Security Benchmarks™
A DIVISION OF CENTER FOR INTERNET SECURITY

CIS IBM AIX 7.1 Benchmark

v1.1.0 - 09-20-2013

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document, Security Configuration Benchmark for AIX 7.1, provides prescriptive guidance for establishing a secure configuration posture for AIX version 7.1 running on the Power Systems platform. This guide was tested against AIX 7.1 installed from IBM base installation media. 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 AIX 7.1 on the Power Systems platform.

A working knowledge of `vi` is assumed in order to implement some of the configuration changes.

Consensus Guidance

This benchmark was created using a consensus review process comprised 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://community.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**

  Level-I Benchmark recommendations are intended to:

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

- **Level 2**

  Level-II Benchmark recommendations 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:

Author
Paul Sharpe-Deacon

Contributors and Reviewers

Shailesh Athalye, *Symantec Inc.*
Christiane Cuculo, *CPqD*
Blake Frantz, *Center for Internet Security*
Gary Harwood
Huibert Kivits
Boris Kleiman, *Lightening International*
Nikhil Mittal
Steve Parham, *IBM*
Ely Pinto
Jeff Saxon, *IBM*

Recommendations

1 Introduction

This benchmark provides security configuration guidance for use during the configuration of the AIX 7.1 Operating System. The scope of the guide is applicable to AIX 7.1 TL-0 SP1 and above. The recommendations in this guide have been explicitly tested on AIX 7.1 TL-0 SP1 and AIX 7.1 TL-01.

1.1 Approach

The suggested approach in terms of implementing this guide would be to install a vanilla AIX image, via NIM or the AIX product DVD's, followed by the recommendations detailed in this guide and any other corporate standardization i.e. software installation, filesystem and user creation. Once completed, a mksysb backup of the system could then be taken and this image could be deployed via NIM for any subsequent operating system builds. This would provide a standard build mechanism, ensuring 100% compliance to all company standards and the best practice recommendations detailed in this benchmark.

Within the AIX Base Operating System Installation Menus it is recommended that the following options are selected:

- JFS2 filesystems
- Enable System Backups to install any system = yes *

* This is to ensure that all device drivers are installed into the operating system image for deploying to different server hardware configurations.

Also consider selecting the following option (dependant on environmental requirements as this may be too restrictive):

- Secure By Default = yes *

* This option performs a minimal software installation, and removes all clear password access such as telnet and rlogin. Secure by Default (SbD) also applies the AIX Security Expert high-security settings. Once installed the expansion pack cd is prompted for as SSH and SSL are installed for secure remote system accessibility. If the SbD installation option is selected through NIM, the system administrator should ensure that the relevant NIM lpp_source has the openssh and openssl images in place.

1.2 Maintenance Cadence

Before entering into the recommendation section of this paper it is important to put into context the relevance of an AIX software maintenance strategy. It is imperative that regular Technology Level (TL) and Service Pack (SP) updates are regularly applied, to ensure that all known security vulnerabilities are addressed and to remain within a supported TL stream.

The current IBM software maintenance strategy revolves around the release of Technology Levels and Service Packs. Technology Levels are released twice per year, one in the spring and the other in fall. They introduce support for new hardware, new functionality, and new features and contain cumulative fixes since the release of the previous TL. The fix support window for a given TL is two years from its release date.

Service Packs are released throughout the lifecycle of the TL and address security vulnerabilities and other critical fixes. They are typically released every 12 weeks; obviously this timeframe is dependent on the number and criticality of the issues found.

It is recommended that full TL's or SP's are applied rather than individual fixes, due to the far more rigorous certification and testing process. The large and complex matrix of possible fix combinations are not subjected to the same degree of testing and therefore installing individual fixes is not recommended.

A security fix will be initially released as an interim fix, which is installed and maintained via the `emgr` framework. It is recommended that, unless it is an extremely critical security issue, to wait and apply the fix as part of a full SP release to ensure maximum system stability.

1.2.1 Summary

The recommended maintenance strategy is as follows:-

- Stay current and refresh the TL of each system at least once a year - For maximum system stability wait until SP3 is released on the newer TL and then migrate
- Review the Service Packs for any security or critical fixes - apply these regularly throughout the life cycle of a TL
- Do not apply interim fixes or individual fixes unless there is an urgent requirement to do so. Instead apply full TL's and SP's for maximum stability
- There should be a monthly review of the security advisory bulletins to remain apprised of all known security issues. These can currently be viewed at the following URL:

http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd

- The security fixes published in the vulnerability advisories are posted here for download:

  ftp://aix.software.ibm.com/aix/efixes/security

- When any new AIX operating system images are deployed, review the latest available TL and SP releases and update where required. The information regarding the latest fixes can be gleaned from the IBM Fix Central website:

  http://www-933.ibm.com/support/fixcentral/

- Further details on the IBM recommended maintenance strategies can be found in the "IBM AIX Operating System Service Strategy Details and Best Practices" guide:

  http://www14.software.ibm.com/webapp/set2/sas/f/best/home.html

2 AIX Security Expert Introduction

This section will focus on the AIX Security Expert framework. The tool has been introduced to standardize and simplify the security hardening process in AIX, with over 300 settings and commands within its scope. It can be used to replace in-house security scripts and procedures.

2.1 Security Levels

There are three standard security levels, other than default, and the ability to create a customized hybrid policy.

2.1.1 Low Level Security

This policy implements common non-disruptive security enhancements.

Typically this is suited to servers residing in an internal and secure local network environment. It provides a basic security lockdown, from a minimal default level.

2.1.2 Medium Level Security

This policy implements more advanced hardening parameters than the Low Level. These include: port scan protection and an enhanced password management policy. This security level does allow clear text password protocol access, e.g. ftp, rlogin, and telnet.

Typically, this is suited to servers residing in a corporate network protected by a firewall.

2.1.3 High Level Security

This policy implements the highest possible security hardening standards. These include: port scan protection and no access for any clear text password protocols. It assumes that the local network is not trusted and is potentially unsafe.

Typically, this is suited to servers residing in an unsafe network. For example, those which are internet facing.

Within modern IT infrastructure, internal firewalls are typically implemented to separate the internal network from any corporate or internet environments and external firewalls to further protect these environments from the outside world. These firewall devices are typically only configured to allow access to the systems on the required core application or database ports. Therefore, port shunning and scan protection are typically something implemented by a firewall, rather than at the operating system level.

2.1.4 Custom Level Security

The approach of this benchmark is to implement a hybrid policy, which contains a combination of recommended settings from both the Medium and High Level default policies. A customized XML file provides the ultimate flexibility in terms of being able to choose whether or not to implement every recommended AIX Security Expert controlled setting in this benchmark e.g. whether clear text password protocols are allowed. This policy can be easily modified depending on the environmental requirements. A simple edit of the customized XML file, prior to it being implemented, is all that is required. This flexibility is not present within the default Low, Medium and High Level policies which provide a pre-defined rigid level of security hardening standards.

2.1.5 Implementing the Custom Level Policy

This section details how to automatically implement all of the AIX Security Expert managed settings from this benchmark. The use of the supplied AIX Security Expert Customized XML file is purely optional, as there is remediation guidance provided with each recommendation in this benchmark.

The absolute path tar file can be extracted via the following command:

```
tar -xvf <PATH to tar file>/CIS_IBM_AIX_7.1_Benchmark_v1.0.0_AIXPERT_7.1.tar
```

This will place the customized XML file into its default location:

```
/etc/security/aixpert/custom/custom_7.1.xml
```

Prior to implementing the AIX Security Expert customized settings, please review the benchmark recommendations in the next section. If there are any settings that need to be changed from a recommended value, based on environmental requirements, edit the XML file using the vi command.

As much of the guide as possible has been automated within the AIX Security Expert customized XML file. This includes a number of recommendations normally outside the remit of the tool. In these instances the execmds functionality has been used to execute the appropriate commands and implement the recommendations.

Once the recommendations have been reviewed, implementation of the customized XML file should be performed in the following way:

```
aixpert -f /etc/security/aixpert/custom/custom_7.1.xml
```

Once the XML has been successfully implemented, the applied settings are placed in the following file:

```
cat /etc/security/aixpert/core/appliedaixpert.xml
```

The values set by the customized XML file can be validated via:

```
aixpert -c
```

This compares the settings, defined in the appliedaixpert.xml file, to those currently set on the system.
If there is deviation from these standards i.e. a setting has been changed, it will be reported in the following log file:

```
cat /etc/security/aixpert/check_report.txt
```

Any deviations can be corrected manually, or the AIX Security Expert Customized XML file can be re-applied.

During the customized XML implementation, the following files are copied prior to being changed:

```
cp -p /etc/inittab /etc/inittab.$date
cp -p /etc/rc.tcpip /etc/rc.tcpip.$date
cp -p /etc/inetd.conf /etc/inetd.conf.$date
```

3 AIX Security Expert Recommendations

This section provides details of the recommended settings controlled within the AIX Security Expert framework. The settings within this section can all be automatically applied, utilizing the aixpert command to implement the customized XML file.

3.1 AIX Security Expert - Password Policy

This section provides guidance on the configuration of the password policy. This includes recommended length, complexity, reuse and expiration.

The recommendations in this section affect the parameters of the default user stanza. The values set are only applicable if specific values are not defined during the creation of a user. It is therefore recommended to not set any of these values explicitly, unless there is a specific requirement to do so when a user is created.

3.1.1 /etc/security/user - mindiff (Scored)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of characters that are required in a new password which were not in the old password.

Rationale:

In setting the `mindiff` attribute, it ensures that users are not able to reuse the same or similar passwords.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a mindiff
```

The above command should yield the following output:

```
default mindiff=4
```

Remediation:

In `/etc/security/user`, set the default user stanza `mindiff` attribute to be greater than or equal to `4`:

```
chsec -f /etc/security/user -s default -a mindiff=4
```

This means that when a user password is set it needs to comprise of at least 4 characters not present in the previous password.

3.1.2 /etc/security/user - minage (Scored)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of weeks before a password can be changed.

Rationale:

In setting the `minage` attribute, it prohibits users changing their password until a set number of weeks have passed.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minage
```

The above command should yield the following output:

```
default minage=1
```

Remediation:

In`/etc/security/user`, set the default user stanza `minage` attribute to `1`:

```
chsec -f /etc/security/user -s default -a minage=1
```

This means that a user cannot change their password until at least a week after being set.

3.1.3 /etc/security/user - maxage (Scored)

Profile Applicability:

- Level 1

Description:

Defines the maximum number of weeks that a password is valid.

Rationale:

In setting the `maxage` attribute, it enforces regular password changes.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a maxage
```

The above command should yield the following output:

```
default maxage=13
```

Remediation:

In `/etc/security/user`, set the default user stanza `maxage` attribute to a number greater than `0` but less than or equal to `13`:

```
chsec -f /etc/security/user -s default -a maxage=13
```

This means that a user password must be changed 13 weeks after being set . If 0 is set then this effectively disables password ageing.

3.1.4 /etc/security/user - minlen (Scored)

Profile Applicability:

- Level 1

Description:

Defines the minimum length of a password.

Rationale:

In setting the `minlen` attribute, it ensures that passwords meet the required length criteria.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minlen
```

The above command should yield the following output:

```
default minlen=8
```

Remediation:

In `/etc/security/user`, set the default user stanza `minlen` attribute to be greater than or equal to `8`:

```
chsec -f /etc/security/user -s default -a minlen=8
```

This means that all user passwords must be at least 8 characters in length.

NOTE: If a password length greater than 8 is required, an enhanced password hashing algorithm must be selected. The default crypt algorithm only supports 8 character passwords.

3.1.5 /etc/security/user - minalpha (Scored)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of alphabetic characters in a password.

Rationale:

In setting the `minalpha` attribute, it ensures that passwords have a minimum number of alphabetic characters.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minalpha
```

The above command should yield the following output:

```
default minalpha=2
```

Remediation:

In `/etc/security/user`, set the default user stanza `minalpha` attribute to be greater than or equal to `2`:

```
chsec -f /etc/security/user -s default -a minalpha=2
```

This means that there must be at least 2 alphabetic characters within an 8 character user password.

3.1.6 /etc/security/user - minother (Scored)

Profile Applicability:

- Level 1

Description:

Defines the number of characters within a password which must be non-alphabetic.

Rationale:

In setting the `minother` attribute, it increases password complexity by enforcing the use of non-alphabetic characters in every user password.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minother
```

The above command should yield the following output:

```
default minother=2
```

Remediation:

In `/etc/security/user`, set the default user stanza `minother` attribute to be greater than or equal to `2`:

```
chsec -f /etc/security/user -s default -a minother=2
```

This means that there must be at least 2 non-alphabetic characters within an 8 character user password.

3.1.7 /etc/security/user - maxrepeats (Scored)

Profile Applicability:

- Level 1

Description:

Defines the maximum number of times a character may appear in a password.

Rationale:

In setting the `maxrepeats` attribute, it enforces a maximum number of character repeats within a password.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a maxrepeats
```

The above command should yield the following output:

```
default maxrepeats=2
```

Remediation:

In`/etc/security/user`, set the default user stanza `maxrepeats` attribute to `2`:

```
chsec -f /etc/security/user -s default -a maxrepeats=2
```

This means that a user may not use the same character more than twice in a password.

3.1.8 /etc/security/user - histexpire (Scored)

Profile Applicability:

- Level 1

Description:

Defines the period of time in weeks that a user will not be able to reuse a password.

Rationale:

In setting the `histexpire` attribute, it ensures that a user cannot reuse a password within a set period of time.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a histexpire
```

The above command should yield the following output:

```
default histexpire=13
```

Remediation:

In `/etc/security/user`, set the default user stanza `histexpire` attribute to be greater than or equal to `13`:

```
chsec -f /etc/security/user -s default -a histexpire=13
```

This means that a user will not be able to reuse any password set in the last 13 weeks.

3.1.9 /etc/security/user - histsize (Scored)

Profile Applicability:

- Level 1

Description:

Defines the number of previous passwords that a user may not reuse.

Rationale:

In setting the `histsize` attribute, it enforces a minimum number of previous passwords a user cannot reuse.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a histsize
```

The above command should yield the following output:

```
default histsize=20
```

Remediation:

In /etc/security/user, set the default user stanza histsize attribute to be greater than or equal to 20:

```
chsec -f /etc/security/user -s default -a histsize=20
```

This means that a user may not reuse any of the previous 20 passwords.

3.1.10 /etc/security/user - maxexpired (Scored)

Profile Applicability:

- Level 1

Description:

Defines the number of weeks after `maxage`, that a password can be reset by the user.

Rationale:

In setting the `maxexpired` attribute, it limits the number of weeks after password expiry when it may be changed by the user.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a maxexpired
```

The above command should yield the following output:

```
default maxexpired=2
```

Remediation:

In `/etc/security/user`, set the default user stanza `maxexpired` attribute to `2`:

```
chsec -f /etc/security/user -s default -a maxexpired=2
```

This means that a user can only reset their password up to 2 weeks after it has expired. After this an administrative user would need to reset the password.

3.1.11 /etc/security/user - minloweralpha (Scored)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of lower case alphabetic characters in a password.

Rationale:

In setting the `minloweralpha` attribute, the password must contain a lower case alphabetic character when it is changed by the user.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minloweralpha
```

The above command should yield the following output:

```
default minloweralpha=1
```

Remediation:

In `/etc/security/user`, set the default user stanza `minloweralpha` attribute to `1`:

```
chsec -f /etc/security/user -s default -a minloweralpha=1
```

This means that there must be at least 1 lower case alphabetic character within an 8 character user password.

3.1.12 /etc/security/user - minupperalpha (Scored)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of upper case alphabetic characters in a password.

Rationale:

In setting the `minupperalpha` attribute, the password must contain an upper case alphabetic character when it is changed by the user.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minupperalpha
```

The above command should yield the following output:

```
default minupperalpha=1
```

Remediation:

In `/etc/security/user`, set the default user stanza `minupperalpha` attribute to `1`:

```
chsec -f /etc/security/user -s default -a minupperalpha=1
```

This means that there must be at least 1 upper case alphabetic character within an 8 character user password.

3.1.13 /etc/security/user - mindigit (Scored)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of digits in a password.

Rationale:

In setting the `mindigit` attribute, the password must contain a digit when it is changed by the user.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a mindigit
```

The above command should yield the following output:

```
default mindigit=1
```

Remediation:

In `/etc/security/user`, set the default user stanza `mindigit` attribute to `1`:

```
chsec -f /etc/security/user -s default -a mindigit=1
```

This means that there must be at least 1 digit within an 8 character user password.

3.1.14 /etc/security/user - minspecialchar (Scored)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of special characters in a password.

Rationale:

In setting the `minspecialchar` attribute, the password must contain a special character when it is changed by the user.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minspecialchar
```

The above command should yield the following output:

```
default minspecialchar=1
```

Remediation:

In `/etc/security/user`, set the default user stanza `minspecialchar` attribute to `1`:

```
chsec -f /etc/security/user -s default -a minspecialchar=1
```

This means that there must be at least 1 special character within an 8 character user password.

3.1.15 /etc/security/login.cfg - pwd_algorithm (Scored)

Profile Applicability:

- Level 1

Description:

Defines the loadable password algorithm used when storing user passwords.

Rationale:

A development in AIX 6.1 was the ability to use different password algorithms as defined in `/etc/security/pwdalg.cfg`. The traditional UNIX password algorithm is `crypt`, which is a one-way hash function supporting only 8 character passwords. The use of brute force password guessing attacks means that `crypt` no longer provides an appropriate level of security and so other encryption mechanisms are recommended.

The recommendation of this benchmark is to set the password algorithm to `ssha256`. This algorithm supports long passwords, up to 255 characters in length and allows passphrases including the use of the extended ASCII table and the space character. Any passwords already set using `crypt` will remain supported, but there can only one system password algorithm active at any one time.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s usw -a pwd_algorithm
```

The above command should yield the following output:

```
usw pwd_algorithm=ssha256
```

Remediation:

In `/etc/security/login.cfg`, set the usw user stanza `pwd_algorithm` attribute to `ssha256`:

```
chsec -f /etc/security/login.cfg -s usw -a pwd_algorithm=ssha256
```

Impact:

Ensure that all running applications support SHA256 password encyption

3.2 AIX Security Expert - Login Policy

This section provides guidance on the configuration of the system login policy. This includes login timeouts, delays and remote root access.

The recommendations in this section affect the general login policy of the system for all users. Every user should have a dedicated account, to ensure accountability and audit trailing. Any generic accounts should be disabled from direct login, where possible. All remote logons as root should also be prohibited, instead elevation to root should only be allowed once a user has authenticated locally through their individual user account.

3.2.1 System Account Lockdown

This section deals with disabling direct local and remote login to the generic system accounts i.e. daemon, bin, sys, adm, uucp, nobody and lpd. It is recommended that a password is not set on these accounts to ensure that the only access is via su from the root account.

There should not be a requirement to log in as any of these users directly. All users should be given their own unique logon ids to ensure traceability and accountability.

3.2.1.1 system account lockdown - daemon (Scored)

Profile Applicability:

- Level 2

Description:

This change disables direct login access for the `daemon` user account.

Rationale:

This change disables direct local and remote login to the `daemon` user account. It is recommended that a password is not set on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `daemon` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the `daemon` user:

```
lsuser -a login rlogin daemon
```

The above command should yield the following output:

```
daemon login=false rlogin=false
```

Remediation:

Change the login and remote login user flags to disable `daemon` user access:

```
chuser login=false rlogin=false daemon
```

3.2.1.2 system account lockdown - bin (Scored)

Profile Applicability:

- Level 2

Description:

This change disables direct login access for the `bin` user account.

Rationale:

This change disables direct local and remote login to the `bin` user account. It is recommended that a password is not set on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `bin` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the `bin` user:

```
lsuser -a login rlogin bin
```

The above command should yield the following output:

```
bin login=false rlogin=false
```

Remediation:

Change the login and remote login user flags to disable `bin` user access:

```
chuser login=false rlogin=false bin
```

3.2.1.3 system account lockdown - sys (Scored)

Profile Applicability:

- Level 2

Description:

This change disables direct login access for the `sys` user account.

Rationale:

This change disables direct local and remote login to the `sys` user account. It is recommended that a password is not set on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `sys` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the `sys` user:

```
lsuser -a login rlogin sys
```

The above command should yield the following output:

```
sys login=false rlogin=false
```

Remediation:

Change the login and remote login user flags to disable `sys` user access:

```
chuser login=false rlogin=false sys
```

3.2.1.4 system account lockdown - adm (Scored)

Profile Applicability:

- Level 2

Description:

This change disables direct login access for the `adm` user account.

Rationale:

This change disables direct local and remote login to the `adm` user account. It is recommended that a password is not set on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `adm` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the `adm` user:

```
lsuser -a login rlogin adm
```

The above command should yield the following output:

```
adm login=false rlogin=false
```

Remediation:

Change the login and remote login user flags to disable `adm`user access:

```
chuser login=false rlogin=false adm
```

3.2.1.5 system account lockdown - nobody (Scored)

Profile Applicability:

- Level 2

Description:

This change disables direct login access for the `nobody` user account.

Rationale:

This change disables direct local and remote login to the `nobody` user account. It is recommended that a password is not set on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `nobody` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the `nobody`user:

```
lsuser -a login rlogin nobody
```

The above command should yield the following output:

```
nobody login=false rlogin=false
```

Remediation:

Change the login and remote login user flags to disable `nobody` user access:

```
chuser login=false rlogin=false nobody
```

3.2.1.6 system account lockdown - uucp (Scored)

Profile Applicability:

- Level 2

Description:

This change disables direct login access for the `uucp` user account.

Rationale:

This change disables direct local and remote login to the `uucp` user account. It is recommended that a password is not set on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `uucp` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the `uucp` user:

```
lsuser -a login rlogin uucp
```

The above command should yield the following output:

```
uucp login=false rlogin=false
```

Remediation:

Change the login and remote login user flags to disable `uucp` user access:

```
chuser login=false rlogin=false uucp
```

3.2.1.7 system account lockdown - lpd (Scored)

Profile Applicability:

- Level 2

Description:

This change disables direct login access for the `lpd` user account.

Rationale:

This change disables direct local and remote login to the `lpd` user account. It is recommended that a password is not set on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `lpd` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the `lpd`user:

```
lsuser -a login rlogin lpd
```

The above command should yield the following output:

```
lpd login=false rlogin=false
```

Remediation:

Change the login and remote login user flags to disable `lpd`user access:

```
chuser login=false rlogin=false lpd
```

3.2.2 /etc/security/login.cfg - logininterval (Scored)

Profile Applicability:

- Level 1

Description:

Defines the time interval, in seconds, when the unsuccessful logins must occur to disable a port. This parameter is applicable to alltty connections and the system console.

Rationale:

In setting the `logininterval` attribute, a port will be disabled if the incorrect password is entered a pre-defined number of times, set via `logindisable`, within this interval.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s default -a logininterval
```

The above command should yield the following output:

```
default logininterval=300
```

Remediation:

In `/etc/security/login.cfg`, set the default stanza `logininterval` attribute to `300` or less:

```
chsec -f /etc/security/login.cfg -s default -a logininterval=300
```

This means that the port will be disabled if the incorrect password is typed the appropriate number of times, within a 300 second interval.

3.2.3 /etc/security/login.cfg - logindisable (Scored)

Profile Applicability:

- Level 1

Description:

Defines the number of unsuccessful login attempts required before a port will be locked. This parameter is applicable to all `tty` connections and the system console.

Rationale:

In setting the `logindisable` attribute, a port will be disabled if the incorrect password is entered a set number of times within a specified interval, set via `logininterval`.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s default -a logindisable
```

The above command should yield the following output:

```
default logindisable=10
```

Remediation:

In `/etc/security/login.cfg`, set the default stanza `logindisable` attribute to `10` or less:

```
chsec -f /etc/security/login.cfg -s default -a logindisable=10
```

This means that the port will be disabled if the incorrect password is typed 10 times within a 300 second interval.

3.2.4 /etc/security/login.cfg - loginreenable (Scored)

Profile Applicability:

- Level 1

Description:

Defines the number of minutes after a port is locked when it will be automatically un-locked. This parameter is applicable to all `tty` connections and the system console.

Rationale:

In setting the `loginreenable` attribute, a locked port will be automatically re-enabled once a given number of minutes have passed.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s default -a loginreenable
```

The above command should yield the following output:

```
default loginreenable=360
```

Remediation:

In `/etc/security/login.cfg`, set the default stanza `loginreenable` attribute to `360` or greater:

```
chsec -f /etc/security/login.cfg -s default -a loginreenable=360
```

This means that a locked port will be automatically re-enabled 360 minutes after being locked.

3.2.5 /etc/security/login.cfg - logintimeout (Scored)

Profile Applicability:

- Level 1

Description:

Defines the number of seconds during which the password must be typed at login.

Rationale:

In setting the `logintimeout` attribute, a password must be entered within a specified time period.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s usw -a logintimeout
```

The above command should yield the following output:

```
usw logintimeout=30
```

Remediation:

In `/etc/security/login.cfg`, set the usw stanza `logintimeout` attribute to `30` or less:

```
chsec -f /etc/security/login.cfg -s usw -a logintimeout=30
```

This means that a user will have 30 seconds, from prompting, in which to type in their password.

3.2.6 /etc/security/login.cfg - logindelay (Scored)

Profile Applicability:

- Level 1

Description:

Defines the number of seconds delay between each failed login attempt. This works as a multiplier, so if the parameter is set to 10, after the first failed login it would delay for 10 seconds, after the second failed login 20 seconds etc.

Rationale:

In setting the `logindelay` attribute, this implements a delay multiplier in-between unsuccessful login attempts.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s default -a logindelay
```

The above command should yield the following output:

```
default logindelay=10
```

Remediation:

In `/etc/security/login.cfg`, set the default stanza `logindelay` attribute to `10` or greater:

```
chsec -f /etc/security/login.cfg -s default -a logindelay=10
```

This means that a user will have to wait 10 seconds before being able to re-enter their password. During subsequent attempts this delay will increase as a multiplier of (the number of failed login attempts * logindelay)

3.2.7 /etc/security/user - loginretries (Scored)

Profile Applicability:

- Level 1

Description:

Defines the number of attempts a user has to login to the system before their account is disabled.

