```
# svcs -Ho state svc:/system/console-login:terma

disabled

# svcs -Ho state svc:/system/console-login:termb

disabled
```

Remediation:

Perform the following to implement the recommended state:

```
# svcadm disable svc:/system/console-login:terma

# svcadm disable svc:/system/console-login:termb
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.2 Set EEPROM Security Mode and Log Failed Access (SPARC) (Not Scored)

Profile Applicability:

- Level 1

Description:

Oracle SPARC systems support the use of an EEPROM password for the console.

Rationale:

Setting the EEPROM password helps prevent attackers who gain physical access to the system console from booting from an external device (such as a CD-ROM or floppy).

Audit:

Perform the following to verify that the result is as recommended:

```
# eeprom security-mode | awk -F= '{ print $2 }'

[command|full|none]

# eeprom security-#badlogins | awk -F= '{ print $2 }'

0
```

If a password has been set, the command will return `command` or `full`. If a password has not been set, the command will return `none`.

Remediation:

Perform the following to implement the recommended state:

```
# eeprom security-mode=command

# eeprom security-#badlogins=0
```

After entering the last command above, the administrator will be prompted for a password. This password will be required to authorize any future command issued at boot-level on the system (the ok or > prompt) except for the normal multi-user boot command (i.e., the system will be able to reboot unattended).
Write down the password and store it in a sealed envelope in a secure location (note that locked desk drawers are typically not secure). If the password is lost or forgotten, simply log into the system and run the command:

```
# eeprom security-mode=none
```

This will erase the forgotten password. If the password is lost or forgotten and this action cannot be completed, then the EEPROM must be replaced to gain access to the system.
To set a new password, run the command:

```
# eeprom security-mode=command
```

Impact:

If the EEPROM password is lost or forgotten and `# eeprom security-mode=none` cannot be completed, then the EEPROM must be replaced to gain access to the system

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.3 Restrict at/cron to Authorized Users (Scored)

Profile Applicability:

- Level 1

Description:

The `cron.allow` and `at.allow` files contain a list of users who are allowed to run the `crontab` and at commands to submit jobs to be run at scheduled intervals.

Rationale:

On many systems, only the system administrator needs the ability to schedule jobs. Even though a given user is not listed in `cron.allow`, `cron` jobs can still be run as that user. The `cron.allow` file only controls administrative access to the `crontab` command for scheduling and modifying `cron` jobs. Much more effective access controls for the `cron` system can be obtained by using Role-Based Access Controls (RBAC).

Audit:

Perform the following to verify that the result is as recommended:

```
# ls /etc/cron.d/cron.deny

/etc/cron.d/cron.deny: No such file or directory

# ls /etc/cron.d/at.deny

/etc/cron.d/at.deny: No such file or directory

# cat /etc/cron.d/cron.allow

root

# wc -l /etc/cron.d/at.allow | awk '{ print $1 }'

 0
```

Remediation:

Perform the following to implement the recommended state:

```
# mv /etc/cron.deny /etc/cron.deny.cis

# mv /etc/at.deny /etc/at.deny.cis

# echo root > /etc/cron.allow

# cp /dev/null at.allow

# chown root:root cron.allow at.allow

# chmod 400 cron.allow at.allow
```

Note that the root/superuser is always allowed to use the `at` command and is not required to be specifically listed in `at.allow`.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.4 Set Default Screen Lock for GNOME Users (Scored)

Profile Applicability:

- Level 1

Description:

The `timeout` parameter dictates the invocation of a password-protected screen saver after a specified time of keyboard and mouse inactivity, specific to the `xscreensaver` application used in the GNOME windowing environment.

Rationale:

As a screensaver timeout provides protection for a desktop that has not been locked by the user upon his/her departure, to help prevent session hijacking, this value should be set as appropriate to the needs of the user.

Audit:

Perform the following to verify that the result is as recommended:

```
# cd /usr/share/X11/app-defaults

# grep "^\*timeout:" XScreenSaver

*timeout: 0:10:00

# grep "^\*lockTimeout:" XScreenSaver

*lockTimeout: 0:00:00

# grep "^\*lock:" XScreenSaver

*lock: True
```

Remediation:

Perform the following to implement the recommended state:

```
# cd /usr/share/X11/app-defaults

# cp XScreenSaver XScreenSaver.orig

# awk '/^\*timeout:/ { $2 = "0:10:00" } /^\*lockTimeout:/ { $2 = "0:00:00" }
/^\*lock:/ { $2 = "True" } { print }' xScreenSaver > xScreenSaver.CIS

# mv xScreenSaver.CIS xScreenSaver
```

CIS Controls:

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

6.5 Remove Autologin Capabilities from the GNOME desktop (Scored)

Profile Applicability:

- Level 1

Description:

The GNOME Display Manager is used for login session management. See the manual page `gdm`(1) for more information. By default, GNOME automatic login is defined in `/etc/pam.d/gdm-autologin` to allow users to access the system without a password.

Rationale:

As automatic logins are a known security risk for other than "kiosk" types of systems, GNOME automatic login should be disabled in `/etc/pam.d/gdm-autologin`.

Audit:

Ensure there are no uncommented `gdm-autologin` lines in `/etc/pam.d/gdm-autologin`:

```
# egrep "auth|account" /etc/pam.d/gdm-autologin | grep -vc ^#

0
```

If the command returns other than "0", this is a finding.

Remediation:

Comment out or remove all lines from `/etc/pam.d/gdm-autologin`:

```
# cp /etc/pam.d/gdm-autologin /etc/pam.d/gdm-autologin.orig

# awk '{ if ( $1 ~ /auth/ || $1 ~ /account/) $1 = "#"$1 } { print };'
/etc/pam.d/gdm-autologin > /etc/pam.d/gdm-autologin.CIS

# cp /etc/pam.d/gdm-autologin.CIS /etc/pam.d/gdm-autologin
```

CIS Controls:

Version 7

16.8 Disable Any Unassociated Accounts

Disable any account that cannot be associated with a business process or business owner.

6.6 Set Delay between Failed Login Attempts to 4 (Scored)

Profile Applicability:

- Level 1

Description:

The `SLEEPTIME` variable in the `/etc/default/login` file controls the number of seconds to wait before printing the "login incorrect" message when a bad password is provided. The default value for SLEEPTIME is 4 seconds.

Rationale:

As an immediate return of an error message, coupled with the capability to try again may facilitate automatic and rapid-fire brute-force password attacks by a malicious user, this delay time should be set as appropriate to the needs of the user.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^SLEEPTIME=" /etc/default/login

SLEEPTIME=4
```

If SLEEPTIME entry is commented out, this is also considered a passing state as the default value for `SLEEPTIME` is 4 seconds.

Remediation:

Perform the following to implement the recommended state:

```
# cd /etc/default

# cp login login.orig

# awk '/SLEEPTIME=/ { $1 = "SLEEPTIME=4" } { print }' login > login.CIS

# mv login.CIS login
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.7 Disable Rhost-based Authentication for SSH (Scored)

Profile Applicability:

- Level 1

Description:

The `IgnoreRhosts` parameter specifies that existing `.rhosts` and `.shosts` files, which may apply to application rather than user logins, will not be used in `RhostsRSAAuthentication` or `HostbasedAuthentication`.

Rationale:

Setting this parameter forces users to enter a password when authenticating with SSH.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^IgnoreRhosts" /etc/ssh/sshd_config

IgnoreRhosts yes
```

If the `IgnoreRhosts` line does not exist in the file, the default setting of `Yes` is automatically applied.

Remediation:

Perform the following to implement the recommended state:

```
# awk '/^IgnoreRhosts/ { $2 = "yes" } { print }' /etc/ssh/sshd config >
/etc/ssh/sshd_config.CIS

# mv /etc/ssh/sshd_config.CIS /etc/ssh/sshd_config

# svcadm restart svc:/network/ssh
```

This action will only set the `IgnoreRhosts` line if it already exists in the file to ensure that it is set to the proper value. If the `IgnoreRhosts` line does not exist in the file, the default setting of `Yes` is automatically used, so no additional changes are needed.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.8 Restrict FTP Use (Scored)

Profile Applicability:

- Level 1

Description:

If FTP is permitted to be used on the system, the file `/etc/ftpd/ftpusers` is used to specify a list of users who are not allowed to access the system via FTP.

