CXL SECURE

AZScan

Report for
Demo

07-Dec-2008 18:20

Report for	Demo
Company	CXL Finance
Business Unit	Finance Division
Location	London
System	FINSYS202

Report Name	c:\tbxnew-works\reports\myrepu.doc
Report Date	07-Dec-2008 18:20

Key to colors

Risks	L Low risk	M Medium risk	H High risk
Results	L Correct or low risk	M Medium impact	H Major problem

1 UPWDSUser Passwords

1.1	DUPPWD	L Duplicate names in password file	H 9 users.
1.2	NOPWD	H Users without passwords	H 5 users.
1.3	DISPWD	L Disabled accounts	M 11 users.
1.4	BADFIELD	M Incorrect number of fields	M 2 users.
1.5	UNMATCH	M Unmatched password file entries	H 47 users.
1.6	PWDLIFE	M Password lifetimes	H 80 users.
1.7	ACCTINFO	L Account information	L

2 UUIDSUser UIDs

2.1	ZEROUID	M UID=0	M 5 users.
2.2	NOUID	H No UID	H 26 users.
2.3	BADUID	H Invalid UIDs	H 4 users.
2.4	DUPUID	M Duplicate UIDs in the password file	H 35 users.

3 UGIDSUser GIDs

3.1	ZEROGID	L Users with GID=0	H 7 users.
3.2	NOGID	M Users with no GID	H 28 users.
3.3	BADGID	M Users with an invalid GID	H 4 users.
3.4	DUPGID	L Duplicate GIDs in the password file	H 44 users.
3.5	EXSTGID	L Non-existent GIDs	H 18 users.

4 UHDIRS.User Home dirs.

4.1	NOHDIR	L No home directory	H 26 users.
4.2	INVHDIR	M Invalid home directory	H 54 users.
4.3	SHAREHDIR	L Shared home directory	H 29 users.
4.4	STKYHDIR	L Home directory NOT sticky	L 0 users.

4.5	WRITEHDIR	(M) Writeable home directory	(L) 0 users.
4.6	SUSHDIR	(H) Home directory contains suspicious files	(H) 27 users.

5 USHELLSUser Shells

5.1	NOSHELL	(L) No shell shown	(H) 29 users.
5.2	INVSHELL	(L) Invalid shells	(H) 12 users.
5.3	SHARESHELL	(L) Shared shells	(M) 38 users.
5.4	SUIDSHELL	(M) Shells which are SUID/SGID	(H) 40 users.
5.5	WRITESHELL	(M) Shells which are writeable	(H) 42 users.

6 GRPSGroups

6.1	DUPGRPNAME	(L) Duplicate group names	(H) 1 groups.
6.2	PWDGROUP	(L) Password protected	(L) 1 groups.
6.3	BADFIELDS	(L) Improper number of fields	(H) 2 groups.
6.4	NOUSERGRP	(L) No users	(H) 5 groups.
6.5	BADUSER	(L) Non-existent users	(H) 7 groups.
6.6	DUPUSER	(L) Duplicate users	(H) 6 groups.
6.7	USRSGRP	(L) Users in each group	(L) 16 groups.

7 GRPGIDSGroup GIDs

7.1	ZEROGID	(L) GID=0	(H) 2 groups.
7.2	NOGID	(L) No GID	(H) 3 groups.
7.3	BADGID	(L) Invalid GIDs	(H) 2 groups.
7.4	DUPGID	(L) Duplicate GIDs	(H) 4 groups.