Rationale:

In setting the `loginretries` attribute, this ensures that a user can have a pre-defined number of attempts to get their password right, prior to locking the account.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a loginretries
```

The above command should yield the following output:

```
default loginretries=3
```

Remediation:

In `/etc/security/user`, set the default stanza `loginretries` attribute to `3`:

```
chsec -f /etc/security/user -s default -a loginretries=3
```

This means that a user will have 3 attempts to enter the correct password. This does not apply to the root user, which has its own stanza entry disabling this feature.

3.2.8 /etc/security/user - rlogin (Scored)

Profile Applicability:

- Level 1

Description:

Defines whether or not the root user can login remotely.

Rationale:

In setting the `rlogin` attribute to false, this ensures that the root user cannot remotely log into the system. All remote logins as root should be prohibited, instead elevation to root should only be allowed once a user has authenticated locally through their individual user account.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s root -a rlogin
```

The above command should yield the following output:

```
root rlogin=false
```

Remediation:

In `/etc/security/user`, set the root stanza `rlogin` attribute to `false`:

```
chsec -f /etc/security/user -s root -a rlogin=false
```

This means that the root user will not be able to log in the system directly.

3.2.9 /etc/security/user - sugroups (Scored)

Profile Applicability:

- Level 1

Description:

Restricts access to root, via `su`, to members of a specific group.

Rationale:

In setting the `sugroups` attribute to `system`, this ensures that only members of the system group are able to su root. This makes it difficult for an attacker to use a stolen root password as the attacker first has to get access to a system user ID.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s root -a sugroups -a su
```

The above command should yield the following output:

```
root sugroups=system su=true
```

Remediation:

In `/etc/security/user`, set the root stanza `sugroups a`ttribute to `system`:

```
chuser su=true sugroups=system root
```

3.3 AIX Security Expert - System Services Management

The objective of this section is to reduce the number of running services down to those which are core to the common functions of a UNIX server. When a superfluous service is not running, the system will not be subject to any latent vulnerability later discovered with that service and not require any subsequent remediation.

This section provides guidance on the startup of system services in /etc/inittab, /etc/rc.tcpip and /etc/inetd.conf. The majority of services within these files are disabled in AIX by default, so this section will focus on those services which are enabled, which if possible, should be disabled.

3.3.1 /etc/inittab - qdaemon (Scored)

Profile Applicability:

- Level 2

Description:

This is the printing scheduling daemon that manages the submission of print jobs to `piobe`.

Rationale:

If there is not a requirement to support local or remote printing, remove the `qdaemon` entry from`/etc/inittab`.

Audit:

From the command prompt, execute the following command:

```
lsitab qdaemon
```

The above command should yield not yield output

Remediation:

In `/etc/inittab`, remove the `qdaemon` entry:

```
rmitab qdaemon
```

3.3.2 /etc/inittab - lpd (Scored)

Profile Applicability:

- Level 2

Description:

The `lpd` daemon accepts remote print jobs from other systems.

Rationale:

If there is not a requirement for the system to act as a remote print server for other servers, remove the `lpd` entry.

Audit:

From the command prompt, execute the following command:

```
lsitab lpd
```

The above command should not yield output

Remediation:

In `/etc/inittab`, remove the `lpd` entry:

```
rmitab lpd
```

3.3.3 /etc/inittab - piobe (Scored)

Profile Applicability:

- Level 2

Description:

The `piobe` daemon is the I/O back end for the printing process, handling the job scheduling and spooling.

Rationale:

If there is not a requirement for the system to support either local or remote printing, remove the `piobe` entry.

Audit:

From the command prompt, execute the following command:

```
lsitab piobe
```

The above command should yield not yield output

Remediation:

In `/etc/inittab`, remove the `piobe` entry:

```
rmitab piobe
```

3.3.4 /etc/inittab - dt (Scored)

Profile Applicability:

- Level 2

Description:

This entry executes the CDE startup script which starts the AIX Common Desktop Environment.

Rationale:

If there is not an `lft` connected to the system and there are no other X11 clients that require CDE, remove the dt entry.

Audit:

From the command prompt, execute the following command:

```
lsitab dt
```

The above command should yield not yield output

Remediation:

In `/etc/inittab`, remove the `dt` entry:

```
rmitab dt
```

3.3.5 /etc/inittab - rcnfs (Scored)

Profile Applicability:

- Level 2

Description:

The `rcnfs` entry starts the NFS daemons during system boot.

Rationale:

NFS is a service with numerous historical vulnerabilities and should not be enabled unless there is no alternative. If NFS serving is required, then read-only exports are recommended

and no filesystem or directory should be exported with root access. Unless otherwise required the NFS daemons will be disabled.

Audit:

From the command prompt, execute the following command:

```
lsitab rcnfs
```

The above command should yield not yield output

Remediation:

Use the `rmitab` command to remove the NFS start-up script from `/etc/inittab`:

```
rmitab rcnfs
```

3.3.6 /etc/rc.tcpip - sendmail (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `sendmail` daemon on system startup. This means that the system can operate as a mail server.

Rationale:

`sendmail` is a service with many historical vulnerabilities and where possible should be disabled. If the system is not required to operate as a mail server i.e. sending, receiving or processing e-mail, comment out the `sendmail` entry.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/lib/sendmail" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/lib/sendmail "$src_running" "-bd -q${qpi}"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `sendmail` entry:

```
chrctcp -d sendmail
```

3.3.7 /etc/rc.tcpip - snmpd (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `snmpd` daemon on system startup. This allows remote monitoring of network and server configuration.

Rationale:

The `snmpd` daemon is used by many 3rd party applications to monitor the health of the system. If `snmpd` is not required, it is recommended that it is disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/snmpd" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/snmpd "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `snmpd` entry:

```
chrctcp -d snmpd
```

3.3.8 /etc/rc.tcpip - dhcpcd (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `dhcpcd` daemon on system startup. The `dhcpcd` deamon receives address and configuration information from the DHCP server.

Rationale:

The `dhcpcd` daemon is the DHCP client that receives address and configuration information from the DHCP server. This must be disabled if DHCP is not used to serve IP address to the local system.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/dhcpcd" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/dhcpcd "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `dhcpcd` entry:

```
chrctcp -d dhcpcd
```

3.3.9 /etc/rc.tcpip - dhcprd (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `dhcprd` daemon on system startup. The `dhcprd` daemon listens for broadcast packets, receives them, and forwards them to the appropriate server.

Rationale:

The `dhcprd` daemon is the DHCP relay deamon that forwards the DHCP and BOOTP packets in the network. You must disable this service if DHCP is not enabled in the network.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/dhcprd" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/dhcprd "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `dhcprd` entry:

```
chrctcp -d dhcprd
```

3.3.10 /etc/rc.tcpip - dhcpsd (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `dhcpsd` daemon on system startup. The `dhcpsd` deamon is the DHCP server that serves addresses and configuration information to DHCP clients in the network.

Rationale:

The `dhcpsd` daemon is the DHCP server that serves addresses and configuration information to DHCP clients in the network. You must disable this service if the server is not a DHCP server.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/dhcpsd" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/dhcpsd "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `dhcpsd` entry:

```
chrctcp -d dhcpsd
```

3.3.11 /etc/rc.tcpip - autoconf6 (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts `autoconf6` on system startup. This is to automatically configure IPv6 interfaces at boot time.

Rationale:

`authoconf6` is used to automatically configure IPv6 interfaces at boot time. Running this service may allow other hosts on the same physical subnet to connect via IPv6, even when the network does not support it. You must disable this unless you utilize IPv6 on the server.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/autoconf6" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/autoconf6 ""
```

Remediation:

In`/etc/rc.tcpip`, comment out the `autoconf6` entry:

```
chrctcp -d autoconf6
```

3.3.12 /etc/rc.tcpip - gated (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `gated` daemon system startup. This daemon provides gateway routing functions for protocols such as RIP and SNMP.

Rationale:

The `gated` daemon provides gateway routing functions for protocols such as RIP and SNMP. It is recommended that this daemon is disabled, unless the server is functioning as a network router.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/gated" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/gated "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `gated` entry:

```
chrctcp -d gated
```

3.3.13 /etc/rc.tcpip - mrouted (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `mrouted` daemon at system startup. This daemon is an implementation of the multicast routing protocol.

Rationale:

The `mrouted` daemon is an implementation of the multicast routing protocol. It is recommended that this daemon is disabled, unless the server is functioning as a multicast router.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/mrouted" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/mrouted "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `mrouted` entry:

```
chrctcp -d mrouted
```

3.3.14 /etc/rc.tcpip - named (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `named` daemon at system startup. This is the server for the DNS protocol and controls domain name resolution for its clients.

Rationale:

The `named` daemon is the server for the DNS protocol and controls domain name resolution for its clients. It is recommended that this daemon is disabled, unless the server is functioning as a DNS server.This entry starts the `named` daemon at system startup. This is the server for the DNS protocol and controls domain name resolution for its clients.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/named" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/named "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `named` entry:

```
chrctcp -d named
```

3.3.15 /etc/rc.tcpip - routed (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `routed` daemon at system startup. The `routed` daemonmanages the network routing tables in the kernel.

Rationale:

The `routed` daemon manages the network routing tables in the kernel. It is recommended that this daemon is disabled, unless the server is functioning as a network router.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/routed" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/routed "$src_running" -q
```

Remediation:

In `/etc/rc.tcpip`, comment out the `routed` entry:

```
chrctcp -d routed
```

3.3.16 /etc/rc.tcpip - rwhod (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `rwhod` daemon at system startup. This is the remote WHO service.

Rationale:

The `rwhod` daemon is the remote WHO service, which collects and broadcasts status information to peer servers on the same network. It is recommended that this daemon is disabled, unless it is required.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/rwhod" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/rwhod "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `rwhod` entry:

```
chrctcp -d rwhod
```

3.3.17 /etc/rc.tcpip - timed (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `timed` daemon at system startup. This is the old UNIX time service.

Rationale:

The `timed` daemon is the old UNIX time service. You must disable this service and use `xntp`, if time synchronization is required in your environment.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/timed" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/timed "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `timed` entry:

```
chrctcp -d timed
```

3.3.18 /etc/rc.tcpip - dpid2 (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `dpid2` daemon on system startup. The `dpid2` daemon acts as a protocol converter, which enables DPI (SNMP v2) sub-agents, such as `hostmibd`, to talk to a SNMP v1 agent that follows SNMP MUX protocol.

Rationale:

The `dpid2` deamon acts as a protocol converter, which enables DPI (SNMP v2) sub-agents, such as `hostmibd`, to talk to a SNMP v1 agent that follows SNMP MUX protocol. Unless the server hosts an SNMP agent, it is recommended that `dpid2` is disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/dpid2" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/dpid2 "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `dpid2` entry:

```
chrctcp -d dpid2
```

3.3.19 /etc/rc.tcpip - hostmibd (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `hostmibd` daemon on system startup. This is a dpi2 sub-agent that may be required if the server runs SNMP.

Rationale:

The `hostmibd` daemon is a dpi2 sub-agent which manages a number of MIB variables. If `snmpd` is not required, it is recommended that it is disabled.

The specific MIB variables which are managed by `hostmibd` are defined by RFC 2790. Further details relating to these MIBS can be found in the URL below:

http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.cmds/doc/aixcmds2/hostmibd.htm?resultof=%22%68%6f%73%74%6d%69%62%64%22%20

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/hostmibd" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/hostmibd "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `hostmibd` entry:

```
chrctcp -d hostmibd
```

3.3.20 /etc/rc.tcpip - snmpmibd (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `snmpmibd` daemon on system startup. This is a dpi2 sub-agent that may be required if the server runs SNMP.

Rationale:

The `snmpmibd` daemon is a dpi2 sub-agent which manages a number of MIB variables. If snmpd is not required, it is recommended that it is disabled.

The specific MIB variables which are managed by `snmpmibd` are defined by numerous RFCs. Further details relating to these MIBS can be found in the URL below:

http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.cmds/doc/aixcmds5/snmpmibd.htm?resultof=%22%73%6e%6d%70%6d%69%62%64%22%20

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/snmpmibd" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/snmpmibd "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `snmpmibd` entry:

```
chrctcp -d snmpmibd
```

3.3.21 /etc/rc.tcpip - aixmibd (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `aixmibd` daemon on system startup. This is a dpi2 sub-agent that may be required if the server runs SNMP.

Rationale:

The `aixmibd` daemon is a dpi2 sub-agent which manages a number of MIB variables. If `snmpd` is not required, it is recommended that it is disabled.

The `aixmibd` collects data from an AIX specific MIB. Further details relating to this MIB can be found in the URL below:

http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.cmds/doc/aixcmds1/aixmibd.htm?resultof=%22%61%69%78%6d%69%62%64%22%20

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/aixmibd" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/aixmibd "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `aixmibd` entry:

```
chrctcp -d aixmibd
```

3.3.22 /etc/rc.tcpip - ndpd-host (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts `ndpd-host` on system startup. This is the Neighbor Discovery Protocol (NDP) daemon, required in IPv6.

Rationale:

The `ndpd-host` is the NDP deamon for the server. Unless the server utilizes IPv6, this is not required and should be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/ndpd-host" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/ndpd-host "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `ndpd-host` entry:

```
chrctcp -d ndpd-host
```

3.3.23 /etc/rc.tcpip - ndpd-router (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts `ndpd-router` on system startup. This manages the Neighbor Discovery Protocol (NDP) for non kernel activities, required in IPv6.

Rationale:

The `ndpd-router` manages NDP for non-kernel activities. Unless the server utilizes IPv6, this is not required and should be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/ndpd-router" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/ndpd-router "$src_running"
```

Remediation:

In `/etc/rc.tcpip`, comment out the `ndpd-router` entry:

```
chrctcp -d ndpd-router
```

3.3.24 /etc/inetd.conf - telnet (Scored)

Profile Applicability:

- Level 1

Description:

This entry starts the `telnetd` daemon when required. This provides a protocol for command line access, from a remote machine.

Rationale:

This `telnet` service is used to service remote user connections. This is historically the most commonly used remote access method for UNIX servers. The username and passwords are passed over the network in clear text and therefore insecurely. Unless required the `telnetd` daemon will be disabled.

Many older legacy systems do not support SSH and still require telnet as a protocol for access. If this is not required, it is recommended that telnet is disabled and SSH is used as a replacement authentication mechanism.

Audit:

From the command prompt, execute the following command:

```
grep "^#telnet[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#telnet stream  tcp6    nowait  root    /usr/sbin/telnetd       telnetd -a
```

Remediation:

In `/etc/inetd.conf`, comment out the `telnet` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'telnet' -p 'tcp6'
```

3.3.25 /etc/inetd.conf - exec (Scored)

Profile Applicability:

- Level 1

Description:

This entry starts the `rexecd` daemon when required. This daemon executes a command from a remote system, once the connection has been authenticated.

Rationale:

The `exec` service is used to execute a command sent from a remote server. The username and passwords are passed over the network in clear text and therefore insecurely. Unless required the `rexecd` daemon will be disabled. This function, if required, should be facilitated through SSH.

Audit:

From the command prompt, execute the following command:

```
grep "^#exec[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#exec    stream  tcp6    nowait  root    /usr/sbin/rexecd        rexecd
```

Remediation:

In `/etc/inetd.conf`, comment out the `exec` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'exec' -p 'tcp6'
```

3.3.26 /etc/inetd.conf - daytime (Scored)

Profile Applicability:

- Level 1

Description:

This entry starts the `daytime` servicewhen required. This provides the current date and time to other servers on a network.

Rationale:

This `daytime` service is a defunct time service, typically used for testing purposes only. The service should be disabled as it can leave the system vulnerable to DoS ping attacks.

Audit:

From the command prompt, execute the following command:

```
grep "^#daytime[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#daytime        stream  tcp     nowait  root    internal
#daytime        dgram   udp     wait    root    internal
```

Remediation:

In `/etc/inetd.conf`, comment out the `daytime` entries:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'daytime' -p 'tcp'
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'daytime' -p 'udp'
```

3.3.27 /etc/inetd.conf - shell (Scored)

Profile Applicability:

- Level 1

Description:

This entry starts the `rshd` daemon when required. This daemon executes a command from a remote system.

Rationale:

This `shell` service is used to execute a command from a remote server. The username and passwords are passed over the network in clear text and therefore insecurely. Unless required the `rshd` daemon will be disabled. This function, if required, should be facilitated through SSH.

Audit:

From the command prompt, execute the following command:

```
grep "^#shell[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#shell  stream  tcp6    nowait  root    /usr/sbin/rshd  rshd
```

Remediation:

In `/etc/inetd.conf`, comment out the `shell` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'shell' -p 'tcp6'
```

3.3.28 /etc/inetd.conf - cmsd (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `cmsd` service when required. This is a calendar and appointment service.

Rationale:

The `cmsd` service is utilized by CDE to provide calendar functionality. If CDE is not required, this service should be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#cmsd[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#cmsd   sunrpc_udp      udp     wait    root    /usr/dt/bin/rpc.cmsd cmsd
100068 2-5
```

Remediation:

In `/etc/inetd.conf`, comment out the `cmsd` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'cmsd' -p 'sunrpc_udp'
```

3.3.29 /etc/inetd.conf - ttdbserver (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `ttdbserver` servicewhen required. It is not a pre-requisite service for CDE, which is fully functional when it is disabled.

Rationale:

The `ttdbserver` service is the tool-talk database service for CDE. This service runs as root and should be disabled. Unless required the `ttdbserver` service will be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#ttdbserver[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#ttdbserver     sunrpc_tcp      tcp     wait    root    /usr/dt/bin/rpc.ttdbs
erver rpc.ttdbserver 100083 1
```

Remediation:

In `/etc/inetd.conf`, comment out the `ttdbserver` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'ttdbserver' -p
'sunrpc_tcp'
```

3.3.30 /etc/inetd.conf - uucp (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `uucp` service when required. This service facilitates file copying between networked servers.

Rationale:

The `uucp` (UNIX to UNIX Copy Program), service allows users to copy files between networked machines. Unless an application or process requires UUCP this should be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#uucp[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#uucp    stream  tcp     nowait  root    /usr/sbin/uucpd uucpd
```

Remediation:

In `/etc/inetd.conf`, comment out the `uucp` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'uucp' -p 'tcp'
```

3.3.31 /etc/inetd.conf - time (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `time` service when required. This service can be used to synchronize system clocks.

Rationale:

The `time` service is an obsolete process used to synchronize system clocks at boot time. This has been superseded by NTP, which should be use if time synchronization is necessary. Unless required the `time` service will be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#time[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#time   stream  tcp     nowait  root    internal
#time   dgram   udp     wait    root    internal
```

Remediation:

In `/etc/inetd.conf`, comment out the `time` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'time' -p 'udp'
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'time' -p 'tcp'
```

3.3.32 /etc/inetd.conf - login (Scored)

Profile Applicability:

- Level 1

Description:

This entry starts the `rlogin` daemon when required. This service authenticates remote user logins.

Rationale:

This `login` service is used to authenticate a remote user connection when logging in via the `rlogin` command. The username and password are passed over the network in clear text and therefore insecurely. Unless required the rlogin daemon will be disabled. This function, if required, should be facilitated through SSH.

Audit:

From the command prompt, execute the following command:

```
grep "^#login[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#login  stream  tcp6    nowait  root    /usr/sbin/rlogind       rlogind
```

Remediation:

In `/etc/inetd.conf`, comment out the `login` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'login' -p 'tcp'
```

3.3.33 /etc/inetd.conf - talk (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `talkd` daemon when required. This service establishes a two-way communication link between two users, either locally or remotely.

Rationale:

This `talk` service is used to establish an interactive two-way communication link between two UNIX users. It is unlikely that there would be a requirement to run this type of service on a UNIX system. Unless required the `talk` service will be disabled

Audit:

From the command prompt, execute the following command:

```
grep "^#talk[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#talk   dgram   udp     wait    root    /usr/sbin/talkd talkd
```

Remediation:

In `/etc/inetd.conf`, comment out the `talk` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'talk' -p 'udp'
```

3.3.34 /etc/inetd.conf - ntalk (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `talkd` daemon when required. This service establishes a two-way communication link between two users, either locally or remotely.

Rationale:

This `ntalk` service is used to establish an interactive two-way communication link between two UNIX users. It is unlikely that there would be a requirement to run this type of service on a UNIX system. Unless required the `ntalk` service will be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#ntalk[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#ntalk   dgram   udp     wait    root    /usr/sbin/talkd talkd
```

Remediation:

In `/etc/inetd.conf`, comment out the `ntalk` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'ntalk' -p 'udp'
```

3.3.35 /etc/inetd.conf - ftp (Scored)

Profile Applicability:

- Level 1

Description:

This entry starts the `ftpd` daemon when required. This service is used for transferring files from/to a remote machine.

Rationale:

This `ftp` service is used to transfer files from or to a remote machine. The username and passwords are passed over the network in clear text and therefore insecurely. Unless required the `ftpd` daemon will be disabled.

Many older legacy systems do not support SSH and still required `ftp` as a service for data copying. If this is not required it is recommended that `ftp` is disabled and `sftp` is used as a replacement file and directory copying mechanism.

Audit:

From the command prompt, execute the following command:

```
grep "^#ftp[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#ftp    stream  tcp6    nowait  root    /usr/sbin/ftpd  ftpd
```

Remediation:

In `/etc/inetd.conf`, comment out the `ftp` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'ftp' -p 'tcp6'
```

3.3.36 /etc/inetd.conf - chargen (Scored)

Profile Applicability:

- Level 1

Description:

This entry starts the `chargen` service when required. This service is used to test the integrity of TCP/IP packets arriving at the destination.

Rationale:

This `chargen` service is a character generator service and is used for testing the integrity of TCP/IP packets arriving at the destination. An attacker may spoof packets between machines running the chargen service and thus provide an opportunity for DoS attacks. You must disable this service unless you are testing your network.

Audit:

From the command prompt, execute the following command:

```
grep "^#chargen[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#chargen        stream  tcp     nowait  root    internal
#chargen        dgram   udp     wait    root    internal
```

Remediation:

In `/etc/inetd.conf`, comment out the `chargen` entries:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'chargen' -p 'tcp'
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'chargen' -p 'udp'
```

3.3.37 /etc/inetd.conf - discard (Scored)

Profile Applicability:

- Level 1

Description:

This entry starts the `discard` service when required. This service is used as a debugging tool by setting up a listening socket which ignores the data it receives.

Rationale:

The `discard` service is used as a debugging and measurement tool. It sets up a listening socket and ignores data that it receives. This is a /dev/null service and is obsolete. This can be used in DoS attacks and therefore, must be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#discard[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#discard        stream  tcp     nowait  root    internal
#discard        dgram   udp     wait    root    internal
```

Remediation:

In `/etc/inetd.conf`, comment out the `discard` entries:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'discard' -p 'tcp'
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'discard' -p 'udp'
```

3.3.38 /etc/inetd.conf - dtspc (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `dtspc` service when required. This service is used in response to a CDE client request.

Rationale:

The `dtspc` service deals with the CDE interface of the X11 daemon. It is started automatically by the `inetd` daemon in response to a CDE client requesting a process to be started on the daemon's host. This makes it vulnerable to buffer overflow attacks, which may allow an attacker to gain root privileges on a host. This service must be disabled unless it is absolutely required.

Audit:

From the command prompt, execute the following command:

```
grep "^#dtspc[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#dtspc stream  tcp     nowait  root    /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
```

Remediation:

In `/etc/inetd.conf`, comment out the `dtspc` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'dtspc' -p 'tcp'
```

3.3.39 /etc/inetd.conf - echo (Scored)

Profile Applicability:

- Level 1

Description:

This entry starts the `echo` service when required. This service sends back data received by it on a specified port.

Rationale:

The `echo` service sends back data received by it on a specified port. This can be misused by an attacker to launch DoS attacks or Smurf attacks by initiating a data storm and causing network congestion. The service is used for testing purposes and therefore must be disabled if not required.

Audit:

From the command prompt, execute the following command:

```
grep "^#echo[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#echo   stream  tcp     nowait  root    internal
#echo   dgram   udp     wait    root    internal
```

Remediation:

In `/etc/inetd.conf`, comment out the `echo` entries:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'echo' -p 'tcp'
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'echo' -p 'udp'
```

3.3.40 /etc/inetd.conf - pcnfsd (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `pcnfsd` daemon when required. This service is an authentication and printing program, which uses NFS to provide file transfer services.

Rationale:

The `pcnfsd` service is an authentication and printing program, which uses NFS to provide file transfer services. This service is vulnerable and exploitable and permits the machine to be compromised both locally and remotely. If PC NFS clients are required within the environment, Samba is recommended as an alternative software solution. The `pcnfsd` daemon predates Microsoft's release of SMB specifications. This service should therefore be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#pcnfsd[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#pcnfsd
sunrpc_udp      udp     wait    root    /usr/sbin/rpc.pcnfsd    pcnfsd 150001
1-2
```

Remediation:

In `/etc/inetd.conf`, comment out the `pcnfsd` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'pcnfsd' -p 'udp'
```

3.3.41 /etc/inetd.conf - rstatd (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `rstatd` daemon when required. This service is used to provide kernel statistics and other monitorable parameters such as CPU usage, system uptime, network usage etc.

Rationale:

The `rstatd` service is used to provide kernel statistics and other monitorable parameters pertinent to the system such as: CPU usage, system uptime, network usage etc. An attacker may use this information in a DoS attack. This service should be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#rstatd[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#rstatd
sunrpc_udp      udp     wait    root    /usr/sbin/rpc.rstatd    rstatd 100001
1-3
```

Remediation:

In `/etc/inetd.conf`, comment out the `rstatd` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rstatd' -p 'udp'
```

3.3.42 /etc/inetd.conf - rusersd (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `rsusersd` daemon when required. This service provides a list of current users active on a system.