Rationale:

FTP is an old and insecure protocol that transfers files and credentials in clear text and can be replaced by using `sftp`. However, if FTP is permitted for use in your environment, it is important to ensure that the default "system" accounts are not permitted to transfer files via FTP, especially the `root` role. Consider also adding the names of other privileged or shared accounts that may exist on your system such as user `oracle` and the account which your Web server process runs under. It should be reminded that the Solaris FTP service is disabled by default.

Audit:

Perform the following to verify that the result is as recommended:

```
# for user in `logins -s | awk '{ print $1 }'` aiuser noaccess nobody
nobody4; do
 grep -w "${user}" /etc/ftpd/ftpusers >/dev/null 2>&1
 if [ $? != 0 ]; then
 echo "User '${user}' not in /etc/ftpd/ftpusers."
 fi
done
```

(No output should be returned.)

Remediation:

Perform the following to implement the recommended state:

```
# cd /etc/ftpd

# cp ftpusers ftpusers.orig

# for user in `logins -s | awk '{ print $1 }'` aiuser noaccess nobody
nobody4; do
$(echo $user >> ftpusers)
done

# sort -u ftpusers > ftpusers.CIS

# mv ftpusers.CIS ftpusers
```

If your site policy states that users have to be authorized to use FTP, consider placing all users in the `/etc/ftpd/ftpusers` file and then explicitly removing those who are permitted to use the service. To accomplish this, use the command:

```
# getent passwd | cut -f1 -d":" > /etc/ftpd/ftpusers
```

This prohibits any user on the system from using ftp unless they are explicitly removed from the file. Note that this file will need to be updated as users are added to or removed from the system.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.9 Disable root login for SSH (Scored)

Profile Applicability:

- Level 1

Description:

The `PermitRootLogin` value (in `/etc/ssh/sshd_config`) allows for direct `root` login by a remote user/application to resources on the local host.

Rationale:

By default, it is not possible for the `root` account to log directly into the system console because the account is configured as a role. This setting therefore does not significantly alter the security posture of the system unless the `root` account is changed from this default and configured to be a normal user.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^PermitRootLogin" /etc/ssh/sshd_config

PermitRootLogin no
```

Remediation:

Perform the following to implement the recommended state:

```
# awk '/^PermitRootLogin/ { $2 = "no" } { print }' /etc/ssh/sshd_config >
/etc/ssh/sshd_config.CIS

# mv /etc/ssh/sshd_config.CIS /etc/ssh/sshd_config

# svcadm restart svc:/network/ssh
```

CIS Controls:

Version 7

16.8 Disable Any Unassociated Accounts

Disable any account that cannot be associated with a business process or business owner.

6.10 Disable Host-based Authentication for Login-based Services (Scored)

Profile Applicability:

- Level 1

Description:

The `.rhosts` files are used for automatic login to remote hosts and contain username and hostname combinations. The `.rhosts` files are unencrypted (usually group- or world-readable) and present a serious risk in that a malicious user could use the information within to gain access to a remote host with the privileges of the original application or user.

Rationale:

The use of `.rhosts` authentication is an old and insecure protocol and can be replaced with public-key authentication using Secure Shell. As automatic authentication settings in the `.rhosts` files can provide a malicious user with sensitive system credentials, the use of `.rhosts` files should be disabled. It should be noted that by default the Solaris services that use this file, including `rsh` and `rlogin`, are disabled by default.

Audit:

In Solaris 11.4, the /etc/pam.conf is delivered with no entries. Ensure that no uncommented `pam_rhosts_auth` lines exist:

```
# grep "pam_rhosts_auth" /etc/pam.conf

#rlogin auth sufficient pam_rhosts_auth.so.1

#rsh auth sufficient pam_rhosts_auth.so.1

# grep "pam_rhosts_auth" /etc/pam.d/*
```

Remediation:

Edit `/etc/pam.conf` and any `/etc/pam.d/*` results from audit procedure and comment out or remove any `pam_rhosts_auth` lines:

```
#rlogin auth sufficient pam_rhosts_auth.so.1

#rsh auth sufficient pam_rhosts_auth.so.1
```

CIS Controls:

Version 7

16.5 Encrypt Transmittal of Username and Authentication Credentials

Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

6.11 Blocking Authentication Using Empty/Null Passwords for SSH (Scored)

Profile Applicability:

- Level 1

Description:

The `PermitEmptyPasswords` value allows for direct login through SSH without a password by a remote user/application to resources on the local host in the same way a standard remote login would.

Rationale:

Permitting login without a password is inherently risky.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^PermitEmptyPasswords" /etc/ssh/sshd_config

PermitEmptyPasswords no
```

If the PermitEmptyPasswords entry is commented out, this is also considered a passing state as the default value is “no”.

Remediation:

Perform the following to implement the recommended state:

```
# awk '/^.PermitEmptyPasswords/ { $1 = “PermitEmptyPasswords” ; $2 = "no" } { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.CIS

# mv /etc/ssh/sshd_config.CIS /etc/ssh/sshd_config

# svcadm restart svc:/network/ssh
```

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

6.12 Limit Consecutive Login Attempts for SSH (Scored)

Profile Applicability:

- Level 1

Description:

The 'MaxAuthTries' parameter in the `/etc/ssh/sshd_config` file specifies the maximum number of authentication attempts permitted per connection. By restricting the number of failed authentication attempts before the server terminates the connection, malicious users are blocked from gaining access to the host by using repetitive brute-force login exploits.

Rationale:

By setting the authentication login limit to a low value this will disconnect the attacker and force a reconnect, which severely limits the speed of such brute force attacks.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^MaxAuthTries" /etc/ssh/sshd_config

MaxAuthTries 6
```

If MaxAuthTries is commented out, this is also considered a passing state as the default setting is 6.

Remediation:

Perform the following to implement the recommended state:

```
# awk '/MaxAuthTries/ { $1 = "MaxAuthTries"; $2 = "6" } { print }'
/etc/ssh/sshd_config > /etc/ssh/sshd_config.CIS

# mv /etc/ssh/sshd_config.CIS /etc/ssh/sshd_config

# svcadm restart svc:/network/ssh
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.13 Disable X11 Forwarding for SSH (Scored)

Profile Applicability:

- Level 1

Description:

The `X11 Forwarding` parameter defined within the `/etc/ssh/sshd_config` file specifies whether or not X11 Forwarding via SSH is enabled on the server: The Secure Shell service provides an encrypted 'tunnel' for the data traffic passing through it. While commonly used to substitute for clear-text, CLI-based remote connections such as telnet, Secure Shell can be used to forward an 'X Window' session through the encrypted tunnel, allowing the remote user to have a GUI interface.

Rationale:

As enabling X11Forwarding on the host can permit a malicious user to secretly open another X11 connection to another remote client during the session and perform unobtrusive activities such as keystroke monitoring, if the X11 services are not required for the system's intended function, it should be disabled or restricted as appropriate to the user's needs.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^X11Forwarding" /etc/ssh/sshd_config

X11Forwarding no
```

Remediation:

Perform the following to implement the recommended state:

```
# cp /etc/ssh/sshd_config /etc/ssh/sshd_config.orig

# awk '/^X11Forwarding / { $2 = "no" } { print }' /etc/ssh/sshd_config >
/etc/ssh/sshd_config.CIS

# mv /etc/ssh/sshd_config.CIS /etc/ssh/sshd_config

# svcadm restart svc:/network/ssh
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.14 Disable "nobody" Access for RPC Encryption Key Storage Service (Scored)

Profile Applicability:

- Level 1

Description:

This action listed prevents `keyserv` from using default keys for the nobody user, effectively stopping the nobody user from accessing information via Secure RPC.