8 FILESFiles

8.1	UKNOWNR	(L) Files - Unknown owners	(H) 9 files.
8.2	UKNGRPS	(L) Files - Unknown groups	(H) 35 files.
8.3	WLDWRITE	(M) Files - WORLD writeable	(H) 14 files.
8.4	WLDEXEC	(M) Files - WORLD executable	(L) 3 files.
8.5	GRPWRIT	(L) Files - GROUP writeable	(H) 124 files.
8.6	GRPEXEC	(L) Files - GROUP executable	(L) 2 files.
8.7	BADPRIV	(M) Files - Uneven privileges	(H) 13 files.
8.8	SUID	(L) Files - SUID	(L) 1 files.
8.9	SGID	(L) Files - SGID	(L) 1 files.
8.10	STICKY	(L) Files - Sticky	(L) 1 files.
8.11	SUID+WW	(M) Files - SUID/SGID and WORLD executable/writeable	(M) 4 files.
8.12	HOSTINFO	(M) Files likely to contain host information	(M) 4 files.
8.13	SUWW	(H) Startup files which are world writeable	(M) 4 files.

9 DIRSDirectories

9.1	UNKOWN	M Dir - Unknown owners	M 3 dirys.
9.2	UNKGRP	L Dir - Unknown groups	H 15 dirys.
9.3	WRLDWRT	M Dir - WORLD writeable	H 8 dirys.
9.4	WRLDEXE	M Dir - WORLD executable	L 1 dirys.
9.5	GRPWRT	M Dir - GROUP writeable	H 64 dirys.
9.6	GRPEXE	M Dir - GROUP executable	M 2 dirys.
9.7	BADPRIV	M Dir - Uneven privileges	H 6 dirys.
9.8	SGID	L Dir - SGID	H 72 dirys.
9.9	NSTICKY	L Dir - Not Sticky	H 7 dirys.

10 FTPFTP

10.1	FTPOWNBIN	L Anonymous FTP bin directory has wrong owner	L Dir. not found.
10.2	FTPOWNETC	M Anonymous FTP etc directory has wrong owner	L Dir. not found.
10.3	FTPHDIROWN	M Anonymous FTP home directory has wrong owner	L Dir. not found.

11 /ETC/etc

11.1	ETCWW	M Directories under /etc has world write access	L False
11.2	ETCPWD	M File /etc/default/passwd has insecure permissions	H True
11.3	ETCPROF	M File /etc/profile has insecure permissions	L False

12 LOG FILESLog files

12.1	LOGLOGEX	M The login log file does not exist	M
12.2	LOGLOGOWN	M Login log not correctly owned	M

14 AIXAIX15 NISNIS

15.1	NISUSED	L Is NIS being used.	L

1 UPWDS - User Passwords

RISKS

Passwords are the main access control mechanism employed to prevent unauthorised access to you system.
Users with short, easy to guess or non-existent passwords all make your system vulnerable to attack.

1.1 DUPPWD - Duplicate names in password file

L

RISKS

If the PASSWORD file has been manually edited, it is possible that someone could have created a duplicate user.
This will confuse the operating system and administrators and should be rectified.

ACTIONS

Delete the duplicate users so that each user is unique.

H

RESULTS

```
Name                Number
--------------------
cbea                2
dup1                2
tkea                3
yxxxx               2

9 users found
```

1.2 NOPWD - Users without passwords

H

RISKS

There is a high risk of unauthorised access to your system from accounts which do not require a password.
A user without a password has nothing in the second field of the password file. If a shadow password file is being used however, this field in the shadow file will be blank and the ordinary password file will contain a o or and !.
Anyone knowing (or guessing) these user-IDs can log on without a password and access your system.

ACTIONS

Ensure that every user MUST have a valid password.Enforce password ageing if available.

H

RESULTS

```
The following users do NOT have a password:

gopherr          | marvel           | kell             | bin
adm

5 users found
```

1.3 DISPWD - Disabled accounts

L

RISKS

These users cannot access your system since their password is disabled.
If the user does a remote login to another machine which is classed as a trusted host, they will not be required to enter a password and will simply be logged in.

ACTIONS

Delete these accounts if no longer required orSet the login shell to a non-existent filename.Set the home directory to a non-existent directory.Do NOT delete any system accounts such as root,bin,sys,uucp,nobody or daemon.