Rationale:

The `rusersd` service runs as `root` and provides a list of current users active on a system. An attacker may use this service to learn valid account names on the system. This is not an essential service and should be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#rusersd[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#rusersd        sunrpc_udp      udp     wait    root    /usr/lib/netsvc/ruser
s/rpc.rusersd      rusersd 100002 1-2
```

Remediation:

In `/etc/inetd.conf`, comment out the `rusersd` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rusersd' -p 'udp'
```

3.3.43 /etc/inetd.conf - rwalld (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `rwalld` daemon when required. This service allows remote users to broadcast system wide messages.

Rationale:

The `rwalld` service allows remote users to broadcast system wide messages. The service runs as root and should be disabled unless absolutely necessary.

Audit:

From the command prompt, execute the following command:

```
grep "^#rwalld[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#rwalld
sunrpc_udp      udp     wait    root    /usr/lib/netsvc/rwall/rpc.rwalld
   rwalld 100008 1
```

Remediation:

In `/etc/inetd.conf`, comment out the `rwalld` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rwalld' -p 'udp'
```

3.3.44 /etc/inetd.conf - sprayd (Scored)

Profile Applicability:

- Level 1

Description:

This entry starts the `sprayd` daemon when required. This service is used as a tool to generate UDP packets for testing and diagnosing network problems.

Rationale:

The `sprayd` service is used as a tool to generate UDP packets for testing and diagnosing network problems. The service must be disabled if you are not running NFS, as it can be used by attackers in a Distributed Denial of Service (DDoS) attack.

Audit:

From the command prompt, execute the following command:

```
grep "^#sprayd[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#sprayd
sunrpc_udp      udp     wait    root    /usr/lib/netsvc/spray/rpc.sprayd
   sprayd 100012 1
```

Remediation:

In `/etc/inetd.conf`, comment out the `sprayd` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'sprayd' -p 'udp'
```

3.3.45 /etc/inetd.conf - klogin (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `klogin`service when required. This is a kerberized login service, which provides a higher degree of security over traditional `rlogin` and `telnet`.

Rationale:

The `klogin` service offers a higher degree of security than traditional rloginor telnetby eliminating most clear-text password exchanges on the network. However, it is still not as secure as SSH, which encrypts all traffic. If you use kloginto login to a system, the password is not sent in clear text; however, if you suto another user, that password exchange is open to detection from network-sniffing programs. The recommendation is to utilize SSH wherever possible instead of klogin.

If the `klogin` service is used, you must use the latest kerberos version available and make sure that all the latest patches are installed.

Audit:

From the command prompt, execute the following command:

```
grep "^#klogin[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#klogin stream  tcp     nowait  root    /usr/sbin/krlogind      krlogind
```

Remediation:

In `/etc/inetd.conf`, comment out the `klogin` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'klogin' -p 'tcp'
```

3.3.46 /etc/inetd.conf - kshell (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `kshell` service when required. This is a kerberized remote shell service, which provides a higher degree of security over traditional `rsh`.

Rationale:

The `kshell` service offers a higher degree of security than traditional rsh services. However, it still does not use encrypted communications. The recommendation is to utilize SSH wherever possible instead of `kshell`.

If the `kshell` service is used, you should use the latest kerberos version available and must make sure that all the latest patches are installed.

Audit:

From the command prompt, execute the following command:

```
grep "^#kshell[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#kshell stream  tcp     nowait  root    /usr/sbin/krshd krshd
```

Remediation:

In `/etc/inetd.conf`, comment out the `kshell` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'kshell' -p 'tcp'
```

3.3.47 /etc/inetd.conf - rquotad (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `rquotad` service when required. This allows NFS clients to enforce disk quotas on locally mounted filesystems.

Rationale:

The `rquotad` serviceallows NFS clients to enforce disk quotas on file systems that are mounted on the local system. This service should be disabled if it is not required.

Audit:

From the command prompt, execute the following command:

```
grep "^#rquotad[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#rquotad        sunrpc_udp      udp     wait    root    /usr/sbin/rpc.rquotad
   rquotad 100011 1
```

Remediation:

In `/etc/inetd.conf`, comment out the `rquotad` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rquotad' -p 'udp'
```

3.3.48 /etc/inetd.conf - tftp (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `tftp` service when required.

Rationale:

The `tftp` service allows remote systems to download or upload files to the `tftp` server without any authentication. It is therefore a service that should not run, unless needed. One of the main reasons for requiring this service to be activated is if the host is a NIM master. However, the service can be enabled and then disabled once a NIM operation has completed, rather than left running permanently.

Audit:

From the command prompt, execute the following command:

```
grep "^#tftp[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#tftp   dgram   udp6    SRC     nobody  /usr/sbin/tftpd tftpd -n
```

Remediation:

In `/etc/inetd.conf`, comment out the `tftp` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'tftp' -p 'udp'
```

3.3.49 /etc/inetd.conf - imap2 (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `imap2` service when required.

Rationale:

The `imap2` service orInternet Message Access Protocol (IMAP) supports the IMAP4 remote mail access protocol. It works with `sendmail` and `bellmail`. This service should be disabled if it is not required.

Audit:

From the command prompt, execute the following command:

```
grep "^#imap2[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#imap2  stream  tcp     nowait  root    /usr/sbin/imapd imapd
```

Remediation:

In `/etc/inetd.conf`, comment out the `imap2` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'imap2' -p 'tcp'
```

3.3.50 /etc/inetd.conf - pop3 (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `pop3` service when required.

Rationale:

The `pop3` service provides a `pop3` server. It supports the `pop3` remote mail access protocol. It works with `sendmail` and `bellmail`. This service should be disabled if it is not required.

Audit:

From the command prompt, execute the following command:

```
grep "^#pop3[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#pop3   stream  tcp     nowait  root    /usr/sbin/pop3d pop3d
```

Remediation:

In `/etc/inetd.conf`, comment out the `pop3` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'pop3' -p 'tcp'
```

3.3.51 /etc/inetd.conf - finger (Scored)

Profile Applicability:

- Level 1

Description:

This entry starts the `fingerd` daemon.

Rationale:

The `fingerd` daemon provides the server function for the `finger` command. This allows users to view real-time pertinent user login information on other remote systems. This service should be disabled as it may provide an attacker with a valid user list to target.

Audit:

From the command prompt, execute the following command:

```
grep "^#finger[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#finger stream  tcp     nowait  nobody  /usr/sbin/fingerd     fingerd
```

Remediation:

In `/etc/inetd.conf`, comment out the `finger` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'finger' -p 'tcp'
```

3.3.52 /etc/inetd.conf - instsrv (Scored)

Profile Applicability:

- Level 2

Description:

This entry starts the `instsrv` service when required.

Rationale:

The `instsrv` service is part of the Network Installation Tools, used for servicing servers running AIX 3.2. This service should be disabled.

Audit:

From the command prompt, execute the following command:

```
grep "^#instsrv[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#instsrv stream tcp     nowait  netinst /u/netinst/bin/instsrv instsrv -r
/tmp/netinstalllog /u/netinst/scripts
```

Remediation:

In `/etc/inetd.conf`, comment out the `instsrv` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'instsrv' -p 'tcp'
```

3.3.53 /etc/inetd.conf - permissions and ownership (Scored)

Profile Applicability:

- Level 1

Description:

The recommended permissions and ownership for `/etc/inetd.conf` are applied.

Rationale:

The `/etc/inetd.conf` file contains the list of services that `inetd` controls and determines their current status i.e. active or disabled. This file must be protected from unauthorized access and modifications to ensure that the services disabled in this benchmark remain locked down.

Audit:

From the command prompt, execute the following command:

```
ls -l /etc/inetd.conf | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r--r--   root     system         /etc/inetd.conf
```

Remediation:

Set the recommended permissions and ownership to `/etc/inetd.conf`:

```
chmod u=rw,go=r /etc/inetd.conf
chown root:system /etc/inetd.conf
```

3.4 AIX Security Expert - Disabling Remote Services

This section provides guidance on the local disablement of remote system services. In the previous section, recommendations were made to disable the remote services in /etc/inetd.conf. This stops the server from accepting connections, but the binaries to initiate remote connections from the server to another host should also be restricted along with the daemons themselves being fully disabled. There are also many known security vulnerabilities that relate to these services, they are a primary target for any DoS attack. It is recommended that, unless otherwise required, that the following services and daemons will have their execute permissions removed:
/usr/bin/rcp
/usr/bin/rlogin
/usr/bin/rsh
/usr/sbin/rlogind
/usr/sbin/rshd

3.4.1 Remote command lockdown (Scored)

Profile Applicability:

- Level 2

Description:

Removes all permissions from the remote service commands: `rsh`, `rlogin` and `rcp`.

Rationale:

This effectively disables the following commands, for all users:
`/usr/bin/rcp`
`/usr/bin/rlogin`
`/usr/bin/rsh`

These remote services send usernames and passwords in clear text and should not be used. Unless required these binaries will be disabled for all users. The SSH suite of commands should be utilized to provide equivalent functionality

Audit:

From the command prompt, execute the following commands:

```
ls -l /usr/bin/rcp | awk '{print $1}'
ls -l /usr/bin/rlogin | awk '{print $1}'
ls -l /usr/bin/rsh | awk '{print $1}'
```

Each of the above commands should return with the following permissions:

```
----------
```

Remediation:

Use the `chmod` command to remove all permissions on the remote services:

```
chmod ugo= /usr/bin/rcp
chmod ugo= /usr/bin/rlogin
chmod ugo= /usr/bin/rsh
```

3.4.2 Remote daemon lockdown (Scored)

Profile Applicability:

- Level 2

Description:

Removes all permissions from the remote service daemons: , `rlogind, rshd` and also `tftpd`.

Rationale:

This effectively disables the following daemons, for all users:
`/usr/sbin/rlogind`
`/usr/sbin/rshd`
`/usr/sbin/tftpd`

These remote services both send and receive usernames and passwords in clear text and should not be used. Unless required these daemons will be disabled for all users.

Audit:

From the command prompt, execute the following commands:

```
ls -l /usr/sbin/rlogind | awk '{print $1}'
ls -l /usr/sbin/rshd | awk '{print $1}'
ls -l /usr/sbin/tftpd | awk '{print $1}'
```

Each of the above commands should return with the following permissions:

```
----------
```

Remediation:

Use the `chmod` command to remove all permissions on the remote services:

```
chmod ugo= /usr/sbin/rlogind
chmod ugo= /usr/sbin/rshd
chmod ugo= /usr/sbin/tftpd
```

3.5 AIX Security Expert - Automated Authentication

This section provides guidance on the removal of .nertrc, .rhostsfiles and /etc/hosts.equiv entries. The existence of these files could allow remote access to the system without user or password authentication. It is recommended, that unless otherwise required, any such files are removed from all home directories on the system.

3.5.1 Removal of .rhosts and .netrc files (Scored)

Profile Applicability:

- Level 2

Description:

This recommendation removes all instances of `.rhosts` and `.netrc` files from the system.

Rationale:

The `.rhosts` and `.netrc` files can be used to circumvent normal login or change control procedures. The existence of such files, with the relevant entries, can allow remote user access to a system bypassing local user and password authentication. Unless required these files will be removed from all user home directories.

Audit:

From the command prompt, execute the following commands:

```
find / -name ".netrc" -print
find / -name ".rhosts" -print
```

The above commands should not yield output

Remediation:

Remove the `.rhosts` and `.netrc` files from all user home directories:

```
find / -name ".netrc" -exec rm {} \;
find / -name ".rhosts" -exec rm {} \;
```

3.5.2 Removal of entries from /etc/hosts.equiv (Scored)

Profile Applicability:

- Level 2

Description:

This process removes all entries from the `/etc/hosts.equiv` file.

Rationale:

The `/etc/hosts.equiv` file can be used to circumvent normal login or change control procedures. The existence of this file, with the relevant entries, can allow remote user access to a system bypassing local user and password authentication. Unless required all entries will be removed from this file.

Audit:

From the command prompt, execute the following command:

```
grep -v "^\s*#" /etc/hosts.equiv
```

The above command should not yield output

Remediation:

Remove all entries from the `/etc/hosts.equiv` file:

```
sed '/^\s*$/d; s/^\(\s*[^#].*\)/#\1/' /etc/hosts.equiv >
/etc/hosts.equiv.work
mv hosts.equiv.work hosts.equiv
chown root:system /etc/hosts.equiv
chmod 644 /etc/hosts.equiv
```

Note: the above command removes blank lines and comments out any non commented entries.

3.6 AIX Security Expert - TCP/IP Hardening

This section of the benchmark will focus on the hardening of standard TCP/IP tuning parameters. This is particularly important for the security of the system as the risk of SYN, source routing and smurf attacks can all be significantly reduced or eliminated by following the recommendations in this section. It is anticipated that any firewalls will also be configured to safeguard against these types of attack.

3.6.1 TCP/IP Tuning - ipsrcrouteforward (Scored)

Profile Applicability:

- Level 2

Description:

The `ipsrcrouteforward` parameter determines whether or not the system forwards IPV4 source-routed packets.

Rationale:

The `ipsrcrouteforward` will be set to 0, to prevent source-routed packets being forwarded by the system. This would prevent a hacker from using source-routed packets to bridge an external facing server to an internal LAN, possibly even through a firewall.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipsrcrouteforward[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsrcrouteforward = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipsrcrouteforward` entry:

```
no -p -o ipsrcrouteforward=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

3.6.2 TCP/IP Tuning - ipignoreredirects (Scored)

Profile Applicability:

- Level 2

Description:

The `ipignoreredirects` parameter determines whether or not the system will process IP redirects.

Rationale:

The `ipignoreredirects`will be set to 1, to prevent IP re-directs being processed by the system.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipignoreredirects[[:blank:]]=[[:blank:]]1"
```

The above command should yield the following output:

```
ipignoreredirects = 1
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipignoreredirects` entry:

```
no -p -o ipignoreredirects=1
```

This makes the change permanent by adding the entry into`/etc/tunables/nextboot`

3.6.3 TCP/IP Tuning - clean_partial_conns (Scored)

Profile Applicability:

- Level 2

Description:

The `clean_partial_conns` parameter determines whether or not the system is open to SYN attacks. This parameter, when enabled, clears down connections in the SYN RECEIVED state

after a set period of time. This attempts to stop DoS attacks when a hacker may flood a system with SYN flag set packets.

Rationale:

The `clean_partial_conns`parameter will be set to 1, to clear down pending SYN received connections after a set period of time.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "clean_partial_conns[[:blank:]]=[[:blank:]]1"
```

The above command should yield the following output:

```
clean_partial_conns = 1
```

Remediation:

In `/etc/tunables/nextboot`, add the `clean_partial_conns` entry:

```
no -p -o clean_partial_conns=1
```

This makes the change permanent by adding the entry into`/etc/tunables/nextboot`

3.6.4 TCP/IP Tuning - ipsrcroutesend (Scored)

Profile Applicability:

- Level 2

Description:

The `ipsrcroutesend` parameter determines whether or not the system can send source-routed packets.

Rationale:

The `ipsrcroutesend` parameter will be set to 0, to ensure that any local applications cannot send source routed packets.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipsrcroutesend[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsrcroutesend = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipsrcroutesend` entry:

```
no -p -o ipsrcroutesend=0
```

This makes the change permanent by adding the entry into`/etc/tunables/nextboot`

3.6.5 TCP/IP Tuning - ipforwarding (Scored)

Profile Applicability:

- Level 2

Description:

The `ipforwarding` parameter determines whether or not the system forwards TCP/IP packets.

Rationale:

The `ipforwarding` parameter will be set to 0, to ensure that redirected packets do not reach remote networks. This should only be enabled if the system is performing the function of an IP router. This is typically handled by a dedicated network device.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipforwarding[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipforwarding = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipforwarding` entry:

```
no -p -o ipforwarding=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

3.6.6 TCP/IP Tuning - ipsendredirects (Scored)

Profile Applicability:

- Level 2

Description:

The `ipsendredirects` parameter determines whether or not the system forwards re-directed TCP/IP packets.

Rationale:

The `ipsendredirects` parameter will be set to 0, to ensure that redirected packets do not reach remote networks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipsendredirects[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsendredirects = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipsendredirects` entry:

```
no -p -o ipsendredirects=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

3.6.7 TCP/IP Tuning - ip6srcrouteforward (Scored)

Profile Applicability:

- Level 2

Description:

The `ip6srcrouteforward` parameter determines whether or not the system forwards IPV6 source-routed packets.

Rationale:

The `ip6srcrouteforward` parameter will be set to 0, to prevent source-routed packets being forwarded by the system. This would prevent a hacker from using source-routed packets to bridge an external facing server to an internal LAN, possibly even through a firewall.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ip6srcrouteforward[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ip6srcrouteforward = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ip6srcrouteforward` entry:

```
no -p -o ip6srcrouteforward=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

3.6.8 TCP/IP Tuning - directed_broadcast (Scored)

Profile Applicability:

- Level 2

Description:

The `directed_broadcast` parameter determines whether or not the system allows a directed broadcast to a network gateway.

Rationale:

The `directed_broadcast` parameter will be set to 0, to prevent directed broadcasts being sent network gateways. This would prevent a redirected packet from reaching a remote network.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "directed_broadcast[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
directed_broadcast = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `directed_broadcast` entry:

```
no -p -o directed_broadcast=0
```

This makes the change permanent by adding the entry into`/etc/tunables/nextboot`

3.6.9 TCP/IP Tuning - tcp_pmtu_discover (Scored)

Profile Applicability:

- Level 2

Description:

The `tcp_pmtu_discover` parameter controls whether TCP MTU discovery is enabled.

Rationale:

The `tcp_pmtu_discover` parameter will be set to 0. The idea of MTU discovery is to avoid packet fragmentation between remote networks. This is achieved by discovering the network route and utilizing the smallest MTU size within that path when transmitting packets. When `tcp_pmtu_discover` is enabled, it leaves the system vulnerable to source routing attacks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "tcp_pmtu_discover[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
tcp_pmtu_discover = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `tcp_pmtu_discover` entry:

```
no -p -o tcp_pmtu_discover=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

3.6.10 TCP/IP Tuning - bcastping (Scored)

Profile Applicability:

- Level 2

Description:

The `bcastping` parameter determines whether the system responds to ICMP echo packets sent to the broadcast address.

Rationale:

The `bcastping` parameterwill be set to 0. This means that the system will not respond to ICMP packets sent to the broadcast address. By default, when this is enabled the system is susceptible to smurf attacks, where a hacker utilizes this tool to send a small number of ICMP echo packets. These packets can generate huge numbers of ICMP echo replies and seriously affect the performance of the targeted host and network. This parameter will be disabled to ensure protection from this type of attack.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "bcastping[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
bcastping = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `bcastping` entry:

```
no -p -o bcastping=0
```

This makes the change permanent by adding the entry into`/etc/tunables/nextboot`

3.6.11 TCP/IP Tuning - icmpaddressmask (Scored)

Profile Applicability:

- Level 2

Description:

The `icmpaddressmask` parameter determines whether the system responds to an ICMP address mask ping.

Rationale:

The `icmpaddressmask` parameter will be set to 0, This means that the system will not respond to ICMP address mask request pings. By default, when this is enabled the system is susceptible to source routing attacks. This is typically a feature performed by a device such as a network router and should not be enabled within the operating system.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "icmpaddressmask[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
icmpaddressmask = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `icmpaddressmask` entry:

```
no -p -o icmpaddressmask=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

3.6.12 TCP/IP Tuning - udp_pmtu_discover (Scored)

Profile Applicability:

- Level 2

Description:

The `udp_pmtu_discover` parameter controls whether MTU discovery is enabled.

Rationale:

The `udp_pmtu_discover` parameter will be set to 0. The idea of MTU discovery is to avoid packet fragmentation between remote networks. This is achieved by discovering the network route and utilizing the smallest MTU size within that path when transmitting packets. When `udp_pmtu_discover` is enabled, it leaves the system vulnerable to source routing attacks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "udp_pmtu_discover[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
udp_pmtu_discover = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `udp_pmtu_discover` entry:

```
no -p -o udp_pmtu_discover=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

3.6.13 TCP/IP Tuning - ipsrcrouterecv (Scored)

Profile Applicability:

- Level 2

Description:

The `ipsrcrouterecv` parameter determines whether the system accepts source routed packets.

Rationale:

The `ipsrcrouterecv` parameter will be set to 0, This means that the system will not accept source routed packets. By default, when this is enabled the system is susceptible to source routing attacks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipsrcrouterecv[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsrcrouterecv = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipsrcrouterecv` entry:

```
no -p -o ipsrcrouterecv=0
```

This makes the change permanent by adding the entry into`/etc/tunables/nextboot`

3.6.14 TCP/IP Tuning - nonlocsrcroute (Scored)

Profile Applicability:

- Level 2

Description:

The `nonlocsrcroute` parameter determines whether the system allows source routed packets to be addressed to hosts outside of the LAN.

Rationale:

The `nonlocsrcroute` parameter will be set to 0. This means that the system will not allow source routed packets to be addressed to hosts outside of the LAN. By default, when this is enabled the system is susceptible to source routing attacks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "nonlocsrcroute[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
nonlocsrcroute = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `nonlocsrcroute` entry:

```
no -p -o nonlocsrcroute=0
```

This makes the change permanent by adding the entry into`/etc/tunables/nextboot`

3.6.15 TCP/IP Tuning - tcp_tcpsecure (Scored)

Profile Applicability:

- Level 2

Description:

The `tcp_tcpsecure` parameter value determines if the system is protected from three specific vulnerabilities:

Fake SYN - This is used to terminate an established connection. A `tcp_tcpsecure` value of 1 protects the system from this vulnerability.

Fake RST - As above, this is used to terminate an established connection. A `tcp_tcpsecure` value of 2 protects the system from this vulnerability.

Fake data - A hacker may inject fake data into an established connection. A `tcp_tcpsecure` value of 4 protects the system from this vulnerability.

Rationale:

The `tcp_tcpsecure` parameterwill be set to 7. This means that the system will be protected from any connection reset and data integrity attacks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "tcp_tcpsecure[[:blank:]]=[[:blank:]]7"
```

The above command should yield the following output:

```
tcp_tcpsecure = 7
```

Remediation:

In `/etc/tunables/nextboot`, add the `tcp_tcpsecure` entry:

```
no -p -o tcp_tcpsecure=7
```

This makes the change permanent by adding the entry into`/etc/tunables/nextboot`

3.6.16 TCP/IP Tuning - sockthresh (Scored)

Profile Applicability:

- Level 2

Description:

The `sockthresh` parameter value determines what percentage of the total memory allocated to networking, set via `thewall`, can be used for sockets.

Rationale:

The `sockthresh` parameterwill be set to `60`. This means that 60% of network memory can be used to service new socket connections, the remaining 40% is reserved for existing sockets. This ensures a quality of service for existing connections.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "sockthresh[[:blank:]]=[[:blank:]]60"
```

The above command should yield the following output:

```
sockthresh = 60
```

Remediation:

In `/etc/tunables/nextboot`, add the `sockthresh` entry:

```
no -p -o sockthresh=60
```

This makes the change permanent by adding the entry into`/etc/tunables/nextboot`

3.6.17 TCP/IP Tuning - rfc1323 (Scored)

Profile Applicability:

- Level 2

Description:

The `rfc1323` parameter determines whether the TCP window sizes (`tcp_sendspace` and `tcp_recvspace`) can be greater than 64KB.

Rationale:

The `rfc1323` parameterwill be set to 1. This means that the system will allow the TCP windows sizes to exceed 64KB. This is a requirement for high performance networks, particularly those which utilize large MTU sizes.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "rfc1323[[:blank:]]=[[:blank:]]1"
```

The above command should yield the following output:

```
rfc1323 = 1
```

Remediation:

In `/etc/tunables/nextboot`, add the `rfc1323` entry:

```
no -p -o rfc1323=1
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

3.6.18 TCP/IP Tuning - tcp_sendspace (Scored)

Profile Applicability:

- Level 2

Description:

The `tcp_sendspace` parameter sets the socket buffer size for sending data. This recommendation changes the default size, but many adapters have specific buffer sizes implemented within the device driver. These are typically 64KB or greater.

Rationale:

The `tcp_sendspace` parameter will be set to 262144. This means that the system default socket buffer size for sending data will be 262KB. This is the minimum recommendation for modern high performance networks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "tcp_sendspace[[:blank:]]=[[:blank:]]262144"
```

The above command should yield the following output:

```
tcp_sendspace = 262144
```

Remediation:

In `/etc/tunables/nextboot`, add the `tcp_sendspace` entry:

```
no -p -o tcp_sendspace=262144
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

3.6.19 TCP/IP Tuning - tcp_recvspace (Scored)

Profile Applicability:

- Level 2

Description:

The `tcp_recvspace` parameter sets the socket buffer size for receiving data. This recommendation changes the default size, but many adapters have specific buffer sizes implemented within the device driver. These are typically 64KB or greater.