Rationale:

If login by the user `nobody` is allowed for secure RPC, there is an increased risk of system compromise. If `keyserv` holds a private key for the nobody user, it will be used by `key_encryptsession` to compute a magic phrase which can be easily recovered by a malicious user.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^ENABLE_NOBODY_KEYS=" /etc/default/keyserv

ENABLE NOBODY KEYS=NO
```

This will return an error if the file does not exist due to the service not being installed. This is also considered a passing state.

Remediation:

Perform the following to implement the recommended state:

```
# cd /etc/default

# cp keyserv keyserv.orig

# awk '/ENABLE_NOBODY_KEYS=/ { $1 = "ENABLE_NOBODY_KEYS=NO" } { print }'
keyserv > keyserv.CIS

# mv keyserv.CIS keyserv
```

CIS Controls:

Version 7

16.8 Disable Any Unassociated Accounts

Disable any account that cannot be associated with a business process or business owner.

6.15 Secure the GRUB Menu (Intel) (Scored)

Profile Applicability:

- Level 1

Description:

GRUB is a boot loader for x64 based systems that permits loading an OS image from any location. Oracle x64 systems support the use of a GRUB Menu password for the console.

Rationale:

The flexibility that GRUB provides creates a security risk if its configuration is modified by an unauthorized user. The failsafe menu entry needs to be secured in the same environments that require securing the systems firmware to avoid unauthorized removable media boots. Setting the `GRUB Menu` password helps prevent attackers with physical access to the system console from booting off some external device (such as a CD-ROM or floppy) and subverting the security of the system. The actions described in this section will ensure you cannot get to failsafe or any of the GRUB command line options without first entering the password.

Audit:

Perform the following to verify that the result is as recommended:

```
# psrinfo -pv | awk '/GenuineIntel/ {print substr($2, 2)}'

GenuineIntel

# /usr/bin/grep "password.cfg" /rpool/boot/grub/grub.cfg

source /@/boot/grub/password.cfg
```

Remediation:

Run the following command to generate your password hash:

```
# /usr/lib/grub2/bios/bin/grub-mkpasswd-pbkdf2

Enter password:
Reenter password:
PBKDF2 hash of your password is <em><password_hash></em>
```

Create the file `/usr/lib/grub2/bios/etc/grub.d/01\_password`:

```
#!/bin/sh
/usr/bin/cat > /rpool/boot/grub/password.cfg<<EOF
#
# GRUB password
#
set superusers="root"
password_pbkdf2 root <em><password_hash></em>
EOF
/usr/bin/chmod 600 /rpool/boot/grub/password.cfg
/usr/bin/echo 'source /@/boot/grub/password.cfg'
```

Run the following to finalize the password configuration and set menu timeout:

```
# /usr/bin/chmod 700 /usr/lib/grub2/bios/etc/grub.d/01_password

# /usr/sbin/bootadm set-menu timeout=30
```

Changes will take effect on the next reboot.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.16 Restrict root Login to System Console (Scored)

Profile Applicability:

- Level 1

Description:

Privileged access to the system via `root` must be accountable to a particular user.

Rationale:

Use an authorized mechanism such as RBAC and the `su` command to provide administrative access to unprivileged accounts. These mechanisms provide an audit trail in the event of problems.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^CONSOLE=/dev/console" /etc/default/login

CONSOLE=/dev/console
```

Remediation:

Perform the following to implement the recommended state:

```
# cd /etc/default

# awk '/CONSOLE=/ { print "CONSOLE=/dev/console"; next }; { print }' login >
login.CIS

# mv login.CIS login
```

CIS Controls:

Version 7

16.8 Disable Any Unassociated Accounts

Disable any account that cannot be associated with a business process or business owner.

6.17 Set Retry Limit for Account Lockout (Scored)

Profile Applicability:

- Level 1

Description:

The `RETRIES` parameter is the number of failed login attempts a user is allowed before being disconnected from the system and forced to reconnect. When `LOCK_AFTER_RETRIES` is set in `/etc/security/policy.conf`, then the user's account is locked after this many failed retries (the account can only be unlocked by the administrator using the command: `passwd -u <username>`. The account lockout threshold (`RETRIES` parameter) restricts the number of failed login attempts allowed before requiring the offending account be locked. The lockout requirement will help block malicious users from gaining access to the host via automated, repetitive brute-force login exploits--trying different passwords until one fits a user name.

Rationale:

Setting the failed login limit to an appropriate value locks the user account, which will severely limit the speed of such attacks, making it much more likely that the attacker's pattern will be noticed and the offending source address and/or port blocked, so this should be set according to the needs of the user.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^RETRIES=" /etc/default/login

RETRIES=3

# grep "^LOCK_AFTER_RETRIES=" /etc/security/policy.conf

LOCK_AFTER_RETRIES=YES

# userattr lock_after_retries <username>
```

(Output should be "no" for any accounts that are exempt from this policy including "root".)

Remediation:

Perform the following to implement the recommended state:

```
# cd /etc/default

# awk '/RETRIES=/ { $1 = "RETRIES=3" } { print }' login >login.CIS

# mv login.CIS login

# cd /etc/security

# awk '/LOCK_AFTER_RETRIES=/ { $1 = "LOCK_AFTER_RETRIES=YES" } { print }'
policy.conf > policy.conf.CIS

# mv policy.conf.CIS policy.conf

# svcadm restart svc:/system/name-service/cache
```

Be careful when enabling these settings as they can create a denial-of-service situation for legitimate users and applications. Account lockout can be disabled for specific users via the usermod command. For example, the following command disables account lock specifically for the oracle account:

```
# usermod -K lock_after_retries=no oracle
```

Note: The root role is configured in this manner by default to prevent accidental lock out.

Notes:

The action specified here sets the lockout limit at 3, which complies with NSA/DISA recommendations, but may be too restrictive for some organizations.

CIS Controls:

Version 7

16.7 Establish Process for Revoking Access

Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

7 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment. Guidance for monitoring these settings and others that may change over time is provided in the System Maintenance section of this document.

7.1 Set Password Expiration Parameters on Active Accounts (Scored)

Profile Applicability:

- Level 1

Description:

The characteristics of an operating system that make 'user identification' via password a secure and workable solution is the combination of settings chosen. By requiring that a series of password-choices be security-centric, it reduces the risk of a malicious user breaking the password through dictionary/brute force attacks or fortuitous guessing based upon 'social engineering.' A basic password security strategy is requiring a new password to be chosen every 45-90 days, so that repeated attempts to gain entry by brute-force tactics will fail when a new password is chosen, which requires starting over again to break the new password.

Rationale:

The commands for this item set all active accounts (except the `root` account) to force password changes every 91 days (13 weeks), and then prevent password changes for seven days (one week), thereafter. Users will begin receiving warnings 7 days (1 week) before their password expires. Sites also have the option of expiring idle accounts after a certain number of days (see the on-line manual page for the `usermod` command, particularly the `-f` option).

Audit:

Perform the following to verify that the result is as recommended:

```
# logins -ox | awk -F: '( $1 != "root" && $8 != "LK" && $8 != "NL" && ( $10 <
7 || $11 > 91 || $12 < 7 )) { print }'
```

(No output should be returned.)