M

RESULTS

```
The following users have a disabled password:

akel             | ftp              | fxxxx            | gophera
gxxxx            | ixxxx            | jlee             | jste
kxxxx            | ldru             | lxxxx

11 users found
```

1.4 BADFIELD - Incorrect number of fields

M

RISKS

Password files consist of 7 fields:
user-ID : password : UID : GID : text field : home directory : shell
Fields are separated by colons.
If the wrong number of fields are in the file, the system will become confused (e.g. the GID could be read as the UID).

ACTIONS

Examine the password file and ensure that every user has the correct number of fields in each user record.

M

RESULTS

```
The following users have the wrong number of fields:

dgol            has only 6 fields.
rden            has only 6 fields.

2 users found
```

1.5 UNMATCH - Unmatched password file entries

M

RISKS

If a shadow password file is being used every entry in the normal password file should have an equivalent entry in the shadow file and visa versa.
The password field in the normal password file should be + o or ! and the encrypted password field (e.g. Fg1k92H/YfqtW) should be found in the shadow password file.
Reliance on the encrypted password field may not be possible and unauthorised access could be gained.

ACTIONS

Examine all entries which are unmatched and delete those which are no longer required.

H

RESULTS

```
These users do NOT have entries in the shadow password file although they
do have entries in the ordinary password file:

adm             | axxxx           | baduser2        | baduser3
bin             | bxxxx           | cbea            | cbea
cgia            | cgra            | cxxxx           | daemon
dup1            | edel            | emil            | gopher7
gopher8         | gopher9         | guest           | hxxxx
i1xxx           | i2xxx           | jcut            | jcut2
lbro            | ldix            | lpd             | MrLongName
MyLongerName    | news            | nobody          | rden
rerw            | rgue            | root            | sxxxx
sys             | tjab            | tkea            | tkea
tkea            | uucp            | vdor            | vsor
vxxxx           | xxxxx           | yxxxx

47 users found
```

1.6 PWDLIFE - Password lifetimes

M

RISKS

On some versions of Unix, password lifetime information is included in the password file or shadow file, at the end of the encrypted password. In others it will be found in a configuration file which is not examined by UScan.
A comma followed by some characters provide information about the maximum and minimum password lifetimes.
If this information is available in your files, it will be shown below.
The max. lifetime means the user must change his password every x weeks.
The min. lifetime means the user must keep the new one for y weeks.
Long maximum lifetimes increase the risk of passwords becoming widely known.
Short minimum lifetimes (change intervals) mean that a user can change the password back to his original one very quickly.

ACTIONS

Implement a minimum/maximum password lifetime for each user.

H

RESULTS

```
The max. password lifetime policy states 90 days.
The min. password lifetime policy states 60 days.
A  *  against a figure indicates that this setting is out of policy.

                Max. Days  Min. Days |                Max. Days  Min. Days
User-ID         Lifetime   Lifetime  | User-ID         Lifetime   Lifetime
--------------------------------------|--------------------------------------
nxxxx           11         1*        | oxxxx           44         38*
rxxxx           60         0*        | txxxx           0          0*
www             7          3*        | zxxxx           12         49*

6 users found

The following users do not have a password life time set:

adm             akel            anonymou        axxxx
baduser2        baduser3        bin             bxxxx
cbea            cbea            cgia            cgra
cxxxx           daemon          dgol            dup1
dup1            dxxxx           edel            emil
exxxx           ftp             fxxxx           gopher
gopher7         gopher8         gopher9         gophera
gopherr         guest           gxxxx           hxxxx
i1xxx           i2xxx           ixxxx           jcut
jcut2           jlee            jste            kell
kpit            kxxxx           larr            lbro
ldix            ldru            lpd             lxxxx
marvel          MrLongName      mxxxx           MyLongerName
news            nobody          pxxxx           qxxxx
rden            rerw            rgue            root
shal            sxxxx           sys             tjab
tkea            tkea            tkea            tlit
tllo            uucp            uxxxx           vdor
vsor            vxxxx           wais            wwwa
wxxxx           xxxxx           yxxxx           yxxxx

80 users found
```