Rationale:

The `tcp_recvspace` parameterwill be set to 262144. This means that the system default socket buffer size for receiving data will be 262KB. This is the minimum recommendation for modern high performance networks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "tcp_recvspace[[:blank:]]=[[:blank:]]262144"
```

The above command should yield the following output:

```
tcp_recvspace = 262144
```

Remediation:

In `/etc/tunables/nextboot`, add the `tcp_recvspace` entry:

```
no -p -o tcp_recvspace=262144
```

This makes the change permanent by adding the entry into`/etc/tunables/nextboot`

3.6.20 TCP/IP Tuning - tcp_mssdflt (Scored)

Profile Applicability:

- Level 2

Description:

The `tcp_mssdflt` parameter sets the maximum segment size for communication to a remote network. This parameter is only relevant if MTU discovery is disabled, which is recommended in this benchmark.

Rationale:

The `tcp_mssdflt` parameter will be set to 1448 . This value reflects the packet size minus the TCP/IP headers.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "tcp_mssdflt[[:blank:]]=[[:blank:]]1448"
```

The above command should yield the following output:

```
tcp_mssdflt = 1448
```

Remediation:

In `/etc/tunables/nextboot`, add the `tcp_mssdflt` entry:

```
no -p -o tcp_mssdflt=1448
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

3.6.21 TCP/IP Tuning - nfs_use_reserved_ports (Scored)

Profile Applicability:

- Level 2

Description:

The `portcheck` and `nfs_use_reserved_ports` parameters force the NFS server process on the local system to ignore NFS client requests that do not originate from the privileged ports range (ports less than 1024).

Rationale:

The `portcheck` and `nfs_use_reserved_ports` parameters will both be set to 1. This value means that NFS client requests that do not originate from the privileged ports range (ports less than 1024) will be ignored by the local system.

Audit:

From the command prompt, execute the following commands:

```
nfso -a |egrep "(portcheck|nfs_use_reserved_ports)[[:blank:]]=[[::blank::]]1"
```

The above commands should yield the following output:

```
portcheck = 1
nfs_use_reserved_ports = 1
```

Remediation:

In `/etc/tunables/nextboot`, add the `portcheck` and `nfs_use_reserved_ports` entries:

```
nfso -p -o portcheck=1
nfso -p -o nfs_use_reserved_ports=1
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

3.7 AIX Security Expert - Miscellaneous Enhancements

This section will detail some of the more generic changes made during the implementation of the customized XML file i.e. those which may not warrant a dedicated section.

If the customized XML file has been used, the recommendations in this section are the final automated AIX Security Expert changes in this benchmark.

3.7.1 Miscellaneous Enhancements - crontab access (Scored)

Profile Applicability:

- Level 2

Description:

This change creates a `cron.allow` file with a root user entry and removes the `cron.deny` file, if it exists.

Rationale:

This ensures that only the root user has the ability to create a crontab. A hacker may exploit use of the crontab to execute programs or processes automatically. Limiting access to the root account only reduces this risk.

Audit:

From the command prompt, execute the following command:

```
egrep "root|adm" /var/adm/cron/cron.allow
```

The above command should yield the following output:

```
root
adm
```

Remediation:

Create the `/var/adm/cron/cron.allow` file and remove `/var/adm/cron/cron.deny` (if it exists):

```
print "root\nadm" > /var/adm/cron/cron.allow
rm /var/adm/cron/cron.deny
```

3.7.2 Miscellaneous Enhancements - at access (Scored)

Profile Applicability:

- Level 2

Description:

This change creates an `at.allow` file with a root user entry and removes the `at.deny` file, if it exists.

Rationale:

This ensures that only the root user has the ability to schedule jobs through the `at` command. A hacker may exploit use of `at` to execute programs or processes automatically. Limiting access to the root account only reduces this risk.

Audit:

From the command prompt, execute the following command:

```
grep "root" /var/adm/cron/at.allow
```

The above command should yield the following output:

```
root
```

Remediation:

Create the `/var/adm/cron/at.allow` file and remove `/var/adm/cron/at.deny` (if it exists):

```
echo "root" > /var/adm/cron/at.allow
rm /var/adm/cron/at.deny
```

3.7.3 Miscellaneous Enhancements - /etc/ftpusers (Scored)

Profile Applicability:

- Level 1

Description:

This change adds the root user to the `/etc/ftpusers` file, which disables `ftp` for root.

Rationale:

This change ensures that direct root `ftp` access is disabled. As detailed previously, `ftp` as a service should be disabled. If the service has to be enabled then this change must be implemented to ensure that remote root file transfer access is not enabled.

Audit:

From the command prompt, execute the following command:

```
grep "root" /etc/ftpusers
```

The above command should yield the following output:

```
root
```

Remediation:

Add root to the `/etc/ftpusers` file:

```
echo "root" >> /etc/ftpusers
```

3.7.4 Miscellaneous Enhancements - login herald (Scored)

Profile Applicability:

- Level 1

Description:

This change adds a default herald to `/etc/security/login.cfg`.

Rationale:

This change puts into place a suggested login herald to replace the default entry. As the herald is presented to a user prior to logon, it should not provide any information about the operating system or version. Instead, it should detail a company standard acceptable use policy. This herald can be subsequently tailored to reflect a corporate standard policy.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s default -a herald |grep
'^default[[:blank:]]herald="Unauthorized use of this system is prohibited.'
```

The above command should yield the following output:

```
default herald="Unauthorized use of this system is prohibited.\nlogin:"
```

Remediation:

Add a default login herald to `/etc/security/login.cfg`:

```
chsec -f /etc/security/login.cfg -s default -a herald="Unauthorized use of\
 this system is prohibited.\nlogin:"
```

3.7.5 Miscellaneous Enhancements - guest account removal (Scored)

Profile Applicability:

- Level 1

Description:

This change removes the `guest` user and home directory from the system.

Rationale:

This change removes the `guest` user. If a user logs in with a generic username, audit trails are of limited value as it is not necessarily possible to identify who has accessed an account.

The guest account should be removed and all users should be given specific logon ids to ensure traceability and accountability.

Audit:

From the command prompt, execute the following command:

```
lsuser guest
```

The above command should yield the following output:

```
3004-687 User "guest" does not exist.
```

Remediation:

Remove the `guest` user:

```
rmuser -p guest
rm -r /home/guest
```

3.7.6 Miscellaneous Enhancements - crontab permissions (Scored)

Profile Applicability:

- Level 1

Description:

This script checks the permissions of all the root `crontab` entries, to ensure that they are owned and writable by the root user only.

Rationale:

All root `crontab` entries must be owned and writable by the root user only. If a script had group or world writable access, it could be replaced or edited with malicious content, which would then subsequently run on the system with root authority.

Audit:

From the command prompt, execute the following script:

```
crontab -l |egrep -v '^#' |awk '{print $6}' |grep "^/" |sort -u | while read
DIR
do
DIR=${DIR:-$(pwd)}
while [[ -a ${DIR} ]]
```

```
do
[[ "$(ls -ld ${DIR})" = @(????????w? *) ]] && print " WARNING ${DIR} is world
writable"
[[ "$(ls -ld ${DIR})" = @(?????w???? *) ]] && print " WARNING ${DIR} is group
writable"
[[ "$(ls -ld ${DIR} |awk '{print $3}')" != @(root|bin) ]] && print " WARNING
${DIR} is not owned by root or bin"
DIR=${DIR%/*}
done
done
```

Remediation:

Ensure that all root crontab entries are owned and writable by root only.

The script below traverses up each individual directory path, ensuring that all directories are not group/world writable and that they are owned by the root or bin user:

```
crontab -l |egrep -v '^#' |awk '{print $6}' |grep "^/" |sort -u | while read
DIR
do
DIR=${DIR:-$(pwd)}
while [[ -a ${DIR} ]]
do
[[ "$(ls -ld ${DIR})" = @(????????w? *) ]] && print " WARNING ${DIR} is world
writable"
[[ "$(ls -ld ${DIR})" = @(?????w???? *) ]] && print " WARNING ${DIR} is group
writable"
[[ "$(ls -ld ${DIR} |awk '{print $3}')" != @(root|bin) ]] && print " WARNING
${DIR} is not owned by root or bin"
DIR=${DIR%/*}
done
done
```

NOTE: Review the output and manually change the directories, if possible. Directories which are group and/or world writable or not owned by root are marked with "WARNING"

To manually change permissions on the files or directories:

To remove group writable access:

```
chmod g-w <name>
```

To remove world writable access:

```
chmod o-w <name>
```

To remove both group and world writable access:

```
chmod go-w <name>
```

To change the owner of a file or directory:

```
chown <new user> <name>
```

3.7.7 Miscellaneous Enhancements - default umask (Scored)

Profile Applicability:

- Level 2

Description:

This changes the default user `umask` in `/etc/security/user`.

Rationale:

The default user `umask` will be set to 027. This means that the default file creation permissions give read and write access to the user, read access to the group and no access to other. The default directory creation permissions give read, write and execute access to the user, read and execute to the group and no access to other. This is the recommended `umask` setting, as world access should be explicitly defined and not added during default creation. Where possible, access to files and directories should be managed via group membership and ACL's, rather than opening up directory structures for world access. In particular, world write access should be avoided.

Consideration should be given to further securing the default user `umask` by implementing 077. This means that only the user has read/write access to the files and directories they create. Group and/or world access would need to be explicitly defined.

As part of this change all explicitly defined `umask` user settings are removed (if using the customized XML file).

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a umask
```

The above command should yield the following output:

```
default umask=27
```

Remediation:

Add the `umask` attribute to the default user stanza in `/etc/security/user`:

```
chsec -f /etc/security/user -s default -a umask=027
```

3.7.8 Miscellaneous Enhancements - disabling core dumps (Scored)

Profile Applicability:

- Level 2

Description:

This change disables core dumps in the default user stanza of `/etc/security/limits` and also ensures the `fullcore` kernel parameter is set to false.

Rationale:

The creation of core dumps can reveal pertinent system information, potentially even passwords, within the core file. The ability to create a core dump is also a vulnerability to be exploited by a hacker.

The commands below disable core dumps by default, but they may be specifically enabled for a particular user in `/etc/security/limits`.

Audit:

From the command prompt, execute the following command to validate the `/etc/security/limits` changes:

```
lssec -f /etc/security/limits -s default -a core -a core_hard
```

The above command should yield the following output:

```
default core=0 core_hard=0
```

Ensure that the `fullcore` kernel parameter has been set to false:

```
lsattr -El sys0 -a fullcore
```

The above command should yield the following output:

```
fullcore false Enable full CORE dump True
```

Remediation:

Change the default user stanza attributes `core` and `core_hard` in `/etc/security/limits` and the set the `fullcore` kernel parameter to false:

```
chsec -f /etc/security/limits -s default -a core=0 -a core_hard=0
chdev -l sys0 -a fullcore=false
```

3.7.9 Miscellaneous Enhancements - AIX Auditing (Scored)

Profile Applicability:

- Level 2

Description:

This recommendation configures AIX auditing in bin mode.

Rationale:

AIX auditing provides a framework within which to capture pertinent system and security related information, such as failed login attempts, cron usage etc. It is recommended that auditing is enabled as part of a group of measures designed to provide enhanced logging of system and security changes.
Further information regarding the setup and management of AIX accounting and auditing can be found in the "Accounting and Auditing for AIX 5L Redbook":

http://www.redbooks.ibm.com/redbooks/pdfs/sg246396.pdf

Audit:

Ensure that the `/audit` filesystem has been created and mounted:

```
df -k /audit
```

The above command should yield the following output:

```
/dev/auditlv       262144    261776    1%        4     1% /audit
```

Validate the configuration in the `/etc/security/audit/config` file, this should match the changes made in the remediation section:

```
cat /etc/security/audit/config
```

Ensure that the `/usr/lib/security/mkuser.default` auditclasses entry has been updated:

```
lssec -f /usr/lib/security/mkuser.default -s user -a auditclasses
```

The above command should yield the following output:

```
user auditclasses=general,SRC,cron,tcpip
```

Ensure that the `cron` audit rotation script has been implemented:

```
crontab -l |grep "cronaudit"
```

The above command should yield the following output:

```
0 * * * * /etc/security/aixpert/bin/cronaudit
```

Ensure that the audit startup line has been added into `/etc/inittab`:

```
lsitab audit
```

This should echo:

```
audit:2:boot:audit start > /dev/console 2>&1 # Start audit
```

Remediation:

Configure AIX auditing in-line with the High Level AIX Security Expert policy.

Create a `/audit` filesystem, at least 100 MB in size:

```
mklv -y <LV name> -t jfs2 -u 1 -c 1 rootvg 1 hdisk0
crfs -v jfs2 -d auditlv -m /audit -A yes -t no
mount /audit
```

Reflect the following configuration in the `/etc/security/audit/config` file:

```
vi /etc/security/audit/config
```

Add in:

```
start:
            binmode = on
            streammode = off
bin:
           trail = /audit/trail
            bin1 = /audit/bin1
            bin2 = /audit/bin2
            binsize = 10240
            cmds = /etc/security/audit/bincmds
```

Add the auditing entries for root and all other users below the pre-defined audit classes:

```
users:
        root = general,SRC,mail,cron,tcpip,ipsec,lvm
        <user 1> = general,SRC,cron,tcpip
        <user 2> = general,SRC,cron,tcpip
        etc.
```

Update the `/usr/lib/security/mkuser.default` auditclasses entry to ensure that auditing is set up for any newly created users:

```
chsec -f /usr/lib/security/mkuser.default -s user -a
auditclasses=general,SRC,cron,tcpip
```

A cron job is implemented to monitor the free space in `/audit`, running hourly, to ensure that `/audit` does not fill up. If `/audit` is greater than 90% used, `/audit/trail` is moved to `/audit/trailOneLevelBack`:

```
crontab -e
```

Add in:

```
0 * * * * /etc/security/aixpert/bin/cronaudit
```

NOTE: The implementation of a script to suit internal security policy is recommended to further enhance the log rotation process.

Add the audit startup command into `/etc/inittab`:

```
mkitab "audit:2:boot:audit start > /dev/console 2>&1 # Start audit"
```

4 Non AIX Security Expert Managed Recommendations

This section of the benchmark will focus on the recommendations which are not automatically applied during the implementation of the AIX Security Expert customized XML file. A number of these recommendations are not scorable, in that the implementation needs to be tailored to suit the needs of a given environment, which also makes compliance checking impossible.

The following recommendations are detailed in this section:

- Configuring syslog
- Secure remote access
- Configuring sendmail
- Configuring CDE
- Configuring NFS
- Configuring SNMP
- TCP Wrappers
- File and directory permissions and ownership
- Privileged command management - Enhanced RBAC and sudo
- Encrypted Filesystem (EFS)
- Trusted Execution
- General Permissions Management

4.1 Configuring syslog

This section will detail the recommendations regarding the configuration of syslog. By default the information sent to syslogd is not logged and important and pertinent information, such as failed switch user and login attempts are not recorded. The type of data which can be captured through this mechanism can be used for real-time and retrospective analysis, and is particularly useful for monitoring access to the system.

Logging data, via syslogd, may also provide unequivocal evidence against any individual or organization that successfully breach, or attempt to circumvent the security access controls surrounding a system.

4.1.1 Configuring syslog - local logging (Scored)

Profile Applicability:

- Level 2

Description:

This recommendation implements a local `syslog` configuration.

Rationale:

Establishing a logging process via `syslog` provides system and security administrators with pertinent information relating to: login, mail, daemon, user and kernel activity. The recommendation is to enable local `syslog` logging, with a weekly rotation policy in a four weekly cycle. The log rotation isolates historical data which can be reviewed retrospectively if an issue is uncovered at a later date.

Audit:

Ensure that the log entries have been added successfully:

```
tail -2 /etc/syslog.conf
```

The above command should yield the following output:

```
auth.info               /var/adm/authlog rotate time 1w files 4
*.info;auth.none        /var/adm/syslog rotate time 1w files 4
```

Check that the `authlog` and `syslog` files have been created:

```
ls -l /var/adm/authlog /var/adm/syslog
```

The output of the command above should list both files

Remediation:

Explicitly define a log file for the `auth.info` output in `/etc/syslog.conf`:

```
printf "auth.info\t\t/var/adm/authlog rotate time 1w files 4\n" >>
/etc/syslog.conf
```

NOTE: This ensures that remote login, `sudo` or `su` attempts are logged separately

Create the `authlog` file and make it readable by root only:

```
touch /var/adm/authlog
chown root:system /var/adm/authlog
chmod u=rw,go= /var/adm/authlog
```

Create an entry in `/etc/syslog.conf` to capture all other output of level info or higher, excluding authentication information, as this is to be captured within `/var/adm/authlog`:

```
printf "*.info;auth.none\t/var/adm/syslog rotate time 1w files 4\n" >>
/etc/syslog.conf
```

Create the `syslog` file:

```
touch /var/adm/syslog
chmod u=rw,g=r,o= /var/adm/syslog
```

Refresh `syslogd` to force the daemon to read the edited `/etc/syslog.conf`:

```
refresh -s syslogd
```

4.1.2 Configuring syslog - remote logging (Scored)

Profile Applicability:

- Level 2

Description:

This recommendation implements a remote `syslog` configuration.

Rationale:

To further enhance the local `syslog` logging process, it is recommended that syslog information, in particular that generated by the auth facility, is logged remotely. This recommendation assumes that a remote and secure syslog server is available on the network. If this is not the case, please skip to the next recommendation.

The primary reason for logging remotely is to provide an un-editable audit trail of system access. If a hacker were to access a system and gain super user authority it would be easy to edit local files and remove all traces of access, providing the system administrator with no way of identifying the individual or group responsible. If the log data is sent remotely at the point of access, these remote logs can then be reconciled with local data to identify tampered and altered files. The logs can also be used as evidence in any subsequent prosecution.

Audit:

Ensure that the log entries have been added successfully:

```
tail -2 /etc/syslog.conf
```

The above command should yield the following output:

```
auth.info               @<IP address of remote syslog server>
*.info;auth.none        @<IP address of remote syslog server>
```

Remediation:

Explicitly define a remote host for auth.info data in `/etc/syslog.conf` (enter the remote host IP address in the example below):

```
printf "auth.info\t\t@<IP address of remote syslog server>\n" >> \
/etc/syslog.conf
```

NOTE: This ensures that remote login, `sudo` or `su` attempts are logged separately

Create a remote host entry in `/etc/syslog.conf` to capture all other output of level info or higher (enter the remote host IP address in the example below):

```
printf "*.info;auth.none\t@<IP address of remote syslog server>\n" >> \
/etc/syslog.conf
```

Refresh `syslogd` to force the daemon to read the edited `/etc/syslog.conf`:

```
refresh -s syslogd
```

4.1.3 Configuring syslog - remote messages (Scored)

Profile Applicability:

- Level 2

Description:

This recommendation prevents the local `syslogd` daemon from accepting messages from other hosts on the network.

Rationale:

Apart from a central `syslog` server, all other hosts should not accept remote `syslog` messages. By default the `syslogd` daemon accepts all remote syslog messages as no authentication is required. This means that a hacker could flood a server with `syslog` messages and potentially fill up the `/var` filesystem.

Audit:

Ensure that daemon is running with the newly updated configuration:

```
ps -ef |grep "syslogd"
```

The above command should yield output similar to the following:

```
root  57758  70094   0 10:22:08      -  0:00 /usr/sbin/syslogd -r
```

NOTE: The -r flag should be present at the end out of the output.

Remediation:

If the server does not act as a central `syslog` server, suppress the logging of messages originating from remote servers:

```
chssys -s syslogd -a "-r"
```

Re-cycle `syslogd` to activate the configuration change:

```
stopsrc -s syslogd
startsrc -s syslogd
```

4.2 Secure Remote Access

The use of SSH provides a secure and encrypted mechanism for connecting to a UNIX server. The recommendations in this benchmark disable clear text password access methods, such as telnet and rlogin. There are many legacy scenarios where telnet and ftp may still be required, but SSH should not be ignored in these situations and used where ever possible alongside the non-encrypted services. The preferred scenario is that SSH is the only available remote access service.

One of the historical issues relating to the use of OpenSSH was the lack of vendor support for the software. This has now been addressed as it has the full support, and is in fact packaged, by IBM for AIX based on the Open source libraries.

This section of the benchmark will focus on the installation and configuration of SSH. Some of the parameters specified in this section are actually the default values, but explicit declaration is preferred, to ensure that these recommendations remain constant over time.

4.2.1 Configuring SSH - installation (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to install OpenSSHand OpenSSL libraries from the expansion pack media, or the IBM supported packages downloaded from the internet.

Rationale:

This is the preferred mechanism for remote client access as it provides socket level encryption, via OpenSSL. If any clear text password service is required for legacy connections the two services may sit side by side, with SSH utilized wherever possible. Ideally, SSH should be the only available remote access mechanism.

If the software is not available from the expansion pack media, download from the following locations.

OpenSSH:

http://sourceforge.net/projects/openssh-aix/files/?source=navbar

OpenSSL:

https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=aixbp

NOTE: A login is required to download OpenSSL.

If the Secure By Default option was selected when installing AIX, both SSH and SSL will already have been installed as part of this process.

Audit:

Validate the installation of the software:

```
lslpp -L |egrep "openssh|ssl"
```

The above command should yield the following output:

```
 openssh.base.client     4.3.0.5300    C     F    Open Secure Shell Commands
  openssh.base.server     4.3.0.5300    C     F    Open Secure Shell Server
  openssh.license         4.3.0.5300    C     F    Open Secure Shell License
  openssh.msg.en_US       4.3.0.5300    C     F    Open Secure Shell Messages
  openssl.base             0.9.8.601    C     F    Open Secure Socket Layer
  openssl.license          0.9.8.601    C     F    Open Secure Socket License
  openssl.man.en_US        0.9.8.601    C     F    Open Secure Socket Layer
  openssl                   0.9.7g-1    C     R    Secure Sockets Layer and
```

NOTE: The version numbers may differ based on the source of the software

Ensure that the SSH daemon is set to automatically start during system IPL:

```
ls -l /etc/rc.d/rc2.d/Ssshd | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-r-xr-xr-x   root     system          Ssshd
```

Remediation:

Place the OpenSSH and OpenSSL software into a convenient location, such as `/tmp` and install via:

```
/usr/lib/instl/sm_inst installp_cmd -a -Q -d /tmp -f
openssl,openssh.license,openssh.base,openssh.man.en_US,openssh.msg.en_US -c -
N -g -X -G -Y
```

NOTE: If the software is not located in `/tmp`, reflect the actual location in the command above.

4.2.2 Configuring SSH - disabling direct root access (Scored)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file to disable direct root login. By default direct root login via SSH is enabled.

Rationale:

All root access should be facilitated through a local logon with a unique and identifiable user ID and then via the `su` command once locally authenticated. Direct root login is extremely insecure and offers little in the way of audit trailing for accountability.

Audit:

Ensure that the `PermitRootLogin` parameter has been changed:

```
grep "^PermitRootLogin[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
PermitRootLogin no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file and disable direct root login for SSH:

```
vi /etc/ssh/sshd_config
```

Replace:

```
#PermitRootLogin yes
```

With:

```
PermitRootLogin no
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.3 Configuring SSH - server protocol 2 (Scored)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file and allow the SSH2 protocol only. By default the SSH1 protocol is also available. This is the SSH server configuration file.

Rationale:

There are publicly known vulnerabilities in SSH1 protocol, because of which the SSH1 protocol was deprecated in early 2001. SSH2 is a complete re-write of SSH1 with additional security features. All SSH connections should communicate over the SSH2 protocol. There are numerous benefits of utilizing SSH2 over SSH1, these include: an enhanced and stronger crypto integrity check and support for RSA and DSA keys, rather than just RSA key support in SSH1. The recommendation is to edit the `/etc/ssh/sshd_config` file and allow the SSH2 protocol only.

Audit:

Ensure that the `Protocol` parameter has been changed:

```
grep "^Protocol[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
Protocol 2
```

Remediation:

Edit the`/etc/ssh/sshd_config` file and explicitly define the SSH2 protocol:

```
vi /etc/ssh/sshd_config
```

Replace:

```
#Protocol 2,1
```

With:

```
Protocol 2
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.4 Configuring SSH - client protocol 2 (Scored)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the `/etc/ssh/ssh_config` file and allow the SSH2 protocol only. By default the SSH1 protocol is also available. This is the SSH client configuration file.

Rationale:

There are publicly known vulnerabilities in SSH1 protocol, because of which the SSH1 protocol was deprecated in early 2001. SSH2 is a complete re-write of SSH1 with additional security features. All SSH connections should communicate over the SSH2 protocol. There are numerous benefits of utilizing SSH2 over SSH1, these include: an enhanced and stronger crypto integrity check and support for RSA and DSA keys, rather than just RSA key support in SSH1. The recommendation is to edit the `/etc/ssh/ssh_config` file and allow the SSH2 protocol only.

Audit:

Ensure that the `Protocol` parameter has been changed:

```
grep "^Protocol[[:blank:]]" /etc/ssh/ssh_config
```

The above command should yield the following output:

```
Protocol 2
```

Remediation:

Edit the`/etc/ssh/ssh_config` file and explicitly define the SSH2 protocol:

```
vi /etc/ssh/sshd_config
```

Replace:

```
#Protocol 2,1
```

With:

```
Protocol 2
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.5 Configuring SSH - banner configuration (Scored)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file and configure a path to a login herald message.

Rationale:

The login herald configured previously is not displayed during the initiation of a new SSH connection. Prior to a password being entered the user should accept the terms and conditions of the corporate acceptable usage policy.