```
# grep "WEEKS=" /etc/default/passwd | sort -u

MAXWEEKS=13
MINWEEKS=1
WARNWEEKS=4
```

Remediation:

Perform the following to implement the recommended state:

```
# logins -ox | awk -F: '($1 == "root" || $8 == "LK" || $8 == "NL") { next } ;
{ cmd = "passwd" } ; ($11 < 91) { cmd = cmd " -x 91" } ($10 < 7) { cmd = cmd
" -n 7" } ($12 < 28) { cmd = cmd " -w 28" } (cmd != "passwd") { print cmd " "
$1 }' > /etc/CISupd_accounts

# /sbin/sh /etc/CISupd_accounts

# rm -f /etc/CISupd_accounts

# cd /etc/default

# cp passwd passwd.orig

# grep -v WEEKS passwd > passwd.CIS

# cat <<EODefaults >> passwd.CIS
MAXWEEKS=13
MINWEEKS=1
WARNWEEKS=1
EODefaults

# mv passwd.CIS passwd
```

Notes:

Since `/etc/default/passwd` sets defaults in terms of number of weeks (even though the actual values on user accounts are kept in terms of days), it is probably best to choose interval values that are multiples of 7.

CIS Controls:

Version 7

16.10 Ensure All Accounts Have An Expiration Date
Ensure that all accounts have an expiration date that is monitored and enforced.

7.2 Set Strong Password Creation Policies (Scored)

Profile Applicability:

- Level 1

Description:

The variables in the `/etc/default/passwd` file indicate various strategies for creating differences required between an old and a new password. As requiring users to select a specific numbers of differences between the characters in the existing password and the new one can strengthen the password by increasing the symbol-set space, to further increase the difficulty of breaking any password by brute-force attacks, these values should be set as appropriate to the needs of the user.

Rationale:

Administrators may wish to add site-specific dictionaries to the `DICTIONLIST` parameter.

Warning: Sites often have differing opinions on the optimal value of the `HISTORY` parameter (how many previous passwords to remember per user in order to prevent re-use). The values specified here are in compliance with NSA/DISA requirements. If this is too restrictive for your site, you may wish to set a HISTORY value of `4` and a MAXREPEATS of `2`. Consult your local security rules for guidance.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^PASSLENGTH=" /etc/default/passwd

PASSLENGTH=14

# grep "^NAMECHECK=" /etc/default/passwd

NAMECHECK=YES

# grep "^HISTORY=" /etc/default/passwd

HISTORY=10

# grep "^MINDIFF=" /etc/default/passwd

MINDIFF=3

# grep "^MINUPPER=" /etc/default/passwd

MINUPPER=1

# grep "^MINLOWER=1" /etc/default/passwd

MINLOWER=1

# grep "^MINSPECIAL=1" /etc/default/passwd

MINSPECIAL=1

# grep "^MINDIGIT=1" /etc/default/passwd

MINDIGIT=1

# grep "^MAXREPEATS=1" /etc/default/passwd

MAXREPEATS=1

# grep "^WHITESPACE=YES" /etc/default/passwd

WHITESPACE=YES

# grep "^DICTIONDBDIR=/var/passwd" /etc/default/passwd

DICTIONDBDIR=/var/passwd

# grep "^DICTIONLIST=/usr/share/lib/dict/words" /etc/default/passwd

DICTIONLIST=/usr/share/lib/dict/words
```

Remediation:

Perform the following to implement the recommended state:

```
# cd /etc/default

# awk '/PASSLENGTH=/ { $1 = "PASSLENGTH=14" };
/NAMECHECK=/ { $1 = "NAMECHECK=YES" };
/HISTORY=/ { $1 = "HISTORY=10" };
/MINDIFF=/ { $1 = "MINDIFF=3" };
/MINUPPER=/ { $1 = "MINUPPER=1" };
/MINLOWER=/ { $1 = "MINLOWER=1" };
/MINSPECIAL=/ { $1 = "MINSPECIAL=1" };
/MINDIGIT=/ { $1 = "MINDIGIT=1" };
/MAXREPEATS=/ { $1 = "MAXREPEATS=1" };
/WHITESPACE=/ { $1 = "WHITESPACE=YES" };
/DICTIONDBDIR=/ { $1 = "DICTIONDBDIR=/var/passwd" };
/DICTIONLIST=/ { $1 = "DICTIONLIST=/usr/share/lib/dict/words" };
{ print }' passwd > passwd.CIS

# mv passwd.CIS passwd
```

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

7.3 Set Default umask for users (Scored)

Profile Applicability:

- Level 1

Description:

The default `umask`(1) determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the `chmod`(1) command. Users who wish to allow their files and directories to be readable by others by default may choose a different default `umask`by inserting the `umask`command into the standard shell configuration files (`.profile`, `.cshrc`, etc.) in their home directories.

Rationale:

Setting a very secure default value for `umask` ensures that users make a conscious choice about their file permissions. A default `umask` setting of `077` causes files and directories created by users to not be readable by any other user on the system. A `umask` of `027` would allow files and directories readable by users in the same Unix group, while a `umask` of `022` would make files readable by every user on the system.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^UMASK=" /etc/default/login

UMASK=027
```

Remediation:

Perform the following to implement the recommended state:

```
# cd /etc/default

# awk '/#UMASK=/ { $1 = "UMASK=027" } { print }' login > login.CIS

# mv login.CIS login
```

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

7.4 Set Default File Creation Mask for FTP Users (Scored)

Profile Applicability:

- Level 1

Description:

If FTP is permitted, set a strong, default file creation mask to apply to files created by the FTP server.

Rationale:

Many users assume that the FTP server will use their system file creation mask; generally it does not. This setting ensures that files transmitted over FTP use a strong file creation mask.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^Umask" /etc/proftpd.conf | awk '{ print $2 }'

027
```

Note: This is only required on systems where the ftp server is installed.

Remediation:

Perform the following to implement the recommended state:

```
# cd /etc

# if [ "`grep '^Umask' proftpd.conf`" ]; then
     awk '/^Umask/ { $2 = "027" } { print }' proftpd.conf > proftpd.conf.CIS
     mv proftpd.conf.CIS proftpd.conf
  else
     echo "Umask 027" >> proftpd.conf
  fi
```

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

7.5 Set "mesg n" as Default for All Users (Scored)

Profile Applicability:

- Level 1

Description:

The "mesg n" command blocks attempts to use the `write` or `talk` commands to contact users at their terminals, but has the side effect of slightly strengthening permissions on the user's tty device.

Rationale:

Since `write` and `talk` are no longer widely used at most sites, the incremental security increase is worth the loss of functionality.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^mesg" /etc/.login

mesg n

# grep "^mesg" /etc/profile

mesg n
```

Remediation:

Perform the following to implement the recommended state:

```
# cd /etc

# for file in profile .login ; do
     if [ "`grep mesg $file`" ]; then
        awk '$1 == "mesg" { $2 = "n" } { print }' $file > $file.CIS
        mv $file.CIS $file
     else
        echo mesg n >> $file
     fi
   done
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

7.6 Lock Inactive User Accounts (Scored)

Profile Applicability:

- Level 1

Description:

Guidelines published by the U.S. Department of Defense specify that user accounts must be locked out after 35 days of inactivity. This number may vary based on the particular site's policy.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Audit:

Perform the following to verify that the result is as recommended:

```
# useradd -D | xargs -n 1 | grep inactive | awk -F= '{ print $2 }'

35

# logins -axo -l "[name]" | awk -F: '{ print $13 }'

35
```

Remediation:

Perform the following to implement the recommended state:

```
# useradd -D -f 35
```

To set this policy on a user account, use the command(s):

```
# usermod -f 35 [name]
```

To set this policy on a role account, use the command(s):

```
# rolemod -f 35 [name]
```

CIS Controls:

Version 7

16.9 Disable Dormant Accounts
Automatically disable dormant accounts after a set period of inactivity.

8 Warning Banners

Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system.

Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. It is important that the organization's legal counsel review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. More information (including citations of relevant case law) can be found at http://www.justice.gov/criminal/cybercrime/

Note: The text provided in the remediation actions for these items is intended as an example ONLY. Please edit to include the specific text for your organization as approved by your legal department.

8.1 Create Warnings for Standard Login Services (Scored)

Profile Applicability:

- Level 1

Description:

The contents of the `/etc/issue` file are displayed prior to the login prompt on the system's console and serial devices and also prior to logins via `telnet` and Secure Shell. The contents of the `/etc/motd` file are generally displayed after all successful logins, regardless from where the user is logging in.

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. As implementing a logon banner to deter inappropriate use and can provide a foundation for legal action against abuse, this warning content should be set as appropriate. Consult with your organization's legal counsel for the appropriate wording as the examples below are for demonstration purposes only.