1.7 ACCTINFO - Account information

RISKS

Some shadow password files contain user information such as how long the account may be used for and the life of the password.
The columns below are:
- o PWD LAST CHANGED The date when the password was last changed.
- o MIN DAYS The minimum number of days before a user can change a password (to prevent immediately returning to old password)
- o MAX DAYS The maximum days that a password is valid for.
- o WARN DAYS Number of days warning that a password needs changing.
- o INACT DAYS Number of days of inactivity allowed for that user.
- o A/C EXPIRES The absolute days when the account cannot be used.

Passwords which are not changed for long periods can become widely known resulting in unauthorised access.

ACTIONS

Compare the figures below with your company standard and highlight any which fall below. Make all users conform to the standard.

RESULTS

User-ID	Pwd last changed	Min days	Max days	Warn days	Inact days	Account expires
adm	27Dec2005	2	30	5	90	26Apr2005
akel	12Nov2005	2	30	5	90	21May2005
anonymou	12Nov2005	2	30	5	90	18May2005
baduser2	30Apr2005	4	30	5	90	14Nov2005
baduser3	17Nov2005	5	30	5	90	10May2005
bin	12Nov2005	2	30	5	90	26Apr2005
daemon	12Nov2005	2	30	5	90	26Apr2005
dgol	12Nov2005	2	30	5	90	23May2005
dup1	15Nov2005	3	30	5	90	09May2005
dxxxx	15Nov2005	0	90	0	30	-
exxxx	15Nov2005	0	90	0	30	-
ftp	12Nov2005	2	30	5	90	26Apr2005
fxxxx	15Nov2005	0	90	0	30	26Apr2005
gopher	19Nov2005	7	90	0	30	-
gophera	20Nov2005	8	90	0	30	-
gopherr	23Nov2005	11	30	5	90	12May2005
guest	12Nov2005	0	90	0	30	17Jan2006
gxxxx	15Nov2005	0	90	0	30	26Apr2005
hxxxx	15Nov2005	0	90	0	30	26Apr2005
ixxxx	16Nov2005	0	40	0	30	26Apr2005
jcut	13Jun1993	00	30	12900	0	-
jlee	27Nov2005	15	30	5	90	27Nov2005
jste	12Nov2005	2	30	5	90	19May2005
kell	12Nov2005	2	30	5	90	25May2005
kpit	26Nov2005	14	90	0	30	-
kxxxx	03Aug2005	0	50	0	22	14Nov2005
larr	12Nov2005	2	30	5	90	20May2005
ldru	12Nov2005	2	30	5	90	24May2005
lpd	14Nov2005	2	30	5	90	29Apr2005
lxxxx	29Jan2006	0	50	0	33	26Apr2005
marvel	24Nov2005	12	30	5	90	13May2005
MrLongName	21Nov2005	9	90	0	30	-
mxxxx	06Feb1994	0	90	0	30	-
MyLongerName	21Nov2005	9	90	0	30	-
nobody	13Nov2005	1	30	5	90	28Apr2005
nxxxx	24Jun1994	0	100			-
oxxxx	15Nov2005	0	90	0	30	-
pxxxx	24Jun1994	0	90	0	30	-
qxxxx	24Jun1994	0	10000			-
root	-	0	90	0	30	-
rxxxx	15Nov2005	0	50	0	34	26Apr2005
shal	12Nov2005	2	30	5	90	26May2005
sxxxx	24Jun1994	0	90	0	30	-
sys	12Nov2005	2	30	5	90	26Apr2005
tlit	18Nov2005	6	30	5	90	11May2005
tllo	15Nov2005	0	92	0	33	27May2005
txxxx	15Nov2005	0	90	0	30	26Apr2005
uucp	16Dec2005	2	30	5	90	27Apr2005
uxxxx	06Feb1994	0	90	0	30	-
vsor	28Nov2005	16	30	5	90	26May2005
wais	22Nov2005	10	90	0	30	-
www	21Nov2005	9	90	0	30	-
wwwa	25Nov2005	13	10000			-
wxxxx	15Nov2005	0	90	0	30	26Apr2005
xxxxx	15Nov2005	0	90	0	30	26Apr2005
yxxxx	24Jun1994	0	90	0	30	26Apr2005
zxxxx	29Apr2005	0	90	0	30	14Nov2005
zxxxx	29Apr2005	0	90	0	30	14Nov2005