Audit:

Ensure that the `Banner` parameter has been changed:

```
grep "^Banner[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
Banner /etc/ssh/ssh_banner
```

Remediation:

Create an SSH banner file:

```
printf "Unauthorized use of this system is prohibited.\n" >
/etc/ssh/ssh_banner
```

NOTE: The content of the banner file can reflect any internal acceptable usage policy standards

Edit the `/etc/ssh/sshd_config` file and customize the `Banner` parameter

```
vi /etc/ssh/sshd_config
```

Replace:

```
#Banner /some/path
```

With:

```
Banner /etc/ssh/ssh_banner
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.6 Configuring SSH - ignore .shosts and .rhosts (Scored)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file and set the `IgnoreRhosts`parameter to ignore `.shosts` and `.rhosts` files.

Rationale:

A user can logon to a remote system without authenticating themselves if `.rhosts` or `.shosts` files exist in the remote home directory and if the client machine name and user name are present in these files. This method is fundamentally insecure as the local system can be exploited by IP, DNS (Domain Name Server) and routing spoofing attacks. Additionally, this authentication method relies on the integrity of the client machine. These weaknesses have been known and exploited for a long time. Since this authentication method is not secure, it must be disabled.

Audit:

Ensure that the `IgnoreRhosts` parameter has been changed:

```
grep "^IgnoreRhosts[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
IgnoreRhosts yes
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to disable the `.shosts` and `.rhosts` authentication parameter:

```
vi /etc/ssh/sshd_config
```

Replace:

```
#IgnoreRhosts yes
```

With:

```
IgnoreRhosts yes
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.7 Configuring SSH - disable null passwords (Scored)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file to ensure that the SSH daemon does not authenticate users with a null password.

Rationale:

If password authentication is used and an account has an empty password, the SSH server must be configured to disallow access to the account. Permitting empty passwords could create an easy path of access for hackers to enter the system.

Audit:

Ensure that the `PermitEmptyPasswords` parameter has been changed:

```
grep "^PermitEmptyPasswords[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
PermitEmptyPasswords no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to disable the acceptance null passwords:

```
vi /etc/ssh/sshd_config
```

Replace:

```
#PermitEmptyPasswords no
```

With:

```
PermitEmptyPasswords no
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.8 Configuring SSH - disallow host based authentication (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file to ensure that host-based authentication is disallowed.

Rationale:

Using host-based authentication, any user on a trusted host can log into another host on which this feature is enabled. Since this feature depends only on system authentication and not on user authentication, it must be disabled.

Audit:

Ensure that the `HostbasedAuthentication` parameter has been changed:

```
grep "^HostbasedAuthentication[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
HostbasedAuthentication no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to ensure that host based authentication is disallowed:

```
vi /etc/ssh/sshd_config
```

Replace:

```
#HostbasedAuthentication no
```

With:

```
HostbasedAuthentication no
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.9 Configuring SSH - set privilege separation (Scored)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file to ensure that privilege separation is enabled.

Rationale:

Setting privilege separation helps to secure remote `ssh` access. Once a user is authenticated the `sshd` daemon creates a child process which has the privileges of the authenticated user and this then handles incoming network traffic. The aim of this is to prevent privilege escalation through the initial root process.

Audit:

Ensure that the `UsePrivilegeSeparation` parameter has been changed:

```
grep "^UsePrivilegeSeparation[[:blank:]]" /etc/ssh/sshd_config
```

The above command **must not** yield the following output:

```
UsePrivilegeSeparation no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to ensure that privilege separation is enabled:

```
vi /etc/ssh/sshd_config
```

Replace:

```
UsePrivilegeSeparation no
```

With:

```
UsePrivilegeSeparation yes
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.10 Configuring SSH - removal of .shosts files (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to remove any existing `.shosts` files from all user home directories.

Rationale:

The existence of `.shosts` files in a user home directory, combined with the correct SSH parameter can allow passwordless authentication between servers. As previous recommendations in this section disable this authentication method, these files, if they exist, should be removed.

Audit:

Ensure that the all of the `.shost` files have been successfully removed:

```
find / -name ".shosts" -print
```

The above command should yield no output.

Remediation:

List out all of the existing `.shost` files:

```
find / -name ".shosts" -print
```

Review the list of `.shost` files and remove them individually, or all at once:

Individually:

```
rm (full pathname)
```

All at once:

```
find / -name ".shosts" -exec rm {} \;
```

4.2.11 Configuring SSH - removal of /etc/shosts.equiv (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to remove the `/etc/shosts.equiv` file.

Rationale:

The existence of a `/etc/shosts.equiv` file, combined with the correct SSH parameter can allow passwordless authentication between servers. As previous recommendations in this section disable this authentication method these files, if they exist, should be removed.

Audit:

Ensure that the `/etc/shosts.equiv` file has been successfully removed:

```
ls /etc/shosts.equiv
```

The above command should yield no output.

Remediation:

Review the content of the /`etc/shosts.equiv` file:

```
cat /etc/shosts.equiv
```

If the file exists:

```
rm /etc/shosts.equiv
```

4.2.12 Configuring SSH - set LogLevel to INFO (Scored)

Profile Applicability:

- Level 1

Description:

The `INFO` parameter specifices that record login and logout activity will be logged.

Rationale:

SSH provides several logging levels with varying amounts of verbosity. `DEBUG` is specifically *not* recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information. `INFO` level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

Audit:

Ensure that the `LogLevel` parameter is set to INFO:

```
grep "^LogLevel[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
LogLevel INFO
```

Remediation:

Edit the `/etc/ssh/sshd_config`:

```
vi /etc/ssh/sshd_config
```

Set:

```
LogLevel INFO
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.13 Configuring SSH - set MaxAuthTries to 4 or Less (Scored)

Profile Applicability:

- Level 1

Description:

The `MaxAuthTries` parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the `syslog` file detailing the login failure.

Rationale:

Setting the `MaxAuthTries` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, it is set the number based on site policy.

Audit:

Ensure that the `MaxAuthTries` parameter is set as recommended:

```
grep "^MaxAuthTries[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
MaxAuthTries 4
```

Remediation:

Edit the `/etc/ssh/sshd_config` file:

```
vi /etc/ssh/sshd_config
```

Set:

```
MaxAuthTries 4
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.14 Configuring SSH - set Idle Timeout Interval for User Login (Scored)

Profile Applicability:

- Level 1

Description:

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of ssh sessions. When the `ClientAliveInterval` variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the `ClientAliveCountMax` variable is set, `sshd` will send client alive messages at every `ClientAliveInterval` interval. When the number of consecutive client alive messages are sent with no response

from the client, the `ssh` session is terminated. For example, if the `ClientAliveInterval` is set to 15 seconds and the `ClientAliveCountMax` is set to 3, the client `ssh` session will be terminated after 45 seconds of idle time.

Rationale:

Having no timeout value associated with a connection could allow an unauthorized user access to another user's `ssh` session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening..

While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for `ClientAliveCountMax` is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Audit:

Ensure that the `ClientAliveCountMax` parameter is set as recommended:

```
grep "^ClientAliveCountMax[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
ClientAliveCountMax 300
```

Ensure that the `ClientAliveInterval` parameter is set as recommended:

```
grep "^ClientAliveInterval[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
ClientAliveInterval 0
```

Remediation:

Edit the `/etc/ssh/sshd_config` file:

```
vi /etc/ssh/sshd_config
```

Set:

```
ClientAliveCountMax 300
ClientAliveInterval 0
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.15 Configuring SSH - restrict Cipher list (Scored)

Profile Applicability:

- Level 1

Description:

This variable limits the types of ciphers that SSH can use during communication.

Rationale:

Based on research conducted at various institutions, it was determined that the symmetric portion of the SSH Transport Protocol (as described in RFC 4253) has security weaknesses that allowed recovery of up to 32 bits of plaintext from a block of ciphertext that was encrypted with the Cipher Block Chaining (CBD) method. From that research, new Counter mode algorithms (as described in RFC4344) were designed that are not vulnerable to these types of attacks and these algorithms are now recommended for standard use.

Audit:

Ensure that the `Ciphers` parameter is set as recommended:

```
grep "^Ciphers [[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
```

Remediation:

Edit the `/etc/ssh/sshd_config` file:

```
vi /etc/ssh/sshd_config
```

Set:

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

References:

1. For more information on the Counter mode algorithms, read RFC4344 at http://www.ietf.org/rfc/rfc4344.txt.

4.2.16 Configuring SSH - ignore user-provided environment variables (Scored)

Profile Applicability:

- Level 1

Description:

The `PermitUserEnvironment` option allows users to present environment options to the `ssh` daemon.

Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has `ssh` executing trojan'd programs)

Audit:

Ensure that the `PermitUserEnvironment` parameter has been changed:

```
grep "^PermitUserEnvironment[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
PermitUserEnvironment no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file:

```
vi /etc/ssh/sshd_config
```

Set:

```
PermitUserEnvironment no
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.17 Configuring SSH - limit access via SSH (Scored)

Profile Applicability:

- Level 1

Description:

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least of the following options be leveraged:

`AllowUsers`

The `AllowUsers` variable gives the system administrator the option of allowing specific users to `ssh` into the system. The list consists of comma separated user names. Numeric userIDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.

`AllowGroups`

The `AllowGroups` variable gives the system administrator the option of allowing specific groups of users to `ssh` into the system. The list consists of comma separated group names. Numeric groupIDs are not recognized with this variable.

`DenyUsers`

The `DenyUsers` variable gives the system administrator the option of denying specific users to `ssh` into the system. The list consists of comma separated user names. Numeric userIDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.

`DenyGroups`

The `DenyGroups` variable gives the system administrator the option of denying specific groups of users to `ssh` into the system. The list consists of comma separated group names. Numeric groupIDs are not recognized with this variable.

Rationale:

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Audit:

Ensure that the `AllowUsers`, `AllowGroups`, `DenyUsers`, or `DenyGroups` is set:

```
grep "^(AllowUsers|AllowGroups|DenyUsers|DenyGroups)[[:blank:]]"
/etc/ssh/sshd_config
```

The above command should yield one of the following output:

```
AllowUsers <userlist> AllowGroups <grouplist> DenyUsers <userlist> DenyGroups
<grouplist>
```

Remediation:

Edit the `/etc/ssh/sshd_config` file:

```
vi /etc/ssh/sshd_config
```

Set one of the following:

```
AllowUsers <userlist>
AllowGroups <grouplist>
DenyUsers <userlist>
DenyGroups <grouplist>
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```

4.2.18 Configuring SSH - sshd_config permissions lockdown (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/ssh/sshd_config` file defines SSH server behavior.

Rationale:

The SSH daemon reads the configuration information from this file and includes the authentication mode and cryptographic levels to use during SSH communication. The recommended value is not to provide any access rights for any user, other than the owner of the file.

Audit:

Ensure that the `/etc/ssh/sshd_config` permissions have been successfully changed:

```
ls -l /etc/ssh/sshd_config | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw------- root system /etc/ssh/sshd_config
```

Remediation:

Change the permissions of the `/etc/ssh/sshd_config` file to ensure that only the owner can read and write to the file:

```
chmod u=rw,go= /etc/ssh/sshd_config
```

4.2.19 Configuring SSH - ssh_config permissions lockdown (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/ssh/sshd_config` file defines SSH client behavior.

Rationale:

The `/etc/ssh/ssh_config` file is the system-wide client configuration file for OpenSSH, which allows you to set options that modify the operation of the client programs. The

recommended value is not to provide any writable access rights for any user, other than the owner of the file.

Audit:

Ensure that the `/etc/ssh/ssh_config` permissions have been successfully changed:

```
ls -l /etc/ssh/ssh_config | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r--r-- root system /etc/ssh/ssh_config
```

Remediation:

Change the permissions of the `/etc/ssh/ssh_config` file to ensure that only the owner can read and write to the file:

```
chmod u=rw,go=r /etc/ssh/ssh_config
```

4.3 Sendmail Configuration

During the implementation of the default customized aixpert XML file the sendmail daemon will have been disabled. However, if the sendmail service is active and required in the environment, the recommendations in this section should be applied.

4.3.1 /etc/mail/sendmail.cf - SmtpGreetingMessage (Scored)

Profile Applicability:

- Level 1

Description:

The recommendation is to change the default `sendmail` greeting string to not display the `sendmail` version and other related information.

Rationale:

The `sendmail` deamon has a history of security vulnerabilities. The recommendation is to change the default `sendmail` greeting string so as not to display the sendmail version and other related information, which can be used by an attacker for fingerprinting purposes.

Audit:

Validate the installation of the software:

```
grep "SmtpGreetingMessage=mailerready" /etc/mail/sendmail.cf
```

The above command should yield the following output:

```
O SmtpGreetingMessage=mailerready
```

Remediation:

Create a backup copy of `/etc/mail/sendmail.cf`:

```
cp -p /etc/mail/sendmail.cf /etc/mail/sendmail.cf.pre_cis
```

Edit:

```
vi /etc/mail/sendmail.cf
```

Change:

```
O SmtpGreetingMessage=$j Sendmail $b
```

To:

```
O SmtpGreetingMessage=mailerready
```

4.3.2 /etc/mail/sendmail.cf - permissions and ownership (Scored)

Profile Applicability:

- Level 1

Description:

The recommended permissions and ownership for `/etc/mail/sendmail.cf` are applied.

Rationale:

The `/etc/mail/sendmail.cf` file is used by the `sendmail` daemon to determine its default configuration. This file must be protected from unauthorized access and modifications.

Audit:

From the command prompt, execute the following command:

```
ls -l /etc/mail/sendmail.cf | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r----- root system sendmail.cf
```

Remediation:

Set the recommended permissions and ownership on `/etc/mail/sendmail.cf`:

```
chmod u=rw,g=r,o= /etc/mail/sendmail.cf
chown root /etc/mail/sendmail.cf
```

4.3.3 /var/spool/mqueue - permissions and ownership (Scored)

Profile Applicability:

- Level 1

Description:

The recommended permissions and ownership for the `/var/spool/mqueue` directoryare applied.

Rationale:

The `sendmail` daemon generally stores its queued mail in the `/var/spool/mqueue` directory. Queued messages are the messages that have not yet reached their final destination. To ensure the integrity of the messages during storage, the mail queue directory must be secured from unauthorized access.

NOTE: It is possible to specify an alternate spool directory in the `/etc/mail/sendmail.cf` file via the `QueueDirectory` parameter.

Audit:

From the command prompt, execute the following command:

```
ls -ld /var/spool/mqueue | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwx------    root     system          /var/spool/mqueue
```

Remediation:

Set the recommended permissions and ownership on `/var/spool/mqueue`:

```
chmod u=rwx,go= /var/spool/mqueue
chown root /var/spool/mqueue
```

4.4 Common Desktop Environment (CDE)

During the implementation of the default customized aixpert XML file, CDE will have been disabled as the /etc/rc.dt startup file will have been removed from /etc/inittab.

CDE has a history of security problems and should remain disabled. However, if the server has a graphics adapter and CDE is used then the recommendations in this section should be followed to enhance security. If CDE is not required and the filesets are installed, is recommended that the filesets are de-installed to avoid exposure to potential security vulnerabilities.

4.4.1 CDE - de-installing CDE (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to de-install CDE from the system, assuming that it is not required and is already installed.

Rationale:

CDE has a history of security problems and should be disabled.

NOTE: If CDE is required, it is vital to patch the software and consider TCP Wrappers to further enhance security.

Audit:

Validate the de-installation of the software:

```
lslpp -L |grep -i CDE
```

The above command should yield no output.

Remediation:

Identity if CDE is already installed:

```
lslpp -L |grep -i CDE
```

If there are CDE filesets installed - de-install them if CDE is not required.
For each fileset preview the de-installation:

```
installp -up <fileset name>
```

Review the fileset removal preview output, paying particular attention to the other pre-requisites that will also be removed. Typically only `X11.Dt` filesets should be de-installed as pre-requisites.
Once reviewed, de-install the fileset and pre-requisites:

```
installp -ug <fileset name>
```

NOTE: Repeat until all CDE filesets are de-installed

4.4.2 CDE - disabling dtlogin (Scored)

Profile Applicability:

- Level 2

Description:

Do not start CDE automatically on system boot.

Rationale:

The implementation of the customized aixpert XML file disables CDE if there is not a graphical console attached to the system. If there is a graphical console or the XML file has not been executed, consider disabling CDE anyway.

Audit:

Validate that CDE start-up is disabled

```
lsitab dt
```

The above command should yield no output.

Remediation:

Disable CDE start up:

```
/usr/dt/bin/dtconfig -d
```

NOTE: If CDE is not installed the command will not be found

4.4.3 CDE - sgid/suid binary lockdown (Scored)

Profile Applicability:

- Level 1

Description:

CDE buffer overflow vulnerabilities may be exploited by a local user to obtain root privilege via `suid/sgid` programs owned by `root:bin` or `root:sys`.

Rationale:

CDE has been associated with major security risks, most of which are buffer overflow vulnerabilities. These vulnerabilities may be exploited by a local user to obtain root privilege via `suid/sgid` programs owned by `root:bin` or `root:sys`. It is recommended that the CDE binaries have the `suid/sgid` removed.

Audit:

Validate the permissions of the binaries:

```
ls -l /usr/dt/bin/dtaction | awk '{print $1 " " $3 " " $4 " " $9}'
ls -l /usr/dt/bin/dtappgather | awk '{print $1 " " $3 " " $4 " " $9}'
ls -l /usr/dt/bin/dtprintinfo | awk '{print $1 " " $3 " " $4 " " $9}'
ls -l /usr/dt/bin/dtsession | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-r-xr-xr-x    root     sys          /usr/dt/bin/dtaction
-r-xr-xr-x    root     bin          /usr/dt/bin/dtappgather
-r-xr-xr-x    root     bin          /usr/dt/bin/dtprintinfo
-r-xr-xr-x    root     bin          /usr/dt/bin/dtsession
```

Remediation:

Remove the `suid/sgid` from the following CDE binaries:

```
chmod ug-s /usr/dt/bin/dtaction
chmod ug-s /usr/dt/bin/dtappgather
chmod ug-s /usr/dt/bin/dtprintinfo
chmod ug-s /usr/dt/bin/dtsession
```

4.4.4 CDE - remote GUI login disabled (Scored)

Profile Applicability:

- Level 2

Description:

The XDMCP service allows remote systems to start local X login sessions.

Rationale:

The XDMCP service should be disabled unless there is a requirement to allow remote X servers to start login sessions. If the ability to host remote X servers is not required, disable the service.

Audit:

Validate the change to `/etc/dt/config/Xconfig`:

```
grep "^Dtlogin.requestPort:[[::space::]]" /etc/dt/config/Xconfig
```

The command above should yield the following output:

```
Dtlogin.requestPort:       0
```

Remediation:

Copy `/usr/dt/config/Xconfig` to `/etc/dt/config` if it does not already exist:

```
ls -l /etc/dt/config/Xconfig
```

If the file does not exist, create it:

```
mkdir -p /etc/dt/config
cp /usr/dt/config/Xconfig /etc/dt/config
```

Disable remote X sessions from being started:

```
vi /etc/dt/config/Xconfig
```

Replace:

```
#  Dtlogin.requestPort:       0
```

With:

```
Dtlogin.requestPort:       0
```

4.4.5 CDE - screensaver lock (Scored)

Profile Applicability:

- Level 1

Description:

The default timeout is 30 minutes of keyboard and mouse inactivity before a password protected screensaver is invoked by the CDE session manager.

Rationale:

The default timeout of 30 minutes prior to a password protected screensaver being invoked is too long. The recommendation is to set this to 10 minutes to protect from unauthorized access on unattended systems.

Audit:

Validate the changes to the `sys.resources` files:

```
egrep "dtsession\*saverTimeout:|dtsession\*lockTimeout:"
/etc/dt/config/*/sys.resources
```

The above command should yield a similar output to the following:

```
/etc/dt/config/en_US/sys.resources:dtsession*saverTimeout:  10
/etc/dt/config/en_US/sys.resources:dtsession*lockTimeout:   10
```

Remediation:

Set the default timeout parameters `dtsession*saverTimeout:` and `dtsession*lockTimeout:`

```
for file in /usr/dt/config/*/sys.resources; do
   dir=`dirname $file | sed -e s/usr/etc/`
   mkdir -p $dir
   echo 'dtsession*saverTimeout: 10' >> $dir/sys.resources
   echo 'dtsession*lockTimeout: 10' >> $dir/sys.resources
done
```

4.4.6 CDE - login screen hostname masking (Scored)

Profile Applicability:

- Level 1

Description:

The `Dtlogin*greeting.labelString` parameter is the message displayed in the first dialogue box on the CDE login screen. This is where the username is entered.

The `Dtlogin*greeting.persLabelString` is the message displayed in the second dialogue box on the CDE login screen. This is where the password is entered.

Rationale:

Potential hackers may gain access to valuable information such as the hostname and the version of the operating system from the default AIX login screen. This information would assist hackers in choosing the exploitation methods to break into the system. For security reasons, change the login screen default messages.

Audit:

Validate the changes to the `Xresources` files:

```
egrep "Dtlogin\*greeting.labelString|Dtlogin\*greeting.persLabelString:"
/etc/dt/config/*/Xresources
```

The above command should yield a similar output to the following:

```
/usr/dt/config/en_US/Xresources:!! Dtlogin*greeting.labelString: Authorized
uses only. All activity may be monitored and reported.
/usr/dt/config/en_US/Xresources:!! Dtlogin*greeting.persLabelString:
Authorized uses only. All activity may be monitored and reported.
```

Remediation:

Copy the files from `/usr/dt/config/*/Xresources` to `/etc/dt/config/*/Xresources` and add the `Dtlogin*greeting.labelString` and `Dtlogin*greeting.persLabelString` parameters to all copied `Xresources` files:

```
for file in /usr/dt/config/*/Xresources; do
dir=`dirname $file | sed s/usr/etc/`
mkdir -p $dir
if [ ! -f $dir/Xresources ]; then
cp $file $dir/Xresources
fi
WARN="Authorized uses only. All activity may be monitored and
reported."
echo "Dtlogin*greeting.labelString: $WARN" >>$dir/Xresources
echo "Dtlogin*greeting.persLabelString: $WARN" >>$dir/Xresources
done
```

4.4.7 CDE - /etc/dt/config/Xconfig permissions and ownership (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/dt/config/Xconfig` file is used to customize CDE DT login attributes. Ensure this file is owned by `root:bin`and permissions prevent `group` and `other` from writing to the file.

Rationale:

The `/etc/dt/config/Xconfig` file can be used to customize CDE DT login attributes. The default file, `/usr/dt/config/Xconfig`, is unconditionally overwritten upon subsequent installation. It is recommended that the appropriate permissions and ownership are applied to secure the file.

Audit:

Validate the ownership and permissions:

```
ls -l /etc/dt/config/Xconfig| awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-r--r--r--  root      bin           /etc/dt/config/Xconfig
```

Remediation:

Check to see if the `/etc/dt/config/Xconfig` exists:

```
ls -l /etc/dt/config/Xconfig
```

Apply the appropriate ownership and permissions to `/etc/dt/config/Xconfig`:

```
chown root:bin /etc/dt/config/Xconfig
chmod go-w /etc/dt/config/Xconfig
```

4.4.8 CDE - /etc/dt/config/Xservers permissions and ownership (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/dt/config/Xservers` contains entries to start the Xserver on the local display. Ensure this file is owned by `root:bin` and prevents `group` and `other` from writing to it.

Rationale:

The `/etc/dt/config/Xservers` contains entries to start the Xserver on the local display. The default file, `/usr/dt/config/Xservers`, is unconditionally overwritten upon subsequent installation. It is recommended that the appropriate permissions and ownership are applied to secure the file.

Audit:

Validate the ownership and permissions:

```
ls -l /etc/dt/config/Xservers | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-r--r--r--  root      bin           /etc/dt/config/Xservers
```

Remediation:

Check to see if the `/etc/dt/config/Xservers` exists:

```
ls -l /etc/dt/config/Xservers
```

If it exists ensure that it is explicitly defined in `/etc/dt/config/Xconfig`:

```
vi /etc/dt/config/Xconfig
```

Replace:

```
Dtlogin.servers:               Xservers
```

With:

```
Dtlogin*servers: /etc/dt/config/Xservers
```

Apply the appropriate ownership and permissions to `/etc/dt/config/Xservers`:

```
chown root:bin /etc/dt/config/Xservers
chmod go-w /etc/dt/config/Xservers
```

4.4.9 CDE - /etc/dt/config//Xresources permissions and ownership (Scored)*

Profile Applicability:

- Level 1

Description:

The `/etc/dt/config/*/Xresources` file contains appearance and behavior resources for the `Dtlogin` login screen.

Rationale:

The `/etc/dt/config/*/Xresources` file defines the customization of the `Dtlogin` screen. The default file, `/usr/dt/config/*/Xresources`, is unconditionally overwritten upon subsequent installation. It is recommended that the appropriate permissions and ownership are applied to secure the file.

Audit:

Validate the ownership and permissions:

```
ls -l /etc/dt/config/*/Xresources | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield a similar output to the following:

```
-rw-r--r-- root sys /etc/dt/config/en_GB/Xresources
-rw-r--r-- root sys /etc/dt/config/en_US/Xresources
```

Remediation:

Set the appropriate permissions and ownership on all `Xresources` files:

```
chown root:sys /etc/dt/config/*/Xresources
chmod u=rw,go=r /etc/dt/config/*/Xresources
```

4.5 NFS

During the implementation of the default customized aixpert XML file, NFS services will have been disabled as the /etc/rc.nfs startup file will have been removed from /etc/inittab.

The first recommendation in this section is to de-install NFS to complete the lockdown of this service. However, if the server acts as either an NFS server or NFS client there are further security recommendations to implement.

4.5.1 NFS - de-install NFS client (Scored)

Profile Applicability:

- Level 2

Description:

De-install NFS client if the server does not remotely mount NFS shares.

Rationale:

NFS is frequently exploited to gain unauthorized access to file and directories. Unless the server needs to act as an NFS server or client, the filesets should be de-installed.

Audit:

Ensure that the software has been successfully de-installed:

```
lslpp -L |grep bos.net.nfs.client
```

The above command should yield no output.

Remediation:

Ensure that there are no current NFS client mounts:

```
mount |grep "nfs"
cat /etc/filesystems |grep "nfs"
```

The above commands should yield no output.

De-install the NFS client software:

```
installp -u bos.net.nfs.client
```

4.5.2 NFS - de-install NFS server (Scored)

Profile Applicability:

- Level 2

Description:

De-install NFS server if the server does not act as an NFS server to remote clients.

Rationale:

NFS is frequently exploited to gain unauthorized access to file and directories. Unless the server needs to act as an NFS server or client, the filesets should be de-installed.

Audit:

Ensure that the software has been successfully de-installed:

```
lslpp -L |grep bos.net.nfs.server
```

The above command should yield no output.

Remediation:

Ensure that there are no current NFS exports:

```
cat /etc/exports
```

The above command should yield no output. Or the file should not exist.