Audit:

Perform the following to verify that the result is as recommended:

```
# cat /etc/motd

Authorized users only. All activity may be monitored and reported.

# ls -l /etc/motd

-rw-r--r-- 1 root sys 67 Dec 20 18:28 /etc/motd

# cat /etc/issue

Authorized users only. All activity may be monitored and reported.

# ls -l /etc/issue

-rw-r--r-- 1 root root 66 Dec 20 18:27 /etc/issue
```

Remediation:

Perform the following to implement the recommended state:

```
# echo "Authorized users only. All activity may be monitored and reported." >
/etc/motd

# echo "Authorized users only. All activity may be monitored and reported." >
/etc/issue

# chown root:root /etc/issue

# chmod 644 /etc/issue
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

8.2 Enable a Warning Banner for the FTP service (Scored)

Profile Applicability:

- Level 1

Description:

The action for this item sets a warning message for FTP users before they log in.

Rationale:

If FTP is permitted for use in your environment, it is important to ensure that Warning Banners inform users who are attempting to access the system of their legal status regarding using the system. The text below is a generic sample only, so consult with your organization's legal counsel for the appropriate wording.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "DisplayConnect" /etc/proftpd.conf

DisplayConnect /etc/issue
```

Remediation:

Perform the following to implement the recommended state:

```
# echo "DisplayConnect /etc/issue" >> /etc/proftpd.conf

# svcadm restart ftp
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

8.3 Enable a Warning Banner for the SSH Service (Scored)

Profile Applicability:

- Level 1

Description:

The contents of the `Banner` string in the `/etc/ssh/sshd_config` file are sent to the remote user before authentication is allowed, requiring that the user read the legal caution.

Rationale:

Performing these steps will ensure the appropriate legal caution is displayed to any user accessing the system via SSH.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^Banner" /etc/ssh/sshd_config

Banner /etc/issue
```

Remediation:

Perform the following to implement the recommended state:

```
# awk '/^#Banner/ { $1 = "Banner" } { print }' /etc/ssh/sshd_config >
/etc/ssh/sshd_config.CIS

# mv /etc/ssh/sshd_config.CIS /etc/ssh/sshd_config

# svcadm restart svc:/network/ssh
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

8.4 Enable a Warning Banner for the GNOME Service (Scored)

Profile Applicability:

- Level 1

Description:

The GNOME Display Manager is used for login session management. See the manual page `gdm`(1) for more information on configuration of the settings, which can be user or group specific.

Rationale:

The remediation action for this item sets a pre-login warning message for GDM users. Additional methods can be employed to display a similar message to a user post-authentication. For more information, see the Oracle Solaris 11 Security Guidelines document.

Audit:

If GDM is installed perform the following to verify that the result is as recommended:

```
# cd /etc/gdm/Init

# grep "Security Message" Default

--title="Security Message" --filename=/etc/issue
```

Remediation:

Perform the following to implement the recommended state:
Edit the `/etc/gdm/Init/Default` file to add the following content before the last line of the file.

```
/usr/bin/zenity --text-info --width=800 --height=300 --title="Security
Message" --filename=/etc/issue
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

8.5 Check that the Banner Setting for telnet is Null (Scored)

Profile Applicability:

- Level 1

Description:

The `BANNER` variable in the file `/etc/default/telnetd` can be used to display text before the telnet login prompt. Traditionally, it has been used to display the OS level of the target system.

Rationale:

The warning banner provides information that can be used in reconnaissance for an attack. By default, this file is distributed with the `BANNER` variable set to null. It is not necessary to create a separate warning banner for `telnet` if a warning is set in the `/etc/issue` file. As `telnet` is an insecure protocol, it should be **disabled** and all remote administrative/user connections take place by Secure Shell.

Audit:

Perform the following to verify that the result is as recommended:

```
# grep "^BANNER" /etc/default/telnetd

BANNER=
```

Remediation:

Perform the following to implement the recommended state:

```
# cd /etc/default

# awk '/^BANNER=/ { $1 = "BANNER=" }; { print }' telnetd > telnetd.CIS

# mv telnetd.CIS telnetd
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

9 System Maintenance

No matter how securely a system has been installed and hardened, administrator and user activity over time can introduce security exposures. This section describes tasks to be performed on a regular, ongoing basis—perhaps in an automated fashion via the `cron` utility. The automated host-based scanning tools provided from the Center for Internet Security can be used for this purposed and are available from http://www.CISecurity.org/.

Note that, unlike other sections, the items in this section specify an Audit action followed by a Remediation action, since it is necessary to determine what the current setting is before determining remediation measures, which will vary depending on the site's policy.

9.1 Check for Remote Consoles (Scored)

Profile Applicability:

- Level 1

Description:

The `consadm` command can be used to select or display alternate console devices.

Rationale:

Since the system console has special properties to handle emergency situations, it is important to ensure that the console is in a physically secure location and that unauthorized consoles have not been defined. The "`consadm -p`" command displays any alternate consoles that have been defined as auxiliary across reboots. If no remote consoles have been defined, there will be no output from this command.

Audit:

Perform the following to verify that the result is as recommended:

```
# /usr/sbin/consadm -p
```

(No output should be returned.)
Note: This only applies to global zones.

Remediation:

Perform the following to implement the recommended state:

```
# /usr/sbin/consadm [-d device...]
```

CIS Controls:

Version 7

1.6 Address Unauthorized Assets

Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.

9.2 Check for Duplicate User Names (Scored)

Profile Applicability:

- Level 1

Description:

Although the `useradd` program will not let you create a duplicate user name, it is possible for an administrator to manually modify `passwd`(4) and change the user name.

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in `passwd`(4). For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a potential security problem.

Audit:

Perform the following to verify that the result is as recommended:

```
# getent passwd | cut -f1 -d":" | sort -n | uniq -c | while read x ; do
       [ -z "${x}" ] && break
       set - $x
       if [ $1 -gt 1 ]; then
            gids=`getent passwd | nawk -F: '($1 == n) { print $3 }' n=$2 |
xargs`
            echo "Duplicate User Name ($2): ${gids}"
       fi
  done
```

(No output should be returned.)

Remediation:

Correct or justify any items discovered in the Audit step. Determine if there are any duplicate user names, and work with their respective owners to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

16.7 Establish Process for Revoking Access
Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

9.3 Check That Defined Home Directories Exist (Scored)

Profile Applicability:

- Level 1

Description:

Users can be defined to have a home directory in `passwd`(4), even if the directory does not actually exist.

Rationale:

If the user's home directory does not exist, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Audit:

Perform the following to verify that the result is as recommended:

```
# logins -xo | while read line; do
    user=`echo ${line} | awk -F: '{ print $1 }'`
    home=`echo ${line} | awk -F: '{ print $6 }'`
      if [ ! -d "${home}" ]; then
       echo ${user}
      fi
  done
```

Starting in Solaris 11.4, uucp is no longer installed by default. With the `uucp` package installed, only `uucp` and `nuucp` should generate errors (as their home directories do not exist). Other entries should be verified for correctness.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if there exists any users whose home directories do not exist, and work with those users to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.4 Verify System Account Default Passwords (Scored)

Profile Applicability:

- Level 1

Description:

There are a number of accounts provided with the Solaris OS that are used to manage applications and are not intended to provide an interactive shell. These accounts are delivered either in a locked or non-login state. Oracle does not support nor recommend changing the passwords associated with these accounts.

Rationale:

System accounts, such as `bin`, `lpd`, and `sys` have special purposes and privileges. By default, these accounts are configured as either locked or non-login. This status should be verified to ensure that these accounts have not accidentally or intentionally been enabled.

Audit:

Perform the following to determine if the system is configured as recommended:

```
# for user in $(logins -s | awk '{ print $1 }'); do
     if [ "${user}" != "root" ]; then
        stat=`passwd -s ${user} | awk '{ print $2 }'`
        if [ "${stat}" != "LK" ] && [ "${stat}" != "NL" ]; then
           echo "Account ${user} is not locked or non-login."
        fi
     fi
  done
```

(No output should be returned.)

Remediation:

To lock a single account, use the command:

```
# passwd -d [username]

# passwd -l <em>[username]
```

To configure a single account to be non-login, use the command:

```
# passwd -d [username]