57 users found

2 UUIDS - User UIDs

RISKS

On Unix systems, the User Identification (UID) is used to define the user to the operating system. The username is not actually used - only by the account owner when signing-on.
Normally, the system manager will give every user a different UID and it is this number which is used to determine the user's privileges.

2.1 ZEROUID - UID=0

M

RISKS

On many Unix systems users with UID=0 are SUPERUSERs. Usually this user is called ROOT but any other users with a UID of 0 will have the same high privileges.
Anyone with a UID of 0 runs without any security checks being performed and the user will have full access to the whole system.
A super user can do the following:
- o Read, modify or delete any file on the system
- o Run any program including compilers
- o Add, change or delete users' accounts
- o Become any other user on the system
- o Access any working device
- o Shut down the computer

ACTIONS

Ensure that every user shown below really should have these privileges.Change the UID of any user who does not need these facilities.

M

RESULTS

```
The following users have a UID=0:

dgol            | edel            | larr            | lxxxx
rerw

5 users found
```

2.2 NOUID - No UID

H

RISKS

This is an odd situation. The system needs a UID to recognise a user since it does not use their user-ID. Thus a user without a UID cannot sign on and does not really exist.

ACTIONS

Delete these users or give them a valid, non-zero UID.Do NOT delete any system accounts such as root,bin,sys,uucp,nobody or daemon.

H

RESULTS

The following users do NOT have a UID:

adm	baduser2	baduser3	bin
bxxxx	daemon	guest	hxxxx
ixxxx	jcut	lbro	lpd
MrLongName	MyLongerName	news	nobody
rden	root	sxxxx	sys
tllo	uucp	vdor	vsor
vxxxx	xxxxx		

26 users found

2.3 BADUID - Invalid UIDs

H

RISKS

A valid UID is one which is an integer in the range 0 to 65535.
Most systems will only recognise UIDs in this range and thus any shown below have something wrong with them.
UIDs are essential for the operating system to recognise the user (not the user-ID).
An unrecognised user may be treated in an unpredictable way by the system.

ACTIONS

Find out why these users have invalid UIDs. Change them to correct values.

H

RESULTS

The following users have an invalid UID:

User	UID	User	UID
cbea	hu229	kpit	899999
tkea	98909	tlit	AA200

4 users found

2.4 DUPUID - Duplicate UIDs in the password file

M

RISKS

Users with duplicate UIDs are treated by the system as being the same person since the system only recognises UIDs, not user-IDs. This is going to cause confusion especially if the accounts have different permissions.
Users will be treated with the same privileges and access to the system.

ACTIONS

Ensure that every user has a unique and valid numeric UID.

