DISCLAIMER! This document is nothing more than the musings of the author as he attempts to perform the stated tasks. Conclusions and approaches
may very well be incorrect, inefficient, or otherwise outside of professionally accepted best practices. Use this document at your own risk! In this
document, screen outputs will be presented in **green**. Where keyboard input is required, the prompt will be in bolded red. **#** means you should be at the
super user prompt, **$** means you should be at an unprivileged user prompt. Do not include these prompts in your input! The command to be typed will be
shown in **blue**.

 # ls -al

means you type ls -al at the super user prompt. **V825 - No 'mesg -n' in login scripts**

The mesg -n in the users .login or profile restricts the ability to use the write or talk commands to contact a user at his/her terminal. It also strengthens the permissions of the user's tty device.

To implement, do the following:

```
echo Set “mesg n” as default for all users
cd /etc
for file in profile .login
do
if [ "`grep mesg $file`" ]; then
awk ‘$1 == “mesg” { $2 = “n” }
{ print }’ $file >$file.new
mv $file.new $file
else
echo mesg n >>$file
fi
pkgchk -f -n -p /etc/$file
done
```

V950 - /usr/aset/userlist not protected

The Automated Security Enhancemen Tool (ASET)

ASET is a security package that provides automated administration tools for controlling and monitoring system security. It runs various tasks that perform specific checks and adjustments based on the *level* at which ASET is run — one of low, medium, or high (access permissions of many files restricted). ASET tasks include:

- System file permissions tuning
- System file checks
- User and group checks
- System configuration files check (in /etc)
- Environment variables check

- EEPROM check
- Firewall setup

The fix is to chmod 0600 /usr/aset/userlist

V22304 Passwords encryption needs to be FIPS 140.2 compliant

Systems must employ cryptographic hashes for passwords using the SHA-2 family of algorithms or FIPS 140-2 approved successors. The use of unapproved algorithms may result in weak password hashes more vulnerable to compromise. I can't find anything on how to force this. The documentation I found just said to change non-compliant passwords.

V22462 Cipher Directive does not appear in /etc/ssh/ssh_config

add the directive. As follows:

Ciphers aes256-ctr,aes192-ctr,aes128-ctr,arcfour256,aes128-cbc

V22459 Cipher Directive does not appear in /etc/ssh/sshd_config

add the directive. As follows:

Ciphers aes256-ctr,aes192-ctr,aes128-ctr,arcfour256,aes128-cbc **V22488 SSH Compression not set to Delayed or Off**

Per SSH Man Page, Compression Specifies whether compression is allowed, or delayed until the user has authenticated successfully. The argument must be "yes","delayed", or "no". The default is "delayed". add directive to /etc/ssh/sshd_config as follows:

Compression Delayed