# passwd -N <em>[username]
```

CIS Controls:

Version 7

16.8 Disable Any Unassociated Accounts

Disable any account that cannot be associated with a business process or business owner.

9.5 Verify System File Permissions (Not Scored)

Profile Applicability:

- Level 1

Description:

The `pkg verify` and command checks the accuracy of installed directory structures and files.

Rationale:

It is important to ensure that system files and directories are maintained with the permissions they were intended to have from the OS vendor (Oracle).

Audit:

Perform the following to verify that the result is as recommended:

```
# pkg verify
```

Errors may be a simple reflection of changes made earlier in this benchmark, such as alteration of the ownership of the `cron` process, so this result indicates that pkg verify is doing its job and detecting file changes.

Remediation:

Correct or justify any items discovered in the Audit step. Perform the following to set correct any identified package errors:

```
# pkg fix
```

Exercise caution in running this command as it may reverse modifications implemented previously including some of those recommended by this document. Rather than use this command broadly, it is recommended that it be used more tactically to correct specific package problems when possible.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.6 Ensure Password Fields are Not Empty (Scored)

Profile Applicability:

- Level 1

Description:

An account with an empty password field means that anybody may log in as that user without providing a password at all (assuming that the value `PASSREQ=NO` is set in `/etc/default/login`).

Rationale:

All accounts must have passwords, be configured as "Non-login," or be locked.

Audit:

Perform the following to verify that the result is as recommended:

```
# logins -p
```

No output should be returned.

Remediation:

Use the `passwd -l` command to lock accounts that are not permitted to execute commands . Use the `passwd -N` command to set accounts to be non-login.

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

9.7 Verify No UID 0 Accounts Exist Other than root (Scored)

Profile Applicability:

- Level 1

Description:

Any account with UID 0 has superuser rights on the system.

Rationale:

This access must be limited to only the default `root` role and be made accessible from the system console only. Administrative access granted to an unprivileged account should use an approved mechanism such as RBAC.

Audit:

Perform the following to verify that the result is as recommended:

```
# logins -o | awk -F: '($2 == 0) { print $1 }'

root
```

Remediation:

Disable or delete any other `0` UID entries that are displayed; there should be only one `root` account. Finer granularity access control for administrative access can be obtained by using the Solaris Role-Based Access Control (RBAC) mechanism. RBAC configurations should be monitored via `user_attr`(4) to make sure that privileges are managed appropriately.

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

9.8 Ensure root PATH Integrity (Scored)

Profile Applicability:

- Level 1

Description:

The `root` user can execute any command on the system and could be tricked into executing programs if the PATH is not set correctly.

Rationale:

Including the current working directory (.) or any other writable directory in `root`'s executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as `root` to execute a malcode, such as a Trojan horse program.

Audit:

Perform the following to verify that the result is as recommended:

```
# if [ "`echo $PATH | grep :: `" != "" ]; then
    echo "Empty Directory in PATH (::)"
  fi
```

No output should be returned

```
# if [ "`echo $PATH | grep :$`"  != "" ]; then
     echo "Trailing : in PATH"
  fi
```

No output should be returned

```
#!/usr/bin/bash

p=`echo $PATH | sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
   if [ "$1" = "." ]; then
      echo "PATH contains ."
      shift
      continue
   fi
   if [ -d $1 ]; then
      dirperm=`ls -ld $1 | cut -f1 -d" "`
      if [ `echo $dirperm | cut -c6 ` != "-" ]; then
         echo "Group Write permission set on directory $1"
      fi
      if [ `echo $dirperm | cut -c9 ` != "-" ]; then
         echo "Other Write permission set on directory $1"
      fi
   fi
   shift
done
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step.

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

9.9 Check Permissions on User Home Directories (Scored)

Profile Applicability:

- Level 1

Description:

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale:

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Perform the following to verify that the result is as recommended:

```
# for dir in `logins -ox | awk -F: '($8 == "PS") { print $6 }'`; do
     find ${dir} -type d -prune \( -perm -g+w -o -perm -o+r -o -perm -o+w -o
-perm -o+x \) -ls
  done
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if any user directory permissions are world-readable, writable, or executable, and work with those users to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.10 Check Permissions on User "." (Hidden) Files (Scored)

Profile Applicability:

- Level 1

Description:

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

Rationale:

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Perform the following to verify that the result is as recommended:

```
# for dir in `logins -ox | awk -F: '($8 == "PS") { print $6 }'`; do
    find ${dir}/.[A-Za-z0-9]* \! -type l \ \( -perm -20 -o -perm -02 \) -ls
  done
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if any user hidden files are world-readable or writable, and work with those users to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.11 Check Permissions on User .netrc Files (Scored)

Profile Applicability:

- Level 1

Description:

While the system administrator can establish secure permissions for users' `.netrc` files, the users can easily override these.

Rationale:

`.netrc` files may contain unencrypted passwords that can be used to attack other systems.

Audit:

Perform the following to verify that the result is as recommended:

```
# for dir in `logins -ox | awk -F: '($8 == "PS") { print $6 }'`; do
     find ${dir}/.netrc -type f \( -perm -g+r -o -perm -g+w -o -perm -g+x -o
-perm -o+r -o -perm -o+w -o -perm -o+x \) -ls 2>/dev/null
  done
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if any user `.netrc` files are group- or world-readable or writable, and work with those users to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.12 Check for Presence of User .rhosts Files (Scored)

Profile Applicability:

- Level 1

Description:

While no `.rhosts` files are shipped with Solaris, users can easily create them.

Rationale:

This action is only meaningful if `.rhosts` support is permitted in the PAM configuration. Even though the `.rhosts` files are ineffective if support is disabled in the PAM configuration, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

Audit:

Perform the following to verify that the result is as recommended:

```
# for dir in `logins -ox | awk -F: '($8 == "PS") { print $6 }'`; do
     find ${dir}/.rhosts -type f -ls 2>/dev/null
  done
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if any user `.rhosts` files are present in user directories and work with those users to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

9.13 Check Groups in passwd (Scored)

Profile Applicability:

- Level 1

Description:

Over time, system administration errors and changes can lead to groups being defined in `passwd` but not in `group`.

Rationale:

Groups defined in `passwd` but not in `group` file pose a threat to system security since group permissions are not properly managed.

Audit:

Perform the following to verify that the result is as recommended:

```
# logins -xo | awk -F: '($3 == "") { print $1 }'
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if any groups are in `passwd` but not in `group`, and work with those users or group owners to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

16.7 Establish Process for Revoking Access
Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

9.14 Check That Users Are Assigned Home Directories (Scored)

Profile Applicability:

- Level 1

Description:

`passwd` defines a home directory that each user is placed in upon login. If there is no defined home directory, a user will be placed in `/` and will not be able to write any files or have local environment variables set.

Rationale:

All users must be assigned a home directory in `passwd`.

Audit:

This following check is to make sure each user has a home directory defined in `passwd`.

```
# logins -xo | while read line; do
     user=`echo ${line} | awk -F: '{ print $1 }'`
     home=`echo ${line} | awk -F: '{ print $6 }'`
     if [ -z "${home}" ]; then
        echo ${user}
     fi
  done
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if there exists any users who are in `passwd` but do not have a home directory, and work with those users to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.15 Check User Home Directory Ownership (Scored)

Profile Applicability:

- Level 1

Description:

The user home directory is space defined for the particular user to set local environment variables and to store personal files.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Audit:

Perform the following to verify that the result is as recommended:

```
# logins -xo | awk -F: '($8 == "PS") { print }' | while read line; do
     user=`echo ${line} | awk -F: '{ print $1 }'`
     home=`echo ${line} | awk -F: '{ print $6 }'`
     find ${home} -type d -prune \! -user ${user} -ls
   done
```

Only uucp and nuucp should generate errors (as their home directories do not exist). Other entries should be verified for correctness.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if there exists any users whose home directory is not properly owned, and work with those users to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.16 Check for Duplicate UIDs (Scored)

Profile Applicability:

- Level 1

Description:

Although the `useradd` program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually modify `passwd` and change the UID field.