H

RESULTS

```
The following duplicate UIDs are used:

UID=0
dgol            | edel            | rerw            | lxxxx
larr

UID=222
dup1            | gopherr         | dup1

UID=225
cgia            | tjab

UID=229
tkea            | cbea

UID=3
mxxxx           | txxxx           | rxxxx           | qxxxx
yxxxx           | yxxxx           | wxxxx           | nxxxx
pxxxx           | kxxxx           | i2xxx           | i1xxx
gxxxx           | fxxxx           | exxxx           | cxxxx
axxxx           | zxxxx           | oxxxx

UID=7
gophera         | gopher7         | gopher8         | gopher9

35 users found

6 UIDs are duplicated.
```

3 UGIDS - User GIDs

RISKS

Every user belongs to one or more groups. Groups are used to collect together users with similar jobs or access to the system.
Like users, each group is given a unique number called a GID which the system recognises to extend the users access to files and directories.

3.1 ZEROGID - Users with GID=0

L

RISKS

The group with a GID of zero is often referred to as the 'system' or 'wheel' group. On many Unix systems only users in this group are able to use the su command. Thus only these users can become super users.
Users in this group could become super users with full access to the system.
The ROOT account will normally be found in this group and is not a problem.

ACTIONS

Review any users shown below and ensure that you are happy for them to possibly become super users.

H

RESULTS

```
The following 'primary' users have a GID=0:

gxxxx           | kpit            | larr            | ldru
rerw            | tlit            | yxxxx

7 users found



The following 'secondary' users have a GID=0:


0 users found
```

3.2 NOGID - Users with no GID

M

RISKS

This is an odd situation. The system needs a GID to recognise a user's GROUP.

ACTIONS

Delete these users or give them a valid, non-zero GID.Do NOT delete any system accounts such as root,bin,sys,uucp,nobody or daemon.

H

RESULTS

```
The following users do NOT have a GID:

adm              | baduser2         | baduser3         | bin
cxxxx            | daemon           | dgol             | edel
emil             | guest            | hxxxx            | ixxxx
jcut             | jcut2            | lbro             | lpd
MrLongName       | MyLongerName     | nobody           | root
shal             | sxxxx            | sys              | tjab
uucp             | uxxxx            | vsor             | xxxxx

28 users found
```

3.3 BADGID - Users with an invalid GID

M

RISKS

The users listed below have invalid GIDs. This is dangerous if the GID translates into a number (e.g. kl0 maybe taken as GID=0).
Users in these groups could become super users with full access to the system.

ACTIONS

Change to a legal numeric value.

H

RESULTS

```
The following users have an invalid GID:

jlee             99990               | tkea             QQ
tkea             90206               | tkea             gg206

4 users found
```

3.4 DUPGID - Duplicate GIDs in the password file

L

RISKS

These users share GIDs. This is not a problem but you should be aware that these users are likely to have the same access profiles to the same files and programs.
Users in these groups could gain unintended access to parts of the system.

ACTIONS

Review users in each group and ensure that they should be grouped in the way they are.

H

RESULTS

```
The following GIDs are shared:

GID=-2
marvel          | gopher

GID=0
gxxxx           | ldru            | rerw            | larr
tlit            | yxxxx           | kpit

GID=1
anonymou        | vdor            | wais            | akel
www

GID=12
gopher8         | gophera         | gopherr         | dup1
dup1            | gopher9         | gopher7

GID=206
tllo            | cgra            | cgia            | cbea
rden            | ldix            | jste            | cbea

GID=207
mxxxx           | wxxxx           | vxxxx           | txxxx
rxxxx           | qxxxx           | pxxxx           | oxxxx
nxxxx           | lxxxx           | bxxxx           | i2xxx
axxxx           | exxxx           | kxxxx

44 users found
```

3.5 EXSTGID - Non-existent GIDs

L

RISKS

These users have GIDs of groups which do not exist in the group file.
Essentially users do not belong to an initial group.

ACTIONS

Reassign these users to valid groups or delete them.Do NOT delete any system accounts such as root,bin,sys,uucp,nobody or daemon.