De-install the NFS sever software:

```
installp -u bos.net.nfs.server
```

If there was an empty `/etc/exports` file, remove it:

```
rm /etc/exports
```

4.5.3 NFS - nosuid on NFS client mounts (Scored)

Profile Applicability:

- Level 1

Description:

Disable suid/sgid program execution within any mounted NFS filesystem.

Rationale:

Setting the `nosuid` option means that on the NFS server the root user cannot make an suid-root program within an exported filesystem. Then log onto an NFS client as a standard user and use the suid-root program to effectively become root on that client.

Audit:

For each NFS filesystem, ensure that the options have been changed to reflect the `nosuid` option:

```
mount |grep "nfs" |wc -l
mount |grep "nfs" |grep "nosuid" |wc -l
```

Both commands should yield the same output.

Remediation:

For each NFS mount, disable suid programs.
List the current NFS mounts:

```
mount |grep "nfs"
```

For each NFS filesystem add the nosuid option, this change should be made via an edit to the `/etc/filesystems` file.
Create a copy of `/etc/filesystems`:

```
cp -p /etc/filesystems /etc/filesystems.pre_cis
```

For each NFS mount edit the options line to reflect the nosuid option:

```
vi /etc/filesystems
```

Reflect in each NFS options line:

```
options = rw,bg,hard,intr,nosuid,sec=sys
```

NOTE: The above options line is an example, the nosuid should be added to the existing options
The NFS mount needs to be re-mounted to reflect this change

4.5.4 NFS - localhost removal (Scored)

Profile Applicability:

- Level 1

Description:

Remove any reference to localhost or localhost aliases from `/etc/exports`.

Rationale:

If the RPC portmapper has proxy forwarding enabled, which is a default setting in many vendor versions. You must not export your local filesytems back to the localhost, either by name or to the alias localhost, and you must not export to any netgroups of which your host is a member. If proxy forwarding is enabled, an attacker may carefully craft NFS packets and send them to the portmapper, which in turn, forwards them to the NFS server. As the packets come from the portmapper process, which runs as root, they appear to be coming from a trusted system. This configuration may allow anyone to alter and delete files at will.

Audit:

Re-review `/etc/exports` if the file was updated, to validate the changes:

```
cat /etc/exports
```

Remediation:

Remove any reference to localhost or localhost aliases in `/etc/exports`:
Review the content of `/etc/exports` and check for localhost or localhost aliases:

```
cat /etc/exports
```

NOTE: If instances of localhost or localhost aliases are found, edit the file and remove them.
Create a copy of `/etc/exports`:

```
cp -p /etc/exports /etc/exports.pre_cis
```

Edit the file:

```
vi /etc/exports
```

Edit the relevant NFS exports to remove the localhost access, for example:

```
/nfsexport sec=sys,rw,access=localhost:testserver
```

If `/etc/exports` is updated, as localhost references have been removed, update the current NFS export options:

```
exportfs -a
```

4.5.5 NFS - restrict NFS access (Scored)

Profile Applicability:

- Level 2

Description:

Only allow explicitly defined host access to NFS exported filesystems and directories.

Rationale:

The NFS server should be configured to only allow explicitly defined hosts to mount filesystems from the server. If an unauthorized host is denied the permission to mount a

filesystem, then the unauthorized users on that host will not be able to access the server's files.

The default value of access allows any machine to mount any exported filesystems/directories.

Audit:

Re-review `/etc/exports` if the file was updated, to validate the changes:

```
cat /etc/exports
```

Remediation:

Ensure that all exports defined in `/etc/exports` have explicit client access options which clearly define the host or hosts allowed access:
Review the content of `/etc/exports` and that all exports have explicit access lists:

```
cat /etc/exports
```

Ensure that each NFS export has an explicit access line, for example:

```
/usr/spool/mail -access=symmachine
```

If the file is updated, to reflect client access changes, update the current NFS export options:

```
exportfs -a
```

4.5.6 NFS - no_root_squash option (Scored)

Profile Applicability:

- Level 1

Description:

For each NFS export, ensure that the root_squash option is set to -2 or -1.

Rationale:

Each NFS export on the server should have the `anon=-2` option set. Without this, an NFS export could be at risk, where the remote root user effectively has root access on the NFS mount. By setting the export option `anon=-2` , when the client attempts to access (read, write, or delete) the NFS mount, the server substitutes the UID to the server's nobody

account, which is -2. This means that the root user on the client cannot access or change files that only root on the server can access or change. It is therefore recommended that root_squash is set on all exported filesystems.
The default value of any exported filesystem or directory is -2, another value has to be explicitly set.
As a more secure option you can set the option to `anon=-1`, which disables anonymous access. By default, secure NFS accepts non-secure requests as anonymous.
NOTE: The root user on the client can still use `su` to become any other user and access and change that users files, assuming that the same user exists on the NFS server and owns files and/or directories in the NFS export.

Audit:

As -2 is the default NFS export value, ensure that there are no explicit `anon=` options set in `/etc/exports`:

```
grep "anon=" /etc/exports
```

The above should command should yield no output.

Remediation:

Use smitty to change/validate this value for all NFS exported filesystems:

```
smitty chnfsexp
```

For each filesystem, as defined in the F4 list, set the following option:

```
Anonymous UID [-2]
```

NOTE: Press enter to accept the change
Once all exported filesystems have been successfully validated or changed, re-export the filesystems and directories to activate the new options:

```
exportfs -a
```

4.5.7 NFS - secure NFS (Scored)

Profile Applicability:

- Level 2

Description:

For each NFS export, ensure that the secure option is selected.

Rationale:

Secure NFS uses DES encryption or Kerberos to authenticate hosts involved in RPC transactions. RPC is a protocol used by NFS to communicate requests between hosts. Secure NFS mitigates attempts by an attacker to spoof RPC requests by encrypting the time stamp in the RPC requests. A receiver successfully decrypts the time stamp and confirms that it is correct. This serves as a confirmation that the RPC request came from a trusted host.

Audit:

Ensure that the relevant `sec=` options set in `/etc/exports`:

```
grep "sec=" /etc/exports
```

The above should command should return each export and the security mode of the export.

Remediation:

Use smitty to change/validate this value for all NFS exported filesystems:

```
smitty chnfsexp
```

For each filesystem, as defined in the F4 list. There are five security methods which can be used to define different security access methods for different clients:

```
Security method 1 [sys,krb5p,krb5i,krb5,d> +
* Mode to export directory read-write +
 Hostname list. If exported read-mostly []
 Hosts & netgroups allowed client access []
 Hosts allowed root access []
```

The security method options are:

```
sys - UNIX authentication
dh - DES authentication
none - Use the anonymous ID if it has a value other than -1
krb5 - Kerberos. Authentication only
krb5i - Kerberos. Authentication and integrity
krb5p - Authentication, integrity, and privacy
```

Once all exported filesystems have been successfully validated or changed, re-export the filesystems and directories to activate the new options:

```
exportfs -a
```

4.6 NIS

Network Information Service (NIS) or Yellow Pages (YP), is a client/server directory service protocol used for distributing system configuration data, such as: users, groups, passwords and hosts between computers in a network. This is typically done in larger environments to centralize the management of this data. If the NIS software is installed but not configured, an attacker can cripple a machine by starting NIS. In environments where NIS is utilized, tools like ypsnarfallow an attacker to grab the contents of your NIS maps, providing large amounts of information about your site.

The first recommendation in this section is to de-install NIS, if it is installed, to lockdown this service. However, if NIS is used in the environment it is recommended that NIS+ is used instead. NIS+ is structured differently from NIS and supports secure and encrypted RPC, which resolves many of the security issues.

The configuration of NIS+ is not within the scope of this benchmark; however the links below can be used for initial reference:

AIX 7.1:

NIS+ transition

4.6.1 NIS - de-install NIS client (Scored)

Profile Applicability:

- Level 2

Description:

If NIS is not used in the environment, disable the NIS client and de-install the software.

Rationale:

As NIS is extremely insecure, the NIS client packages must be removed from the system unless absolutely needed.

Audit:

Ensure that the software has been successfully de-installed:

```
lslpp -L |grep "bos.net.nis.client"
```

The above should command should yield no output.

Remediation:

Ensure that all of the NIS daemons are inactive:

```
stopsrc -g yp
```

De-install the NIS client software:

```
installp -u bos.net.nis.client
```

4.6.2 NIS - de-install NIS server (Scored)

Profile Applicability:

- Level 2

Description:

If NIS is not used in the environment, disable the NIS server and de-install the software.

Rationale:

As NIS is extremely insecure, the NIS server packages must be removed from the system unless absolutely needed.

Audit:

Ensure that the software has been successfully de-installed:

```
lslpp -L |grep "bos.net.nis.server"
```

The above should command should yield no output.

Remediation:

Ensure that all of the NIS daemons are inactive:

```
stopsrc -g yp
```

De-install the NIS server software:

```
installp -u bos.net.nis.server
```

4.6.3 NIS - remove NIS markers from password and group files (Scored)

Profile Applicability:

- Level 2

Description:

If NIS has been de-installed in the environment, or has historically been used, ensure the + markers are removed from `/etc/passwd` and `/etc/group`.

Rationale:

The + entries in `/etc/passwd` and `/etc/group` were used as markers to insert data from a NIS map. These entries may provide an avenue for attackers to gain privileged access on the system. The + entries must be deleted if they still exist.

Audit:

Re-run the command:

```
grep "^+" /etc/passwd /etc/group
```

The command above should yield no output.

Remediation:

Examine the `/etc/passwd` and `/etc/group` files:

```
grep "^+" /etc/passwd /etc/group
```

If the above command yields output, delete the + line:

```
vi /etc/passwd
vi /etc/group
```

4.6.4 NIS - restrict NIS server communication (Scored)

Profile Applicability:

- Level 2

Description:

If NIS must be used in the environment, limit access to the NIS data to specific subnets.

Rationale:

By default the NIS server will authenticate all IP addresses if the `/var/yp/securenets` file does not exist, or exists without any subnets defined. The `/var/yp/securenets` file contains a list of subnets that are considered trusted and are allowed to access NIS data using the `ypserv`and `ypxfrd` daemons. This is a user-created file that resides on a NIS master server and any slave servers. Without configuring this file, anyone with knowledge of the NIS server address and the domain name, can obtain NIS served data, including the contents of the `/etc/passwd`file. Hence, it is recommended that the `/var/yp/securenets` file is configured to restrict access.

Audit:

Review the content of the `/var/yp/securenets` file:

```
cat /var/yp/securenets
```

NOTE: A test should be performed from an allowed client and non-allowed subnet to validate the securenets configuration

Remediation:

Create and secure the `/var/yp/securenets` file (if it does not already exist):

```
touch /var/yp/securenets
chmod u=rw,go= /var/yp/securenets
chown root:system /var/yp/securenets
```

Edit the file:

```
vi /var/yp/securenets
```

Add the allowed subnets:

```
255.255.255.0 128.311.10.0
```

NOTE: The format of the file is netmask netaddr as shown in the example above. Explicitly define all valid network subnets (one entry per line).

Stop and start NIS to implement the configuration changes:

```
stopsrc -g yp
startsrc -g yp
```

4.7 SNMP

The Simple Network Management Protocol (SNMP) is a commonly used service that provides network management and monitoring capabilities. SNMP offers the capability to poll networked devices and monitor data such as utilization and errors from various subsystems on the host. SNMP is also capable of changing the configurations on the host, allowing remote management of the system. The protocol uses a community string for authentication from the SNMP client to the SNMP agent on the managed device.

In AIX, two SNMP community names, private and system, are enabled with read/write privileges, but only allow access from localhost connections. Nevertheless, a local user may install an SNMP client and modify sensitive variables. If SNMP is required, the community strings must be greater than six characters and include a combination of letters, numbers, and special characters to avoid a brute force attack.

4.7.1 SNMP - disable private community string (Scored)

Profile Applicability:

- Level 2

Description:

If `snmpd` is required within the environment, disable the `private` community string.

Rationale:

In AIX, two SNMP community names, `private` and `system`, are enabled with read/write privileges, but are allowed access only from localhost connections. As these SNMP names

are the default, they must not be used. Any SNMP community name should be a combination of letters, numbers and special characters to enhance security.

Audit:

Ensure the `private` entry has been commented out from `/etc/snmpd.conf`:

```
grep "^#community[[:blank:]]*private" /etc/snmpd.conf
```

The above command should yield the following output:

```
#community       private 127.0.0.1 255.255.255.255 readWrite
```

Remediation:

Create a backup of `/etc/snmpd.conf`:

```
cp -p /etc/snmpd.conf /etc/snmpd.conf.pre_cis
```

Edit the file:

```
vi /etc/snmpd.conf
```

Comment out the `private` entry:

```
#community       private 127.0.0.1 255.255.255.255 readWrite
```

4.7.2 SNMP - disable system community string (Scored)

Profile Applicability:

- Level 2

Description:

If `snmpd` is required within the environment, disable the system community string.

Rationale:

In AIX, two SNMP community names, `private` and `system`, are enabled with read/write privileges, but are allowed access only from localhost connections. As these SNMP names

are the default, they must not be used. Any SNMP community name should be a combination of letters, numbers and special characters to enhance security.

Audit:

Ensure the system entry has been commented out from `/etc/snmpd.conf`:

```
grep "^#community[[:blank:]]*system" /etc/snmpd.conf
```

The above command should yield the following output:

```
#community       system  127.0.0.1 255.255.255.255 readWrite 1.17.2
```

Remediation:

Edit the file:

```
vi /etc/snmpd.conf
```

Comment out the system entry:

```
#community       system  127.0.0.1 255.255.255.255 readWrite 1.17.2
```

4.7.3 SNMP - disable public community string (Scored)

Profile Applicability:

- Level 2

Description:

If `snmpd` is required within the environment, disable or change the `public` community string.

Rationale:

The `public` community string can be polled by remote SNMP devices and pertinent information can be read or changed on the host. The `public` community string should but commented out, or if SNMP is a required service the `public` community name should be changed to be a combination of letters, numbers and special characters to enhance security.

Audit:

Ensure the `public` entry has been commented out from `/etc/snmpd.conf`:

```
grep "^#community[[:blank:]]*public" /etc/snmpd.conf
```

The above command should yield the following output:

```
 #community  public
```

Remediation:

Edit the file:

```
vi /etc/snmpd.conf
```

Comment out the `public` entry:

```
#community       public
```

4.7.4 SNMP - disable Readwrite community access (Scored)

Profile Applicability:

- Level 2

Description:

If `snmpd` is required within the environment, disable `readWrite` permissions for all active community strings.

Rationale:

If SNMP is required, none of the available community strings should have global `readWrite` permissions defined. This would allow any remote client to query and to set system configuration parameters. SNMP `readWrite` communities must be disabled unless absolutely necessary. If a `readWrite` community is enabled, then access must be granted to only trusted machines in your network. As SNMP uses community names as part of authentication, you must ensure that all community names are greater than six characters and is a mix of characters, numbers, and special characters.

Audit:

Review the community lines in `/etc/snmpd.conf`:

```
grep "^community[[:blank:]]" /etc/snmpd.conf
```

NOTE: ensure that there is no readWrite access.

Remediation:

Identify if there are any currently configured community strings:

```
grep "^community[[:blank:]]" /etc/snmpd.conf
```

If there are active community strings, edit the configuration file:

```
vi /etc/snmpd.conf
```

Replace all instances of:

```
community <community name> <IP addresses> <netmask> [ readWrite <view>]
```

With:

```
community <community name> <IP addresses> <netmask> [ readOnly <view>]
```

4.7.5 SNMP - restrict community access (Scored)

Profile Applicability:

- Level 2

Description:

If `snmpd` is required within the environment, implement IP access restrictions on the available community strings.

Rationale:

If SNMP is required, IP access restrictions should be put into place to limit which hosts or networks subnets are able to remotely poll the server.

Audit:

Review the available community strings IP access control configuration:

```
grep "^community[[:blank:]]" /etc/snmpd.conf
```

NOTE: validate the allowed IP address and netmasks

Remediation:

Identify if there are any currently configured community strings:

```
grep "^community[[:blank:]]" /etc/snmpd.conf
```

If there are active community strings, edit the configuration file:

```
vi /etc/snmpd.conf
```

Implement IP access restrictions to ALL of the available community names e.g.:

```
community       tivoli  192.132.10.0 255.255.255.0 readOnly
```

The format of each line should reflect:

```
community <community name> <IP addresses> <netmask> [ <permissions> <view>]
```

4.8 Securing inetd

If all inetd services have been disabled and are not required, the inetd daemon itself can be disabled to further enhance security.

4.8.1 inetd - disabling inetd (Scored)

Profile Applicability:

- Level 2

Description:

If all of services run and managed by `inetd` are disabled, disable the `inetd` daemon itself.

Rationale:

If all `inetd` services are disabled, then there is no need to start the daemon at boot time. An administrator can manually start the `inetd` service post-IPL, if any of the `inetd` controlled services are required.

Audit:

Ensure that `inetd` startup has been commented out of `/etc/rc.tcpip`:

```
grep "^#start[[::space::]]/usr/sbin/inetd" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/inetd "$src_running"
```

Remediation:

Review any active `inetd` services:

```
refresh -s inetd
lssrc -ls inetd
```

NOTE: If there are active services and the services are required, do not disable `inetd`. Skip to the next section and consider the implementation of TCP Wrappers to secure access to these active services. If the active services are not required disable them via the `chsubserver` command.

Disable `inetd` if there are no active services:

```
chrctcp -d inetd
stopsrc -s inetd
```

4.9 Portmap Lockdown

The portmap daemon is required for the RPC service. It converts the RPC program numbers into Internet port numbers. The daemon may be disabled if the server is not:

- An NFS client or server
- A NIS (YP) or NIS+ client or server
- Running the CDE GUI
- Running a third-party software application, which is dependent on RPC support

4.9.1 /etc/rc.tcpip - portmap (Scored)

Profile Applicability:

- Level 2

Description:

If all RPC services are disabled, disable the `portmap` daemon itself.

Rationale:

If all RPC services are disabled, then there is no need to start the `portmap` daemon at boot time. An administrator can manually start `portmap` post-IPL, if any of the RPC services are required.

Audit:

Ensure that `portmap` startup has been commented out of `/etc/rc.tcpip`:

```
grep "^#start[[::space::]]/usr/sbin/portmap" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/portmap "$src_running"
```

Remediation:

Review any active RPC services:

```
rpcinfo -p localhost
```

NOTE: If there are active RPC services and the services are required, do not disable `portmap`.

Disable `portmap` if there are no active RPC services:

```
chrctcp -d portmap
stopsrc -s portmap
```

4.10 TCP Wrappers

If some of the services running in /etc/inetd.conf are required, then it is recommended that TCP Wrappers are installed and configured to limit access to any active TCP and UDP services.

TCP Wrappers allow the administrator to control who has access to various inetd network services via source IP address controls. TCP Wrappers also provide logging information via syslog about both successful and unsuccessful connections.

TCP Wrappers are generally triggered via /etc/inetd.conf, but other options exist for "wrappering" non-inetd based software.

The configuration of TCP Wrappers to suit a particular environment is outside the scope of this benchmark; however the following links will provide the necessary documentation to plan an appropriate implementation:

TCP Wrappers Home Page

The website contains source code for both IPv4 and IPv6 versions.

4.10.1 TCP Wrappers - installing TCP Wrappers (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to install and configure TCP Wrappers if there are active `inetd` controlled services on the system.

Rationale:

TCP Wrappers is a freely available IP packet filtering facility. It provides for greater and more specific control over local network services and the hosts that are allowed to access them. It also makes use of the standard `syslog` facility to track local network use.

Audit:

Validate the installation of the software:

```
lslpp -L |grep "netsec.options"
```

The above command should yield the following output:

```
netsec.options.idprotocol  1.1.0.0    C     F    Authentication
daemon(RFC1413)  netsec.options.tcpwrapper.base
netsec.options.tcpwrapper.license
netsec.options.tcpwrapper.man.en_US
netsec.options.tcpwrapper.msg.en_US
```

NOTE: The version numbers may differ based on the source of the software

Remediation:

Identity any active `inetd` services:

```
refresh -s inetd
lssrc -ls inetd
```

If there are any active TCP or UDP services, download and install the TCP Wrappers software:

TCP Wrappers is bundled on the AIX media expansion cdrom.

Alternatively, the source code may be downloaded and compiled from:

TCP Wrappers Source Code

NOTE: Ensure that the latest version is downloaded.

The installation example below assumes that the AIX media expansion pack cdrom has been used as the source of the software.

Place the TCP Wrappers software into a convenient location, such as `/tmp` and install via:

```
/usr/lib/instl/sm_inst installp_cmd -a -Q -d /tmp -f
netsec.options.tcpwrapper,netsec.options.idprotocol -c -N -g -X -G -Y
```

NOTE: If the software is not located in `/tmp`, reflect the actual location in the command above.

4.10.2 TCP Wrappers - creating a hosts.deny file (Scored)

Profile Applicability:

- Level 1

Description:

Once TCP Wrappers are installed a `/etc/hosts.deny` file should be created and be configured.

Rationale:

The `/etc/hosts.deny` file describes the names of the hosts which are not allowed to access the local `inetd` services, as decided by the `/usr/sbin/tcpd` server. All access should be denied by default unless explicitly authorized.

Access is granted when a (daemon,client) pair matches an entry in the `/etc/hosts.allow` file. Access is denied when a (daemon,client) pair matches an entry in the `/etc/hosts.deny` file. However, access is granted if matching entry does not exist in both the files. This is why, by default, all access must be denied.

Audit:

Validate the content of the `/etc/hosts.deny` file:

```
cat /etc/hosts.deny
```

The above command should yield the following output:

```
ALL: ALL
```

Remediation:

Create a `/etc/hosts.deny` file:

```
touch /etc/hosts.deny
chown root:system /etc/hosts.deny
chmod u=rw,go= /etc/hosts.deny
```

Deny all traffic by default, explicit access will be defined in the `/etc/hosts.allow` file:

```
vi /etc/hosts.deny
```

Add:

```
ALL: ALL
```

4.10.3 TCP Wrappers - creating a hosts.allow file (Scored)

Profile Applicability:

- Level 1

Description:

Once TCP Wrappers are installed a `/etc/hosts.allow` file should be created and be configured.

Rationale:

This file describes the names of the hosts which are allowed to access the local `inetd` services as decided by the `/usr/sbin/tcpd` server. Access is granted when a (daemon,client) pair matches an entry in the `/etc/hosts.allow` file. Access is denied when a (daemon,client) pair matches an entry in the `/etc/hosts.deny` file. However, access is granted if matching entry does not exist in both the files.

Audit:

Validate the content of the `/etc/hosts.allow` file:

```
cat /etc/hosts.allow
```

The above command should reflect the defined configuration file.

NOTE:- Since the `/etc/hosts.allow` file is processed before `/etc/hosts.deny`, ensure that there are no entries in `/etc/hosts.allow` that may accidentally grant access to a system which are then subsequently denied in `/etc/hosts.deny`.

Remediation:

Create a `/etc/hosts.allow` file:

```
touch /etc/hosts.allow
chown root:system /etc/hosts.allow
chmod u=rw,go= /etc/hosts.allow
```

Define explicit access to the local `inetd` services:

```
vi /etc/hosts.allow
```

An example configuration:

```
ALL: LOCAL @some_netgroup
ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
```

4.10.4 TCP Wrappers - wrapping inetd services (Scored)

Profile Applicability:

- Level 2

Description:

If TCP Wrappers have been installed because there are active `inetd` services, these services must utilize TCP Wrappers to restrict host access.

Rationale:

By limiting access to the server, you reduce your exposure to threats from attackers on remote systems. Therefore any active `inetd` controlled service which cannot be disabled should be restricted so that it can only be used by trusted hosts.

Audit:

Ensure that the amended service line reflects the `tcpd` path:

```
grep "^<service name>[[:blank::]]" /etc/inetd.conf |grep "tcpd"
```

The above command should yield output.

Remediation:

Prior to implementing this recommendation it is important that `hosts.deny` and `hosts.allow` files have been created.

For each active TCP and UDP `inetd` service, change the entry in `/etc/inetd.conf`, so that `tcpd` is executed.

Copy the current `/etc/inetd.conf` file for reversion purposes:

```
cp -p /etc/inetd.conf /etc/inetd.conf.pre_tcp_wrappers
```

For example, to utilize TCP Wrappers on the telnet service:

Edit:

```
vi /etc/inetd.conf
```

Change:

```
telnet stream tcp6 nowait root /usr/sbin/telnetd telnetd
```

To:

```
telnet stream tcp nowait root /usr/sbin/tcpd telnetd
```

Repeat the change for other services.

4.11 Permissions and Ownership

This section will of the benchmark will focus on locking down access to specific key configuration files, log files and directories. If these critical files and directories have incorrect ownership and permissions, they can provide an attacker with a method of attack, or with pertinent system information.

Some of the files and directories changed in this section may not exist on your system. In this instance the recommendation can be ignored.

4.11.1 Permissions and Ownership - /etc/security (Scored)

Profile Applicability:

- Level 1

Description:

This `/etc/security` directory contains the user and group configuration files and the encrypted passwords.

Rationale:

The `/etc/security` directory contains sensitive files such as `/etc/security/passwd`, `/etc/security/group`. It must be secured from unauthorized access and modifications.

Audit:

Validate the permissions of `/etc/security`:

```
ls -ld /etc/security | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwxr-x---    root     security       /etc/security
```

Remediation:

Remove world read, write and execute access and group write access from `/etc/security`:

```
chown -R root:security /etc/security
chmod u=rwx,g=rx,o= /etc/security
chmod -R go-w,o-rx /etc/security
```

4.11.2 Permissions and Ownership - /etc/group (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/group` file contains a list of the groups defined within the system.

Rationale:

The `/etc/group` file defines basic group attributes. Since the file contains sensitive information, it must be properly secured.