Rationale:

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Audit:

Perform the following to verify that the result is as recommended:

```
# logins -d
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if there exists any users who share a common `UID`, and work with those users to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

9.17 Check for Duplicate GIDs (Scored)

Profile Applicability:

- Level 1

Description:

Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually modify `group` and change the GID field.

Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Audit:

Perform the following to verify that the result is as recommended:

```
# getent group | cut -f3 -d":" | sort -n | uniq -c | while read x ; do
    [ -z "${x}" ] && break
    set - $x
    if [ $1 -gt 1 ]; then
       grps=`getent group | nawk -F: '($3 == n) { print $1 }' n=$2 | xargs`
       echo "Duplicate GID ($2): ${grps}"
    fi
  done
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if there exists any duplicate group identifiers, and work with each respective group owner to remediate this issue and ensure that the group ownership of their files are set to an appropriate value.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.18 Check for Duplicate Group Names (Scored)

Profile Applicability:

- Level 1

Description:

Although the `groupadd` program will not let you create a duplicate group name, it is possible for an administrator to manually modify `group` and change the group name.

Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in `group`. Effectively, the GID is shared, which is a security risk.

Audit:

Perform the following to verify that the result is as recommended:

```
# getent group | cut -f1 -d":" | sort -n | uniq -c | while read x ; do
     [ -z "${x}" ] && break
     set - $x
     if [ $1 -gt 1 ]; then
        gids=`getent group |\
        nawk -F: '($1 == n) { print $3 }' n=$2 | xargs`
        echo "Duplicate Group Name ($2): ${gids}"
     fi
  done
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if there are any duplicate group names, and work with their respective owners to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.19 Check for Presence of User .netrc Files (Scored)

Profile Applicability:

- Level 1

Description:

The `.netrc` file contains data for logging into a remote host for file transfers via FTP.

Rationale:

The `.netrc` file presents a significant security risk since it stores passwords in unencrypted form.

Audit:

Perform the following to verify that the result is as recommended:

```
# for dir in `logins -ox | awk -F: '($8 == "PS") { print $6 }'`; do
    ls -l ${dir}/.netrc 2>/dev/null
  done
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if any `.netrc` files exist, and work with the owner to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

9.20 Check for Presence of User .forward Files (Scored)

Profile Applicability:

- Level 1

Description:

The `.forward` file specifies an email address to which a user's mail is forwarded.

Rationale:

Use of the `.forward` file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The `.forward` file also poses a secondary risk as it can be used to execute commands that may perform unintended actions.

Audit:

Perform the following to verify that the result is as recommended:

```
# for dir in `logins -ox | awk -F: '($8 == "PS") { print $6 }'`; do
    ls -l ${dir}/.forward 2>/dev/null
  done
```

No output should be returned.

Remediation:

Correct or justify any items discovered in the Audit step. Determine if any `.forward` files exist, and work with the owner to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

9.21 Find World Writable Files (Not Scored)

Profile Applicability:

- Level 1

Description:

Unix-based systems support variable settings to control access to files. World-writable files are the least secure. See the `chmod` man page for more information.

Rationale:

Data in world-writable files can be read, modified, and potentially compromised by any user on the system. World-writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

Audit:

Perform the following to verify that the result is as recommended:

```
# find / \( -fstype nfs -o -fstype cachefs -o -fstype autofs -o -fstype ctfs
-o -fstype mntfs -o -fstype objfs -o -fstype proc \) -prune -o -type f -perm
-0002 -print
```

No output should be returned.
Note: The script above does a file traversal of all files under the "/" directory, including NFS attached file systems, so running this search command may take quite some time.

Remediation:

Correct or justify any items discovered in the Audit step. Determine the existence of any "write access" given for the "other" category (`chmod o-w <filename>`), and work with the owner to determine the best course of action in accordance with site policy.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.22 Find SUID/SGID System Executables (Not Scored)

Profile Applicability:

- Level 1

Description:

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID/SGID program is to enable users to perform functions (such as changing their password), which requires root privileges.

Rationale:

There are valid reasons for SUID/SGID programs, but it is important to identify and review such programs to ensure they are legitimate.

Audit:

Perform the following to verify that the result is as recommended:

```
# find  / \( -fstype nfs -o -fstype cachefs -o -fstype autofs -o -fstype ctfs
-o -fstype mntfs -o -fstype objfs -o -fstype proc \) -prune -o -type f \( -
perm -4000 -o -perm -2000 \) -print
```

No output should be returned.
Note: The script above does a transversal of all files under the "/" directory, including NFS attached file systems, so running this search command may take quite some time.

Remediation:

Correct or justify any items discovered in the Audit step. Determine the existence of any set-UID programs that do not belong on the system, and work with the owner (or system administrator) to determine the best course of action in accordance with site policy. Digital signatures on the Solaris Set-UID binaries can be verified with the `elfsign` utility, such as this example:

```
# elfsign verify -e /usr/bin/su

elfsign: verification of /usr/bin/su passed.
```

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

9.23 Find Un-owned Files and Directories (Scored)

Profile Applicability:

- Level 1

Description:

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

Perform the following to verify that the result is as recommended:

```
# find / \( -fstype nfs -o -fstype cachefs -o -fstype autofs -o -fstype ctfs
-o -fstype mntfs -o -fstype objfs -o -fstype proc \) -prune -o \( -nouser -o
-nogroup \) -ls
```

No output should be returned.
Note: The script above does a transversal of all files under the "`/`" directory, including NFS attached file systems, so running this search command may take quite some time. Additionally false positives may be returned in `/zones/` when run in the global zone.

Remediation:

Correct or justify any items discovered in the Audit step. Determine the existence of any files that are not attributed to current users or groups on the system, and determine the best course of action in accordance with site policy. Note that the Solaris OS is shipped with all files appropriately owned.

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

9.24 Find Files and Directories with Extended Attributes (Scored)

Profile Applicability:

- Level 1

Description:

Extended attributes are implemented as files in a "shadow" file system that is not generally visible via normal administration commands without special arguments.

Rationale:

Attackers or malicious users could "hide" information, exploits, etc. in extended attribute areas. Since extended attributes are rarely used, it is important to find files with extended attributes set.

Audit:

Perform the following to verify that the result is as recommended:

```
# find / \( -fstype nfs -o -fstype cachefs -o -fstype autofs -o -fstype ctfs\
-o -fstype mntfs -o -fstype objfs -o -fstype proc \) -prune -o -xattr -ls
```

No output should be returned.
Note: The script above does a transversal of all files under the "/" directory, including NFS attached file systems, so running this search command may take quite some time.

Remediation:

Correct or justify any items discovered in the Audit step. Determine the existence of any files having extended file attributes, and determine the best course of action in accordance with site policy. Note that the Solaris OS does not ship with files that have extended attributes.

CIS Controls:

Version 7

2.6 Address unapproved software
Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

10 Appendix A: Additional Security Notes

The items in this section are security configuration settings that have been suggested by several other resources and system hardening tools. However, compared to the other settings in this document, the settings presented here provide relatively little incremental security benefit. Nevertheless, none of these settings should have a significant impact on the functionality of the system, and some sites may feel that the slight security enhancement of these settings outweighs the (sometimes minimal) administrative cost of performing them.

None of these settings will be checked by the automated scoring tool provided with the benchmark document. They are purely optional and may be applied or not at the discretion of local site administrators.

10.1 SN.1 Restrict access to suspend feature (Not Scored)

Profile Applicability:

- Level 2

Description:

Solaris 11 does not enable the suspend capability by default and now uses the `poweradm` command to suspend the system.

Rationale:

Bear in mind that users with physical access to a system can simply remove power from the machine if they are truly motivated to take the system off-line, and granting the capability to use poweradm may be a more graceful way of allowing desktop users to shut down their own machines.

Audit:

Perform the following to verify that the result is as recommended:

```
# poweradm list | grep suspend

suspend/suspend-enable   current=false, smf=false
```

Remediation:

Perform the following to implement the recommended state:

```
# poweradm set suspend-enable=false

# poweradm update
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

10.2 SN.2 Remove Support for Internet Services (inetd) (Not Scored)

Profile Applicability:

- Level 2

Description:

If the actions in this section result in disabling all `inetd`-based services, then there is no point in running `inetd` at boot time.

Rationale:

If `inetd`-based services are ever re-enabled in the future it will be necessary to re-enable the `inetd` daemon as well ("`svcadm enable svc:/network/inetd:default`").

Audit:

Perform the following to verify that the result is as recommended:

```
# svcs -Ho state svc:/network/inetd

disabled
```

Remediation:

Perform the following to implement the recommended state:

```
# svcadm disable svc:/network/inetd
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Software Installation and Updates**		
1.1	Use the Latest Package Updates (Not Scored)	☐	☐
2	**Disable Unnecessary Services**		
2.1	Configure TCP Wrappers (Not Scored)	☐	☐
2.2	Disable Local-only Graphical Login Environment (Scored)	☐	☐
2.3	Configure sendmail Service for Local-Only Mode (Scored)	☐	☐
2.4	Disable RPC Encryption Key (Scored)	☐	☐
2.5	Disable Generic Security Services (GSS) (Scored)	☐	☐
2.6	Disable Apache Service (Scored)	☐	☐
2.7	Disable Kerberos TGT Expiration Warning (Scored)	☐	☐
2.8	Disable NIS Client Services (Scored)	☐	☐
2.9	Disable NIS Server Services (Scored)	☐	☐
2.10	Disable Removable Volume Manager (Scored)	☐	☐
2.11	Disable automount Service (Scored)	☐	☐
2.12	Disable Telnet Service (Scored)	☐	☐
3	**Kernel Tuning**		
3.1	Disable Response to Broadcast ICMPv4 Echo Request (Scored)	☐	☐
3.2	Disable Response to ICMP Broadcast Netmask Requests (Scored)	☐	☐
3.3	Enable Strong TCP Sequence Number Generation (Scored)	☐	☐
3.4	Disable Response to ICMP Broadcast Timestamp Requests (Scored)	☐	☐
3.5	Disable Source Packet Forwarding (Scored)	☐	☐
3.6	Disable Directed Broadcast Packet Forwarding (Scored)	☐	☐
3.7	Enable Stack Protection (Scored)	☐	☐
3.8	Restrict Core Dumps to Protected Directory (Scored)	☐	☐
3.9	Disable Response to ICMP Timestamp Requests (Scored)	☐	☐
3.10	Disable Response to Multicast Echo Request (Scored)	☐	☐
3.11	Ignore ICMP Redirect Messages (Scored)	☐	☐
3.12	Set Strict Multihoming (Scored)	☐	☐
3.13	Disable ICMP Redirect Messages (Scored)	☐	☐
3.14	Disable TCP Reverse IP Source Routing (Scored)	☐	☐
3.15	Set Maximum Number of Half-open TCP Connections (Scored)	☐	☐
3.16	Set Maximum Number of Incoming Connections (Scored)	☐	☐
3.17	Disable Network Routing (Scored)	☐	☐

4	**Auditing and Logging**		
4.1	Create CIS Audit Class (Scored)	☐	☐
4.2	Enable Auditing of Incoming Network Connections (Scored)	☐	☐
4.3	Enable Auditing of File Metadata Modification Events (Scored)	☐	☐
4.4	Enable Auditing of Process and Privilege Events (Scored)	☐	☐
4.5	Configure Solaris Auditing (Scored)	☐	☐
5	**File/Directory Permissions/Access**		
5.1	Set Sticky Bit on World Writable Directories (Not Scored)	☐	☐
6	**System Access, Authentication, and Authorization**		
6.1	Disable login: Services on Serial Ports (Scored)	☐	☐
6.2	Set EEPROM Security Mode and Log Failed Access (SPARC) (Not Scored)	☐	☐
6.3	Restrict at/cron to Authorized Users (Scored)	☐	☐
6.4	Set Default Screen Lock for GNOME Users (Scored)	☐	☐
6.5	Remove Autologin Capabilities from the GNOME desktop (Scored)	☐	☐
6.6	Set Delay between Failed Login Attempts to 4 (Scored)	☐	☐
6.7	Disable Rhost-based Authentication for SSH (Scored)	☐	☐
6.8	Restrict FTP Use (Scored)	☐	☐
6.9	Disable root login for SSH (Scored)	☐	☐
6.10	Disable Host-based Authentication for Login-based Services (Scored)	☐	☐
6.11	Blocking Authentication Using Empty/Null Passwords for SSH (Scored)	☐	☐
6.12	Limit Consecutive Login Attempts for SSH (Scored)	☐	☐
6.13	Disable X11 Forwarding for SSH (Scored)	☐	☐
6.14	Disable "nobody" Access for RPC Encryption Key Storage Service (Scored)	☐	☐
6.15	Secure the GRUB Menu (Intel) (Scored)	☐	☐
6.16	Restrict root Login to System Console (Scored)	☐	☐
6.17	Set Retry Limit for Account Lockout (Scored)	☐	☐
7	**User Accounts and Environment**		
7.1	Set Password Expiration Parameters on Active Accounts (Scored)	☐	☐
7.2	Set Strong Password Creation Policies (Scored)	☐	☐
7.3	Set Default umask for users (Scored)	☐	☐
7.4	Set Default File Creation Mask for FTP Users (Scored)	☐	☐
7.5	Set "mesg n" as Default for All Users (Scored)	☐	☐
7.6	Lock Inactive User Accounts (Scored)	☐	☐
8	**Warning Banners**		
8.1	Create Warnings for Standard Login Services (Scored)	☐	☐
8.2	Enable a Warning Banner for the FTP service (Scored)	☐	☐

8.3	Enable a Warning Banner for the SSH Service (Scored)	☐	☐
8.4	Enable a Warning Banner for the GNOME Service (Scored)	☐	☐
8.5	Check that the Banner Setting for telnet is Null (Scored)	☐	☐
9	**System Maintenance**		
9.1	Check for Remote Consoles (Scored)	☐	☐
9.2	Check for Duplicate User Names (Scored)	☐	☐
9.3	Check That Defined Home Directories Exist (Scored)	☐	☐
9.4	Verify System Account Default Passwords (Scored)	☐	☐
9.5	Verify System File Permissions (Not Scored)	☐	☐
9.6	Ensure Password Fields are Not Empty (Scored)	☐	☐
9.7	Verify No UID 0 Accounts Exist Other than root (Scored)	☐	☐
9.8	Ensure root PATH Integrity (Scored)	☐	☐
9.9	Check Permissions on User Home Directories (Scored)	☐	☐
9.10	Check Permissions on User "." (Hidden) Files (Scored)	☐	☐
9.11	Check Permissions on User .netrc Files (Scored)	☐	☐
9.12	Check for Presence of User .rhosts Files (Scored)	☐	☐
9.13	Check Groups in passwd (Scored)	☐	☐
9.14	Check That Users Are Assigned Home Directories (Scored)	☐	☐
9.15	Check User Home Directory Ownership (Scored)	☐	☐
9.16	Check for Duplicate UIDs (Scored)	☐	☐
9.17	Check for Duplicate GIDs (Scored)	☐	☐
9.18	Check for Duplicate Group Names (Scored)	☐	☐
9.19	Check for Presence of User .netrc Files (Scored)	☐	☐
9.20	Check for Presence of User .forward Files (Scored)	☐	☐
9.21	Find World Writable Files (Not Scored)	☐	☐
9.22	Find SUID/SGID System Executables (Not Scored)	☐	☐
9.23	Find Un-owned Files and Directories (Scored)	☐	☐
9.24	Find Files and Directories with Extended Attributes (Scored)	☐	☐
10	**Appendix A: Additional Security Notes**		
10.1	SN.1 Restrict access to suspend feature (Not Scored)	☐	☐
10.2	SN.2 Remove Support for Internet Services (inetd) (Not Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Jan 2, 2020	1.0.0	Published