Audit:

Validate the permissions of `/etc/group`:

```
ls -l /etc/group | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r--r--    root     security       /etc/group
```

Remediation:

Ensure correct ownership and permissions are in place for `/etc/group`:

```
chown root:security /etc/group
chmod u=rw,go=r /etc/group
```

4.11.3 Permissions and Ownership - /etc/passwd (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/passwd` file contains a list of the users defined within the system.

Rationale:

The `/etc/passwd` file defines all users within the system. Since the file contains sensitive information, it must be properly secured.

Audit:

Validate the permissions of `/etc/passwd`:

```
ls -l /etc/passwd | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r--r--    root     security       /etc/passwd
```

Remediation:

Ensure correct ownership and permissions are in place for `/etc/passwd`:

```
chown root:security /etc/passwd
chmod u=rw,go=r /etc/passwd
```

4.11.4 Permissions and Ownership - /etc/security/audit (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/security/audit` directory contains the system audit configuration files.

Rationale:

The `/etc/security/audit` directory stores the audit configuration files. This directory must have adequate access controls to prevent unauthorized access.

Audit:

Validate the permissions of `/etc/security/audit`:

```
ls -ld /etc/security/audit | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwxr-x---    root     audit           /etc/security/audit
```

Remediation:

Ensure correct ownership and permissions are in place for `/etc/security/audit`:

```
chown -R root:audit /etc/security/audit
chmod u=rwx,g=rx,o= /etc/security/audit
chmod -R u=rw,g=r,o= /etc/security/audit/*
```

4.11.5 Permissions and Ownership - /audit (Scored)

Profile Applicability:

- Level 1

Description:

The `/audit` directory holds the output produced from the audit subsystem.

Rationale:

The `/audit` directory stores the audit output files. This directory must have adequate access controls to prevent unauthorized access.

Audit:

Validate the permissions of `/audit`:

```
ls -ld /audit | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwxr-x---    root     audit           /audit
```

Remediation:

Ensure correct ownership and permissions are in place for `/audit`:

```
chown root:audit /audit
chmod u=rwx,g=rx,o= /audit
chmod -R u=rw,g=r,o= /audit/*
```

4.11.6 Permissions and Ownership - /smit.log (Scored)

Profile Applicability:

- Level 1

Description:

The `/smit.log` file maintains a history of all smit commands run as root.

Rationale:

The `/smit.log` file may contain sensitive information regarding system configuration, which may be of interest to an attacker. This log file must be secured from unauthorized access and modifications.

Audit:

Validate the permissions of `/smit.log`:

```
ls -l /smit.log | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r-----    root     system        /smit.log
```

Remediation:

Remove world read and write access to `/smit.log`:

```
chmod o-rw /smit.log
```

4.11.7 Permissions and Ownership - /var/adm/cron/log (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/adm/cron/log` file contains a log of all `cron` jobs run on the system.

Rationale:

The `/var/adm/cron/log`, records all cron jobs run on the system. The file permissions must ensure that it is accessible only to its owner and group.

Audit:

Validate the permissions of `/var/adm/cron/log`:

```
ls -l /var/adm/cron/log | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-rw----    root     cron         /var/adm/cron/log
```

Remediation:

Remove world read and write access to `/var/adm/cron/log`:

```
 chmod o-rw /var/adm/cron/log
```

4.11.8 Permissions and Ownership - /var/spool/cron/crontabs (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/spool/cron/crontabs` directory contains all of the `crontabs` for the users on the system.

Rationale:

The `/var/spool/cron/crontabs` directory contains all of the `crontabs` for the users on the system. Crontab files present a security problem because they are run by the `cron` daemon, which runs with super user rights. Allowing other users to have read/write permissions on these files may allow them to escalate their privileges. To negate this risk, the directory and all the files that it contains must be secured.

Audit:

Validate the permissions of `/var/spool/cron/crontabs`:

```
ls -ld /var/spool/cron/crontabs | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwxrwx---    root     cron         /var/spool/cron/crontabs
```

Remediation:

Apply the appropriate permissions to `/var/spool/cron/crontabs`:

```
chmod -R o= /var/spool/cron/crontabs
chmod ug=rwx,o= /var/spool/cron/crontabs
chgrp -R cron /var/spool/cron/crontabs
```

4.11.9 Permissions and Ownership - /var/adm/cron/at.allow (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/adm/cron/at.allow` file contains a list of users who can schedule jobs via the `at` command.

Rationale:

The `/var/adm/cron/at.allow` file controls which users can schedule jobs via the `at` command. Only the root user should have permissions to create, edit, or delete this file.

Audit:

Validate the permissions of `/var/adm/cron/at.allow`:

```
ls -l /var/adm/cron/at.allow | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-r--------    root     sys          /var/adm/cron/at.allow
```

Remediation:

Apply the appropriate permissions to `/var/adm/cron/at.allow`:

```
chown root:sys /var/adm/cron/at.allow
chmod u=r,go= /var/adm/cron/at.allow
```

4.11.10 Permissions and Ownership - /var/adm/cron/cron.allow (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/adm/cron/cron.allow` file contains a list of users who can schedule jobs via the `cron` command.

Rationale:

The `/var/adm/cron/cron.allow` file controls which users can schedule jobs via `cron`. Only the root user should have permissions to create, edit, or delete this file.

Audit:

Validate the permissions of `/var/adm/cron/cron.allow`:

```
ls -l /var/adm/cron/cron.allow | awk '{print $1 " " $3 " " $4 " " $9}' theone
```

The above command should yield the following output:

```
-r--------    root     sys         /var/adm/cron/cron.allow
```

Remediation:

Apply the appropriate permissions to `/var/adm/cron/cron.allow`:

```
chown root:sys /var/adm/cron/cron.allow
chmod u=r,go= /var/adm/cron/cron.allow
```

4.11.11 Permissions and Ownership - /etc/motd (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/motd` file contains the message of the day, shown after successful initial login.

Rationale:

The `/etc/motd` file contains the message of the day, shown after successful initial login. The file should only be editable by its owner.

Audit:

Validate the permissions of `/etc/motd`:

```
ls -l /etc/motd | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r--r--    bin     bin         /etc/motd
```

Remediation:

Apply the appropriate permissions to `/etc/motd`:

```
chown bin:bin /etc/motd
chmod u=rw,go=r /etc/motd
```

4.11.12 Permissions and Ownership - /var/adm/ras (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/adm/ras` directory contains log files which contain sensitive information such as login times and IP addresses.

Rationale:

The log files in the `/var/adm/ras` directory can contain sensitive information such as login times and IP addresses, which may be altered by an attacker when removing traces of

system access. All files in this directory must be secured from unauthorized access and modifications.

Audit:

Validate the permissions of the files in `/var/adm/ras`:

```
ls -l /var/adm/ras | awk '{print $1 " " $3 " " $4 " " $9}'
```

NOTE: The output from the command above will contain numerous files. No files should have read or write permission for other

Remediation:

Remove world read and write access from all files in `/var/adm/ras`:

```
chmod o-rw /var/adm/ras/*
```

4.11.13 Permissions and Ownership - /var/ct/RMstart.log (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/ct/RMstart.log` is the logfile used by RMC and can contain sensitive data that must be secured.

Rationale:

RMC provides a single monitoring and management infrastructure for both RSCT peer domains and management domains. Its generalized framework is used by cluster management tools to monitor, query, modify, and control cluster resources, `/var/ct/RMstart.log` is the logfile used by RMC and can contain sensitive data that must be secured.

Audit:

Validate the permissions of `/var/ct/RMstart.log`:

```
ls -l /var/ct/RMstart.log| awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r-----    root     system       /var/ct/RMstart.log
```

Remediation:

Remove world read and write from `/var/ct/RMstart.log`:

```
chmod o-rw /var/ct/RMstart.log
```

4.11.14 Permissions and Ownership - /var/tmp/dpid2.log (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/tmp/dpid2.log` is the logfile used by `dpid2` daemon, and contains SNMP information.

Rationale:

The `/var/tmp/dpid2.log` logfile is used by the `dpid2` daemon and can contain sensitive SNMP information. This file must be secured from unauthorized access and modifications.

Audit:

Validate the permissions of `/var/tmp/dpid2.log`:

```
ls -l /var/tmp/dpid2.log| awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r-----    root     system       /var/tmp/dpid2.log
```

Remediation:

Remove world read and write from `/var/tmp/dpid2.log`:

```
chmod o-rw /var/tmp/dpid2.log
```

4.11.15 Permissions and Ownership - /var/tmp/hostmibd.log (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/tmp/hostmibd.log` is the logfile used by `hostmibd` daemon, and contains network and machine related information.

Rationale:

The `/var/tmp/hostmibd.log` log file can contain network and machine related statistics logged by the daemon. This file must be secured from unauthorized access and modifications.

Audit:

Validate the permissions of `/var/tmp/hostmibd.log`:

```
ls -l /var/tmp/hostmibd.log| awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r-----    root     system       /var/tmp/hostmibd.log
```

Remediation:

Remove world read and write from `/var/tmp/hostmibd.log`:

```
chmod o-rw /var/tmp/hostmibd.log
```

4.11.16 Permissions and Ownership - /var/tmp/snmpd.log (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/tmp/snmpd.log` is the logfile used by `snmpd` daemon, and contains network and machine related information.

Rationale:

The `/var/tmp/snmpd.log` logfile contains sensitive information through which an attacker can find out about the SNMP deployment architecture in your network. This log file must be secured from unauthorized access.

Audit:

Validate the permissions of `/var/tmp/snmpd.log`:

```
ls -l /var/tmp/snmpd.log| awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r-----    root     system       /var/tmp/snmpd.log
```

Remediation:

Remove world read and write from `/var/tmp/snmpd.log`:

```
chmod o-rw /var/tmp/snmpd.log
```

4.11.17 Permissions and Ownership - /var/adm/sa (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/adm/sa` directory holds the performance data produced by the `sar` utility.

Rationale:

The `/var/adm/sa` directory contains the report files produced by the `sar` utility. This directory must be secured from unauthorized access.

Audit:

Validate the permissions of `/var/adm/sa`:

```
ls -ld /var/adm/sa | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
rwxr-xr-x    adm     adm       /var/adm/sa
```

Remediation:

Set the recommended ownership and permissions on `/var/adm/sa`:

```
chown adm:adm /var/adm/sa
chmod u=rwx,go=rx /var/adm/sa
```

4.11.18 Permissions and Ownership - home directory configuration files (Scored)

Profile Applicability:

- Level 1

Description:

The user configuration files in each home directory e.g. `$HOME/.profile`, must not be group or world writable.

Rationale:

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

Audit:

Re-execute the remediation script and all listed files in each user directory, should not have group or world writable permissions.

Remediation:

Search and remediate any user configuration files which have group or world writable access:

```
lsuser -a home ALL |cut -f2 -d= | while read HOMEDIR; do
echo "Examining $HOMEDIR"
if [ -d $HOMEDIR ]; then
ls -a $HOMEDIR | grep -Ev "^.$|^..$" | \
while read FILE; do
if [ -f $FILE ]; then
ls -l $FILE
chmod go-w $FILE
fi
done
else
echo "No home dir for $HOMEDIR"
```

```
fi
done
```

NOTE: The permission change is automatically applied

4.11.19 Permissions and Ownership - home directory permissions (Scored)

Profile Applicability:

- Level 1

Description:

All user home directories must not have group write or world writable access.

Rationale:

Group or world-writable user home directories may enable malicious users to steal or modify data, or to gain other user's system privileges. Disabling read and execute access for users, who are not members of the same group, allows for appropriate use of discretionary access control by each user.

Audit:

Validate the permissions of all of the directories changed:

```
lsuser -c ALL | grep -v ^#name | cut -f1 -d: | while read NAME; do
if [ `lsuser -f $NAME | grep id | cut -f2 -d=` -ge 200 ]; then
HOME=`lsuser -a home $NAME | cut -f 2 -d =`
ls -ld $HOME
fi
done
```

NOTE: All listed directories should have `drwxr-x---` permissions

Ensure that the change has been made to `/usr/lib/security/mkuser.sys` to reflect permissions setting:

```
grep -c 'mkdir $1 && chmod u=rwx,g=rx,g= $1' /usr/lib/security/mkuser.sys
```

NOTE: The output from the command above should be 1

Remediation:

Change any home directories which have group or world writable access:

```
NEW_PERMS=750
lsuser -c ALL | grep -v ^#name | cut -f1 -d: | while read NAME; do
if [ `lsuser -f $NAME | grep id | cut -f2 -d=` -ge 200 ]; then
HOME=`lsuser -a home $NAME | cut -f 2 -d =`
echo "Changing $NAME homedir $HOME"
chmod $NEW_PERMS $HOME
fi
done
```

NOTE: The permission change is automatically applied to all user directories with a user ID over 200.

Modify `/usr/lib/security/mkuser.sys` to ensure that all new user home directories will be created with a default permission of 750:

```
vi /usr/lib/security/mkuser.sys
```

Replace:

```
mkdir $1
```

With:

```
 mkdir $1 && chmod u=rwx,g=rx,g= $1
```

4.11.20 Permissions and Ownership - world/group writable directory in root PATH (Scored)

Profile Applicability:

- Level 1

Description:

To secure the root users executable PATH, all directories must not be group and world writable.

Rationale:

There should not be group or world writable directories in the root user's executable path. This may allow an attacker to gain super user access by forcing an administrator operating as root to execute a Trojan horse program.

Audit:

Execute the following code as the `root` user:

```
echo "/:${PATH}" | tr ':' '\n' | grep "^/" | sort -u | while read DIR
do
DIR=${DIR:-$(pwd)}
while [[ -d ${DIR} ]]
do
[[ "$(ls -ld ${DIR})" = @(d???????w? *) ]] && print " WARNING ${DIR} is world
wr
itable"
[[ "$(ls -ld ${DIR})" = @(d????w???? *) ]] && print " WARNING ${DIR} is group
wr
itable"
[[ "$(ls -ld ${DIR} |awk '{print $3}')" != @(root|bin) ]] && print " WARNING
${D
IR} is not owned by root or bin"
DIR=${DIR%/*}
done
done
```

The above command should yield no output

Remediation:

Search and report on group or world writable directories in root's PATH. The command must be run as the root user. The script below traverses up each individual directory PATH, ensuring that all directories are not group/world writable and that they are owned by root or the bin user:

```
echo "/:${PATH}" | tr ':' '\n' | grep "^/" | sort -u | while read DIR
do
DIR=${DIR:-$(pwd)}
print "Checking ${DIR}"
while [[ -d ${DIR} ]]
do
[[ "$(ls -ld ${DIR})" = @(d???????w? *) ]] && print " WARNING ${DIR} is world
wr
itable" || print " ${DIR} is not world writable"
[[ "$(ls -ld ${DIR})" = @(d????w???? *) ]] && print " WARNING ${DIR} is group
wr
itable" || print " ${DIR} is not group writable"
[[ "$(ls -ld ${DIR} |awk '{print $3}')" != @(root|bin) ]] && print " WARNING
${D
IR} is not owned by root or bin"
```

```
DIR=${DIR%/*}
done
done
```

NOTE: Review the output and manually change the directories, if possible. Directories which are group and/or world writable are marked with "WARNING"

To manually change permissions on the directories:

To remove group writable access:

```
chmod g-w <dir name>
```

To remove world writable access:

```
chmod o-w <dir name>
```

To remove both group and world writable access:

```
chmod go-w <dir name>
```

To change the owner of a directory:

```
chown <owner> <dir name>
```

To fully automate the PATH directory permission changes execute the following code as the `root` user:

```
echo "/:${PATH}" | tr ':' '\n' | grep "^/" | sort -u | while read DIR
do
DIR=${DIR:-$(pwd)}
while [[ -d ${DIR} ]]
do
[[ "$(ls -ld ${DIR})" = @(d???????w? *) ]] && chmod o-w ${DIR} && print
"Removin
g world write from ${DIR}"
[[ "$(ls -ld ${DIR})" = @(d????w???? *) ]] && chmod g-w ${DIR} && print
"Removin
g group write from ${DIR}"
DIR=${DIR%/*}
```

```
done
done
```

4.12 Miscellaneous Configuration Changes

This section of the benchmark will focus on miscellaneous configuration changes. These are general changes which do not warrant a dedicated section.

4.12.1 Miscellaneous Config - serial port restriction (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to disable the login capability of all connected `tty` devices.

Rationale:

It is recommended that the login capability for all serial ports is disabled, so that unauthorized users cannot attach modems or remote access devices to these ports and bypass any network access control.

If the environment utilizes `tty` devices to facilitate user connections. This recommendation may be ignored.

Audit:

Ensure that all `tty` devices are now disabled:

```
lsitab -a |egrep "respawn:/usr/sbin/getty|on:/usr/sbin/getty"
```

The above command should yield no output (apart from the system console)

Remediation:

Create a list of active `tty` ports:

```
lsitab -a |egrep "respawn:/usr/sbin/getty|on:/usr/sbin/getty"
```

If any `tty` devices are returned from the previous output, lock down each any unrequired devices via:

```
chitab "tty2:2:off:/usr/sbin/getty /dev/tty2"
```

NOTE: Replace `tty2` with the relevant port

4.12.2 Miscellaneous Config - disable i4ls (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to disable the `i4ls` license manager. This is typically used for C and Cobol license management.

Rationale:

It is recommended that the `i4ls` license manager is disabled. The license manager is needed for C and Cobol compilers etc. If the environment supports NCS and a license server is required, a node locked license server should be used instead.

Audit:

Ensure that `i4ls` is now disabled:

```
lsitab i4ls
```

The above command should yield no output.

Remediation:

Identify if `i4ls` is enabled:

```
lsitab i4ls
```

If the command above yields output, remove via:

```
rmitab i4ls
```

4.12.3 Miscellaneous Config - disable NCS (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to disable Network Computing System (NCS). It provide tools for designing, implementing, and supporting applications requiring distributed data and distributed computing.

Rationale:

NCS is an implementation of the Network Computing Architecture developed to provide tools for designing, implementing, and supporting applications requiring distributed data and distributed computing. It is recommended that NCS is disabled, unless it is required within the environment.

Audit:

Ensure that NCS is now disabled:

```
lsitab rcncs
```

NOTE: If the output from the lsitab command was not `rcncs`, substitute that above.

The above command should yield no output.

Remediation:

Identify if NCS is enabled:

```
lsitab -a |grep "/etc/rc.ncs" | cut -f1 -d:
```

If the command above yields output, remove via:

```
rmitab rcncs
```

NOTE: If the output from the `lsitab` command was not `rcncs`, substitute that above.

4.12.4 Miscellaneous Config - disable httpdlite (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to disable `httpdlite`. This is a web server which provides on-line documentation.

Rationale:

`httpdlite` is the Lite NetQuestion Web server software for online documentation. It is recommended that this software is disabled, unless it is required in the environment.

NOTE: The `man` command does not need this to work correctly.

Audit:

Remediation:

Identify if `httpdlite` is enabled:

```
lsitab httpdlite
```

If the command above yields output, remove via:

```
rmitab httpdlite
```

4.12.5 Miscellaneous Config - disable pmd (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to disable `pmd`. This is the power management service that turns the machine off if it has been idle for a specific amount of time.

Rationale:

`pmd` is the power management service that turns the machine off if it has been idle for a specific amount of time. This recommendation is to disable this service.

Audit:

Ensure that `pmd` is now disabled:

```
lsitab pmd
```

The above command should yield no output.

Remediation:

Identify if `pmd` is enabled:

```
lsitab pmd
```

If the command above yields output, remove via:

```
rmitab pmd
```

4.12.6 Miscellaneous Config - disable writesrv (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to disable `writesrv`. This allows users to chat using the system write facility on a terminal.

Rationale:

`writesrv` allows users to chat using the system write facility on a terminal. The recommendation is that this service must be disabled.

Audit:

Ensure that `writesrv` is now disabled:

```
lsitab writesrv
```

The above command should yield no output.

Remediation:

Identify if `writesrv` is enabled:

```
lsitab writesrv
```

If the command above yields output, remove via:

```
rmitab writesrv
```

4.12.7 Miscellaneous Config - block talk/write (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to block `talk` and `write`. This allows connected users to chat within terminal sessions.

Rationale:

The recommendation is to block attempts to use the `write` or `talk` commands. This improves the security of the `tty` device.

However, there are two exceptions:

1. The super user can write to anyone
2. If you are logged in as the same user who has turned the messages off, you can write to the super user

Audit:

Ensure that `talk` and `write` have been disabled:

```
grep -c "mesg n" /etc/profile
grep -c "mesg n" /etc/csh.login
```

NOTE: Both commands should return a value of 1

Remediation:

Disable `talk` and `write` for ALL shells:

```
echo "mesg n" >> /etc/profile
echo "mesg n" >> /etc/csh.login
```

4.12.8 Miscellaneous Config - enable sar accounting (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to enable `sar` performance accounting. This will provide a normal performance baseline which will help identify unusual performance patterns, created through potential attacks via a password cracking program being executed or through a DoS attack etc.

Rationale:

System accounting gathers periodic baseline system data, such as CPU utilization and disk I/O. Once a normal baseline for the system has been established, unauthorized activities, such as a password cracking being executed and activity outside of normal usage hours may be detected due to departure from the normal system performance baseline. It is recommended that the collection script is run on an hourly basis, every day, to help to detect any anomalies. It is also important to generate and review the system activity report on a daily basis.

There may be 3rd party tools, or in-house written scripts in place which perform a similar function. In this instance this recommendation can be ignored.

Audit:

Review the `adm` user crontab:

```
cat /var/spool/cron/crontabs/adm
```

The above command should yield output which reflects the changes made in the remediation section.

Remediation:

Prior to configuring `sar` reporting, ensure that the `bos.acct` fileset is installed:

```
lslpp -L bos.acct
```

NOTE: The `bos.acct` fileset should be listed, along with the currently installed version

If the software is not installed, install from the relevant AIX media pack:

```
/usr/lib/instl/sm_inst installp_cmd -a -Q -d /tmp -f bos.acct -c -N -g -X -G
-Y
```

NOTE: If the software is not located in `/tmp`, reflect the actual location in the command above.

Edit the `adm` user crontab:

```
vi /var/spool/cron/crontabs/adm
```

NOTE: There are commented out example system activity report lines. Review and tailor to the needs of the environment:

```
#==========================================================
#      SYSTEM ACTIVITY REPORTS
#  8am-5pm activity reports every 20 mins during weekdays.
#  activity reports every an hour on Saturday and Sunday.
#  6pm-7am activity reports every an hour during weekdays.
#  Daily summary prepared at 18:05.
#==========================================================
#0 8-17 * * 1-5 /usr/lib/sa/sa1 1200 3 &
#0 * * * 0,6 /usr/lib/sa/sa1 &
#0 18-7 * * 1-5 /usr/lib/sa/sa1 &
#5 18 * * 1-5 /usr/lib/sa/sa2 -s 8:00 -e 18:01 -i 3600 -ubcwyaqvm &
```

NOTE: Change and uncomment the lines where appropriate. Refer to the `sar` documentation for further guidance

Create the reporting directory structure and apply the appropriate permissions:

```
mkdir -p /var/adm/sa
chown adm:adm /var/adm/sa
chmod u=rwx,go=rx /var/adm/sa
```

4.12.9 Miscellaneous Config - /etc/ftpusers (Scored)

Profile Applicability:

- Level 2

Description:

The `/etc/ftpusers` is a configuration file used by `ftp` daemon. It contains a list of users who are not allowed to access the system via `ftp`.

Rationale:

The `/etc/ftpusers` file contains a list of users who are not allowed to access the system via `ftp`. All users with a UID less than 200 should typically be added into the file.

Audit:

Review the content `/etc/ftpusers`, ensure there are no duplicate entries:

```
cat /etc/ftpusers
```

Remediation:

List all users with a UID less than 200 to the `/etc/ftpusers` file:

```
lsuser -c ALL | grep -v ^#name |grep -v root | cut -f1 -d: | while read NAME;
do
if [ `lsuser -f $NAME | grep id | cut -f2 -d=` -lt 200 ] > /dev/null 2>&1;
then
echo "Would add $NAME to /etc/ftpusers"
fi
done
```

NOTE: Review the list of users

Add all relevant users with a UID of less that 200 to the `/etc/ftpusers` file:

```
lsuser -c ALL | grep -v ^#name |grep -v root | cut -f1 -d: | while read NAME;
do
if [ `lsuser -f $NAME | grep id | cut -f2 -d=` -lt 200 ] > /dev/null 2>&1;
then
echo $NAME >> /etc/ftpusers
fi
done
```

4.12.10 Miscellaneous Config - ftp umask (Scored)

Profile Applicability:

- Level 1

Description:

The umask of the `ftp` service should be set to at least 027 in order to prevent the FTP daemon process from creating world-writable files by default.

Rationale:

The umask of the `ftp` service should be set to at least 027 in order to prevent the FTP daemon process from creating world-writable files by default. These files could then be transferred over the network which could result in compromise of the critical information.

Audit:

Validate the umask setting:

```
[[ $(grep -c "^ftp[[:blank:]]" /etc/inetd.conf) -gt 0 ]] && grep
"^ftp[[:blank:]]" /etc/inetd.conf |awk '{print $6 " " $7 " " $8 " " $9}' ||
RC=0
```

The above command should yield the following output (only if the ftp daemon is not disabled):

```
/usr/sbin/ftpd ftpd -l -u077
```

Remediation:

Set the default umask of the `ftp` daemon:

```
[[ $(grep -c "^ftp[[:blank:]]" /etc/inetd.conf) -gt 0 ]] && chsubserver -c -v
ftp -p tcp "ftpd -l -u077" && refresh -s inetd || RC=0
```

NOTE: The umask above restricts read/write permissions for both group and other

4.12.11 Miscellaneous Config - ftp banner (Scored)

Profile Applicability:

- Level 1

Description:

Set an `ftp` login banner which displays the acceptable usage policy.

Rationale:

The message in `banner.msg` is displayed for FTP logins. Banners display necessary warnings to users trying to gain unauthorized access to the system and are required for legal purposes. The recommendation is to set the banner as:

"Authorized uses only. All activity will be monitored and reported".

The content may be changed to reflect any corporate AUP.

Audit:

Open a session to the localhost and validate the banner:

```
dspcat -g /usr/lib/nls/msg/en_US/ftpd.cat | grep "^9[[:blank:]]"
```

The above command should yield the following output:

```
9       "%s Authorized uses only. All activity may be monitored and reported"
```

Remediation:

Ensure that the `bos.msg.en_US.net.tcp.client` fileset is installed:

```
lslpp -L "bos.msg.en_US.net.tcp.client"
```

NOTE: If the fileset is not installed, install it from the AIX media or another software repository. The fileset should reflect the language used on the server.

Once installed set the `ftp` AUP banner:

```
dspcat -g /usr/lib/nls/msg/en_US/ftpd.cat > /tmp/ftpd.tmp
sed "s/\"\%s FTP server (\%s) ready.\"/\"\%s Authorized uses only. All
activity may be monitored and reported\"/" /tmp/ftpd.tmp > /tmp/ftpd.msg
gencat /usr/lib/nls/msg/en_US/ftpd.cat /tmp/ftpd.msg
rm /tmp/ftpd.tmp /tmp/ftpd.msg
```

4.12.12 Miscellaneous Config - /etc/motd (Scored)

Profile Applicability:

- Level 1

Description:

Create a `/etc/motd` file which displays, post initial logon, a statutory warning message.

Rationale:

The creation of a `/etc/motd` file which contains a statutory warning message could aid in the prosecution of offenders guilty of unauthorized system access. The `/etc/motd` is displayed after successful logins from the console, SSH and other system access protocols.

Audit:

Log back into the system via SSH:

```
ssh localhost
```

NOTE: The `/etc/motd` file will now be displayed

Remediation:

Create a `/etc/motd` file:

```
touch /etc/motd
chmod u=rw,go=r /etc/motd
chown bin:bin /etc/motd
```

Below is a sample banner:

```
**************************************************************************
NOTICE TO USERS
This computer system is the private property of its owner, whether
individual, corporate or government. It is for authorized use only. Users
(authorized or unauthorized) have no explicit or implicit expectation of
privacy. Any or all uses of this system and all files on this system may be
intercepted, monitored, recorded, copied, audited, inspected, and disclosed
to your employer, to authorized site, government, and law enforcement
personnel, as well as authorized officials of government agencies, both
domestic and foreign. <p> By using this system, the user consents to such
interception, monitoring,recording, copying, auditing, inspection, and
disclosure at the discretion of such personnel or officials. Unauthorized or
improper use of this system may result in civil and criminal penalties and
administrative or disciplinary action, as appropriate. By continuing to <p>
use this system you indicate your awareness of and consent to these terms and
conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions
stated in this
warning.  ***********************************************************
*********
```

NOTE: Replace "its owner" with the relevant company name

4.12.13 Miscellaneous Config - authorized users in at.allow (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/adm/cron/at.allow` file defines which users on the system are able to schedule jobs via `at`.

Rationale:

The `/var/adm/cron/at.allow` file defines which users are able to schedule jobs via `at`. Review the current at files and add any relevant users to the `/var/adm/cron/at.allow` file.

Audit:

Review the content `/var/adm/cron/at.allow`, ensure that the content reflects the changes made:

```
cat /var/adm/cron/at.allow
```

Remediation:

Review the current `at` files:

```
ls -l /var/spool/cron/atjobs
cat /var/spool/cron/atjobs/*
```

NOTE: Review the list of `at` schedules and remove any files which should not be there, or have no content

Add the recommended system users to the `at.allow` list:

```
echo "adm" >>/var/adm/cron/at.allow
echo "sys" >> /var/adm/cron/at.allow
```

Add any other users who require permissions to use the `at` scheduler:

```
echo <user> >> /var/adm/cron/at.allow
```

NOTE: Where <user> is the username

4.12.14 Miscellaneous Config - authorized users in cron.allow (Scored)

Profile Applicability:

- Level 1

Description:

The `/var/adm/cron/cron.allow` file defines which users on the system are able to schedule jobs via `cron`.

Rationale:

The `/var/adm/cron/cron.allow` file defines which users are able to schedule jobs via `cron`. Review the current `cron` files and add any relevant users to the `/var/adm/cron/cron.allow` file.

Audit:

Review the content `/var/adm/cron/cron.allow`, ensure that the content reflects the changes made:

```
cat /var/adm/cron/cron.allow
```

Remediation:

Review the current `cron` files:

```
ls -l /var/spool/cron/crontabs
cat /var/spool/cron/crontabs/*
```

NOTE: Review the list of `cron` schedules and remove any files which should not be there, or have no content

Add the recommended system users to the `cron.allow` list:

```
echo "sys" >> /var/adm/cron/cron.allow
echo "adm" >> /var/adm/cron/cron.allow
```

Add any other users who require permissions to use the `cron` scheduler:

```
echo <user> >> /var/adm/cron/cron.allow
```

NOTE: Where <user> is the username

4.12.15 Miscellaneous Config - all unlocked accounts must have a password (Scored)

Profile Applicability:

- Level 1

Description:

All unlocked accounts on the server must have a password.

Rationale:

An account password is a secret code word that must be entered to gain access to the account. If an account exists that has a blank password, multiple users may access the account without authentication and leave a weak audit trail. An attacker may gain unauthorized system access or perform malicious actions, which then cannot be attributed to any specific individual.

Audit:

Re-run the command:

```
pwdck -n ALL
```

The command should not yield output

Remediation:

Check for empty passwords:

```
pwdck -n ALL
```

If the command above yields output, set up a password on the account:

```
passwd <username>
```

4.12.16 Miscellaneous Config - all user id must be unique (Scored)

Profile Applicability:

- Level 1

Description:

All users should have a unique UID. In particular the only user on the system to have a UID of 0 should be the root user.

Rationale:

The only user with a UID of 0 on the system must be the root user. Any account with a UID of 0 has super user privileges on the system and is effectively root. All access to the root account should be via `su` or `sudo` to provide an audit trail. All other users must also have a unique UID to ensure that file and directory security is not compromised.

Audit:

Re-run the command:

```
cut -d: -f 3 /etc/passwd |sort -n |uniq -d
```

The command above should not yield output

Remediation:

Examine the user IDs of all configured users:

```
cut -d: -f 3 /etc/passwd |sort -n |uniq -d
```

If a number, or numbers are returned from the command above, these are UID which are not unique within the `/etc/passwd` file. Determine the effected username/s:

```
cut -f "1 3" -d : /etc/passwd |grep ":<UID>$"
```

NOTE: Any user names returned should either be deleted or have the UID changed

To remove:

```
rmuser <username>
```

To change the UID:

```
chuser id=<id> <username>
```

4.12.17 Miscellaneous Config - all group id must be unique (Scored)

Profile Applicability:

- Level 1

Description:

All groups should have a unique GID on the system.

Rationale:

All groups should have an individual and unique GID. If GID numbers are shared this could lead to undesirable file and directory access.

Audit:

Re-run the command:

```
cut -d: -f 3 /etc/group |sort -n |uniq -d
```

The command above should not yield output

Remediation:

Ensure that all group IDs are unique:

```
cut -d: -f 3 /etc/group |sort -n | uniq -d
```

If a number, or numbers are returned from the command above, these are GID which are not unique within the `/etc/group` file. Determine the effected group names:

```
cut -f "1 3" -d : /etc/group |grep ":<GID>$"
```

NOTE: Any group names returned should either be deleted or have the UID changed

To remove:

```
rmgroup <groupname>
```

To change the UID:

```
chgroup id=<id> <groupname>
```

4.12.18 Miscellaneous Config - unnecessary user and group removal (Scored)

Profile Applicability:

- Level 1

Description:

Remove unnecessary administrative user accounts to further enhance security.

Rationale:

Remove unnecessary administrative user accounts and groups, if possible. Generic administrative user accounts are targeted by hackers in an attempt to gain unauthorized access to a server.

Audit:

Ensure that the user accounts have been removed:

```
egrep "uucp|nuucp|lpd|printq" /etc/passwd
```

The command should not yield output

Ensure that the groups have been removed:

```
egrep "uucp|printq" /etc/group
```

The command should not yield output

Remediation:

Remove the `uucp`, `nuucp`, `lpd`, and `printq` user accounts and respective groups, if possible:

```
# Remove users
LIST="uucp nuucp lpd printq"
for USERS in $LIST; do
rmuser -p $USERS
done

# Remove groups
LIST="uucp printq"
for GROUPS in $LIST; do
rmgroup $GROUPS
done
```

NOTE:- Other users and groups can be added to the list if required

4.12.19 Miscellaneous Config - removing current working directory from root's PATH (Scored)

Profile Applicability:

- Level 1

Description:

This change removes any "." or "::" entries from the root PATH. If a "." or "::" is present the current working directory is included in the search path.

Rationale:

Any "." and "::" will be removed from the root PATH. This means that any harmful programs placed in common PATH locations, would never be automatically executed. All directories must be explicitly defined within the PATH variable.

Audit:

Ensure that root's PATH does not contain any "." or "::" entries:

```
su - root -c "echo ${PATH}" |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[
\t]*:)|(^.:)|(:.$)|(:.:))/'
```

The above command should yield no output.

Remediation:

Examine root's PATH to see if it contains any "." or "::" entries:

```
su - root -c "echo ${PATH}" |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[
\t]*:)|(^.:)|(:.$)|(:.:))/'
```

If the command above yields output, remove the "." and "::" entries from the relevant initialization files. The files to examine are dependant on the root users shell definition in `/etc/passwd`. Once the file or files have been identified remove the "." and "::" from the PATH variable

```
vi <filename>
```

4.12.20 Miscellaneous Config - removing current working directory from default /etc/environment PATH (Scored)

Profile Applicability:

- Level 1

Description:

This change removes any "." or "::" entries from `/etc/environment`. If a "." or "::" is present the current working directory is included in the default search path.

Rationale:

Any "." and "::" will be removed from `/etc/environment`. This means that any harmful programs placed in common PATH locations, would never be automatically executed. All directories must be explicitly defined within the PATH variable.

Audit:

Examine PATH in `/etc/environment` to see if it contains any "." or "::" entries:

```
grep "^PATH=" /etc/environment |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[
\t]*:)|(^.:)|(:.$)|(:.:))/'
```

The above command should yield no output.

Remediation:

Examine PATH in `/etc/environment` to see if it contains any "." or "::" entries:

```
grep "^PATH=" /etc/environment |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[
\t]*:)|(^.:)|(:.$)|(:.:))/'
```

If the command above yields output, remove the "." and "::" entries from:

```
vi /etc/environment
```

4.13 Encrypted Filesystems (EFS)

Another enhancement of AIX 6.1 is the introduction of Encrypted Filesystems. This enables an individual user, via keystore files, to encrypt their own data within a jfs2 filesystem. After creating EFS enabled filesystems, individual files can be encrypted or inheritance can be set at the filesystem or directory level. The standard AIX data and user management commands have been modified to work with encryption.

There are a number of reasons for encrypting data in this manner, perhaps to send backups of data off site, or to encrypt sensitive or confidential information such as payroll details.

4.13.1 EFS - implementation (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation, if there is a requirement for file based encryption, is to utilize EFS.

Rationale:

The use of EFS further enhances the file and directory security within AIX. If there are sensitive or confidential files, encryption provides that extra level of security in the event of an accidental `chmod` which may allow read or write access to other users.

The encryption operates at the filesystem level and each file is encrypted with a separate key. From a user perspective the encryption is transparent as the key can be automatically loaded during login.

Audit:

Validate the installation of the CLiC software:

```
lslpp -L |grep "clic"
```

The above command should yield the following output:

```
clic.rte.includes       4.3.0.0     C     F     CrytoLite for C Library
                                                Include File
clic.rte.kernext        4.3.0.0           C     F     CrytpLite for C Kernel
clic.rte.lib            4.3.0.0           C     F     CyrptoLite for C
Library
clic.rte.pkcs11         4.3.0.0           C     F     PKCS11 Software Token
Support
```

NOTE: The version numbers may differ based on the source of the software

Validate that the CLiC kernel extension has loaded:

```
genkex |grep crypt
```

The above command should yield the following output:

```
438b000 39000 /usr/lib/drivers/crypto/clickext
```

Remediation:

There are two pre-requisite requirements for EFS, it requires RBAC and the installation of the CLiC cryptographic fileset. The fileset is located on the expansion pack, shipped with the AIX media.

Place the CLiC software into a convenient location, such as `/tmp` and install via:

```
/usr/lib/instl/sm_inst installp_cmd -a -Q -d /tmp -f clic.rte -c -N -g -X -G
-Y
```

NOTE: If the software is not located in `/tmp`, reflect the actual location in the command above.

Load the CLiC kernel extension:

```
/usr/lib/methods/loadkclic
```

As the EFS administrator, create the initial keystore. This is typically the root user:

```
efsenable -a
```

An EFS enabled filesystem can be created with the following command:

```
chfs -v jfs2 -g <vg_name> -m </filesystem> -a size=<size> -a efs=yes
```

To enable EFS for an existing filesystem:

```
chfs -a efs=yes </filesystem>
```

To encrypt a file, load your keystore via:

```
efskeymgr -o ksh
```

Then encrypt via:

```
efsmgr -c AES_192_ECB -e <filename>
```

To decrypt:

```
efsmgr -d <filename>
```

Further details regarding planning and implementation of EFS can be found within the IBM AIX 7.1 Infocentre:

http://pic.dhe.ibm.com/infocenter/aix/v7r1/index.jsp?topic=%2Fcom.ibm.aix.security%2Fdoc%2Fsecurity%2Fefs_efs.htm

NOTE: The configuration of EFS is completely dependant on the unique requirements of a given environment.

4.14 Privileged Command Management

One of the primary causes of system outages is inadvertent or accidental command usage when a user has root privileges. Many users seemingly forget that they are logged in as root, or use inappropriate command arguments. The carte blanche use of the root account should be limited to those individuals who administer the operating system. Users such as database administrators, application support teams and troubleshooters can be given privileged access to the commands they need via tools such as sudo or enhanced RBAC. These tools require careful planning and implementation, but ultimately can eradicate the need for the root password.

This section of the benchmark will detail the recommended methods of managing privileged command access.

4.14.1 PCM - sudo (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to install and configure sudo, to reflect the privileged command access requirements of all users of the system.

Rationale:

Privileged command access should be limited to and defined by a user's individual needs. Access to a root command prompt should limited, wherever possible, to minimize the risk of inadvertent or deliberate misuse of the account.

The choice between sudo and enhanced RBAC revolves around whether or not the environment is heterogeneous in nature, running different flavors of UNIX, or perhaps different versions of AIX. It may be that sudo is the standard tool of choice for managing privileged command access across an entire UNIX estate. However, if the environment is AIX 6.1+ only, it is recommended that enhanced RBAC is used as the tool of choice. Some implementations however may benefit from a combined approach, utilizing both sudo and enhanced RBAC.

The sudo software is packaged as an RPM by IBM and is available on the AIX Toolbox for LINUX media, or via download from the following location:

http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/download.html

Audit:

Validate the sudo installation:

```
rpm -q sudo
```

The above command should yield the following output:

```
sudo-1.6.9p15-2noldap
```

NOTE: The version reflected above may differ from the one installed.

Remediation:

Place the sudo software into a convenient location, such as `/tmp` and install via:

```
/usr/lib/instl/sm_inst installp_cmd -a -Q -d /tmp -f sudo -c -N -g -X -G -Y
```

NOTE: If the software is not located in `/tmp`, reflect the actual location in the command above.

Once installed refer to the sudo man page for information regarding the creation of a custom `/etc/sudoers` file. It is recommended that, to reduce rule complexity, privileges are assigned at a group level wherever possible:

http://www.gratisoft.us/sudo/man/sudo.html

NOTE: The configuration of sudo is completely dependant on the unique requirements of a given environment.

All editing of the `/etc/sudoers` file must be performed by the following command:

```
visudo
```

Once the `/etc/sudoers` file has been successfully created, validate the syntax of the file:

```
visudo -c
```

4.14.2 PCM - enhanced RBAC (Not Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to configure RBAC to reflect the privileged command access requirements for all users of the system. RBAC is a default component of AIX 7.1.

Rationale:

Privileged command access should be limited to and defined by a user's individual needs. Access to a root command prompt should limited, wherever possible, to minimize the risk of inadvertent or deliberate misuse of the account.

The choice between sudo and enhanced RBAC revolves around whether or not the environment is heterogeneous in nature, running different flavors of UNIX, or perhaps different versions of AIX. It may be that sudo is the standard tool of choice for managing privileged command access across an entire UNIX estate. However, if the environment is AIX 6.1+ only, it is recommended that enhanced RBAC is used as the tool of choice. Some implementations however may benefit from a combined approach, utilizing both sudo and enhanced RBAC.

Audit:

N/A

Remediation:

Enhanced RBAC improves on its legacy implementation by allowing greater flexibility around command lists and authorization definitions, which can be customized. The definitions are also saved to a kernel table rather than in flat files, which improves security.

The implementation of RBAC is role based, allowing users to be specifically granted access to the privileged commands they need to perform their day to day tasks. The tool can be used to replace sudo in many instances, or indeed to work alongside it.

A successful implementation may also allow the root account to be deprecated.

The RBAC definition files:

```
/etc/security/privcmds
/etc/security/privfiles
/etc/security/privdevs
```

The command used to list the active RBAC definitions, i.e. those loaded into the kernel:

```
lskst
```

The command used to update RBAC definitions in the kernel table:

```
setkst
```

Further details regarding planning and implementation of RBAC can be found within the IBM AIX 7.1 Infocentre:

http://pic.dhe.ibm.com/infocenter/aix/v7r1/index.jsp?topic=%2Fcom.ibm.aix.security%2Fdoc%2Fsecurity%2Frbac_in_aix.htm

NOTE: The configuration of enhanced RBAC is completely dependant on the unique requirements of a given environment.

4.15 Trusted Execution (TE)

This is a further development of the Trusted Computing Base (TCB) packaged with previous versions of AIX. Unlike TCB, Trusted Execution is not an install time only option and it can be enabled on previously installed systems. Its primary purpose is to protect from Trojan horse style attacks, by only allowing the execution of certain executables and kernel extensions.

TE has two modes of operation, online and offline. The online mode provides the most comprehensive security, as a check is made every time a file is loaded into memory. If the integrity checks fail, the file will not be loaded into memory. The offline mode checks file integrity at a specified time, via either the command line or via crontab.

4.15.1 TE - implementation (Scored)

Profile Applicability:

- Level 2

Description:

The recommendation is to implement TE to protect the system from Trojan horse style attacks. TE provides a robust system integrity checking process.

Rationale:

One of the common ways a hacker infiltrates a system is through file tampering or the use of a Trojan horse. The implementation of TE can provide a number of integrity checks prior to loading a program into memory, any deviations can also be highlighted when programs and files are validated offline. This ensures that the programs executed are those which are intended to be and not malicious code masquerading as a true program.

When a discrepancy is identified it is classified as either minor or major. A minor discrepancy is automatically reset to the value defined in the TSD. In the event of a major discrepancy the file access permissions are changed to make the file inaccessible.

There is a pre-requisite requirement to install CLiC and SSL software.

Audit:

Ensure that TE is enabled:

```
trustchk -p TE
```

The above command should yield the following output:

```
TE=ON
```

Ensure that TEP is enabled:

```
trustchk -p TEP
```

The above command should yield the following output:

```
TEP=ON
```

Remediation:

It is recommended that TE is configured in online mode. This provides real time protection against Trojan horse attacks.

The `tsd.dat` file contains the important security attributes relating to all of the managed files:

```
cat /etc/security/tsd/tsd.dat
```

NOTE: The `trustchk` command is used to manage the entries in this file.

To enable TE, firstly enable online checking of executables and shell scripts:

```
trustchk -p CHKEXEC=ON
trustchk -p CHKSCRIPT=ON
```

Stop the execution or loading of binaries and files into memory when the integrity checks fail:

```
trustchk -p STOP_ON_CHKFAIL=ON
```

Enable online TE based on the policy selections above:

```
trustchk -p TE=ON
```

To set a Trusted Execution Path or TEP:

```
trustchk -p TEP=<PATH variable>
```

Enable the TEP:

```
trustchk -p TEP=ON
```

NOTE: Commands will not be executed if they reside outside of the TEP.

Further details regarding planning and implementation of TE can be found within the IBM AIX 7.1 Infocentre:

http://pic.dhe.ibm.com/infocenter/aix/v7r1/index.jsp?topic=%2Fcom.ibm.aix.security%2Fdoc%2Fsecurity%2Fbos_trusted_execution.htm

NOTE: The configuration of TE is dependant on the unique requirements of a given environment.

4.16 General Permissions Management

This section will focus on general permissions management i.e. general file and directory permissions and ownership.

4.16.1 General Permissions Management - suid and sgid files and programs (Scored)

Profile Applicability:

- Level 2

Description:

The system is audited for both `suid` and `sgid` files and programs.

Rationale:

An audit should be performed on the system to search for the presence of both `suid` and `sgid` files and programs. In order to prevent these files from being potentially exploited the `suid` and `sgid` permissions should be removed wherever possible.

Audit:

Re-execute the appropriate find command and review the output. This should reflect the changes made in the remediation section.

If there are non-local filesystems which cannot be un-mounted, use the following to find all `suid` and `sgid` files on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -perm -04000 -o -perm -02000 \) -
type f -ls
```

If all non-local filesystems are un-mounted:

```
find / \( -perm -04000 -o -perm -02000 \) -type f -ls
```

Remediation:

Review the currently mounted filesystems:

```
mount
```

Un-mount all non-local filesystems and cdrom media:

```
unmount <mount point>
```

If there are non-local filesystems which cannot be un-mounted, use the following to find all `suid` and `sgid`files on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -perm -04000 -o -perm -02000 \) -
type f -ls
```

If all non-local filesystems have been un-mounted:

```
find / \( -perm -04000 -o -perm -02000 \) -type f -ls
```

Review the files and where possible, use the `chmod` command to remove the appropriate `suid` or `sgid` bits:

```
chmod u-s <file>
chmod g-s <file>
```

4.16.2 General Permissions Management - un-owned files and directories (Scored)

Profile Applicability:

- Level 2

Description:

The system is audited for un-owned files and directories.

Rationale:

An audit should be performed on the system to search for the presence of un-owned files and directories. All files and directories should have a valid owner and group.

Audit:

Re-execute the appropriate `find` command.

If there are non-local filesystems which cannot be un-mounted, use the following to find all un-owned files and directories on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -type d -o -type f \) \( -nouser
-o -nogroup \) -ls
```

If all non-local filesystems have been un-mounted:

```
find / \( -type d -o -type f \) \( -nouser -o -nogroup \) -ls
```

The `find` command should yield not yield output

Remediation:

Review the currently mounted filesystems:

```
mount
```

Un-mount all non-local filesystems and cdrom media:

```
unmount <mount point>
```

If there are non-local filesystems which cannot be un-mounted, use the following command to find all un-owned files and directories on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -type d -o -type f \) \( -nouser
-o -nogroup \) -ls
```

If all non-local filesystems have been un-mounted:

```
find / \( -type d -o -type f \) \( -nouser -o -nogroup \) -ls
```

NOTE: An un-owned file or directory is referred to via the GID or UID as it cannot be translated to a user or group name in `/etc/group` or `/etc/passwd`. This is typically caused by removing users or groups from the system.

Remediate the un-owned file and directory list:

```
chown <owner> <file>
chgrp <group> <file>
```

4.16.3 General Permissions Management - world writable files and directories (Scored)

Profile Applicability:

- Level 2

Description:

The system is audited for world writable files and directories.

Rationale:

An audit should be performed on the system to search for the presence of world writable files and directories. Files and directories should only be world writable when absolutely necessary.

Audit:

Re-execute the appropriate `find` command.

If there are non-local filesystems which cannot be un-mounted, use the following to find all world writable files and directories on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -type d -o -type f \) -perm -o+w
-ls
```

If all non-local filesystems have been un-mounted:

```
find / \( -type d -o -type f \) -perm -o+w -ls
```

NOTE: Review the output based on the performed remediation

Remediation:

Review the currently mounted filesystems:

```
mount
```

Un-mount all non-local filesystems and cdrom media:

```
unmount <mount point>
```

If there are non-local filesystems which cannot be un-mounted, use the following to find all world writable files and directories on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -type d -o -type f \) -perm -o+w
-ls
```

If all non-local filesystems have been un-mounted:

```
find / \( -type d -o -type f \) -perm -o+w -ls
```

Review the world writable files and directories and where possible, if the application configuration allows, remove access via:

```
chmod o-w <dir or file>
```

If a directory must retain world writable access, ensure that sticky bit is set so that users can only remove the files they create:

```
chmod o+t <dir>
```

NOTE: This will retain world writable permissions, but add a sticky bit to the directory.

5 Final Steps

This section will describe the process to reboot and backup the operating system - post customization.

5.1 System Reboot and Backup

Once all of the customization has been successfully performed, reboot the server to initialize all of the new security settings:

```
shutdown -Fr 0
```

When the system has been successfully rebooted, create a mksysb system backup to reflect the new server configuration:

If writing to tape:

```
mksysb -i /dev/rmt<x>
```

If writing to a file:

```
mksysb -i <pathname to file>
```

NOTE: The mksysb can subsequently be used as a source to install new systems, which ensures compliance to this benchmark. If this is intended, it is recommended that a bosinst_data resource is created within NIM and that the following parameter is defined:

```
RECOVER_DEVICES = no
```

Appendix: Change History

Date	Version	Changes for this version
09-20-2013	1.1.0	Resolved Ticket #22 - Missing 3.2.2 - 3.2.9
07-01-2013	1.0.0	Initial Public Release