H

RESULTS

```
User              GID
--------------------
akel              1
anonymou          1
dxxxx             766
fxxxx             987
gopher            -2
i1xxx             932
jlee              99990
kell              1206
marvel            -2
news              208
rgue              -206
tkea              90206
vdor              1
wais              1
www               1
wwwa              9207
yxxxx             223
zxxxx             211

18 users found
```

4 UHDIRS. - User Home dirs.

RISKS

When a user successfully logs onto a system, they are placed in their home directory. This directory may contain their own start-up programs or menus and is used to configure their start-up.

4.1 NOHDIR - No home directory

L

RISKS

On some systems, not having a home directory may prevent a user from logging on to the system and they will be returned to the login prompt.
On other systems the user will be placed in the ROOT directory with the message 'Changing directory to /'.
Initial programs or menus may not be activated when the user logs on.

ACTIONS

Ensure that every user has a valid home directory.This may be used as a means of disabling the account in which case it would be better to delete the user all together. Do NOT delete any system accounts such as root,bin,sys,uucp,nobody or daemon.

H

RESULTS

```
The following users do NOT have a home directory set:

adm              | baduser2         | baduser3         | bin
daemon           | dgol             | emil             | exxxx
guest            | hxxxx            | ixxxx            | jcut
lbro             | lpd              | MrLongName       | mxxxx
MyLongerName     | news             | nobody           | rden
root             | sxxxx            | sys              | uucp
vsor             | xxxxx

26 users found
```

4.2 INVHDIR - Invalid home directory

M

RISKS

On some systems, not having a valid home directory may prevent a user from logging on to the system and they will be returned to the login prompt.
On other systems the user will be placed in the ROOT directory with the message 'Changing directory to /'.
Initial programs or menus may not be activated when the user logs on.

ACTIONS

Ensure that every user has a valid home directory.This may be used as a means of disabling the account in which case it would be better to delete the user all together. Do NOT delete any system accounts such as root,bin,sys,uucp,nobody or daemon.

H

RESULTS

```
User            Directory
-------------------------
adm
akel            /bin/hh1/
anonymou        /anonftp/
baduser2
baduser3
bin
cbea            /u/cbea/
cbea            /u/cbea/
cgra            /u/cgra/
daemon
dgol
dup1            /prod/gopher/data/
dup1            /prod/gopher/data/
edel            /u/edel/
emil
exxxx
ftp             /anonftp/
gopher          /home/gopher/
gopher7         /marvel/gopher/data/
gopher8         /marvel/gopher/data/
gopher9         /marvel/gopher/data/
gophera         /marvel/gopher/data/
gopherr         /prod/gopher/data/
guest
hxxxx
i1xxx           /etc/jj/
i2xxx           /etc/jj/
ixxxx
jcut
jlee            /u/jlee/
jste            /u/jste/
kpit            /u/kpit/
lbro
ldix            /u/ldix/
ldru            /u/ldru/
lpd
marvel          /home/gopher/
MrLongName
mxxxx
MyLongerName
news
nobody
qxxxx           /myhomedir/
rden
rerw            /u/rerw/
root
sxxxx
sys
tlit            /u/tlit/
tllo            /u/tllo/
uucp
vdor            /u/vsor/
vsor
xxxxx

54 users found
```

4.3 SHAREHDIR - Shared home directory

L

RISKS

These users share home directories and are thus likely to have similar access profiles. Ensure that you are satisfied with these groupings of users.
A change made to one user could impact several others.

ACTIONS

Review the users sharing each home directory.

H

RESULTS

```
The following home directories are shared:

Home directory=/bin/
oxxxx           | zxxxx           | yxxxx           | yxxxx
wxxxx           | vxxxx           | uxxxx           | txxxx
fxxxx           | pxxxx           | wais            | nxxxx
lxxxx           | kxxxx           | gxxxx           | dxxxx
cxxxx           | bxxxx           | rxxxx

Home directory=/usr/
tjab            | axxxx

Home directory=/u/larr/
larr            | kell            | shal            | jcut2

Home directory=/u/tkea/
rgue            | tkea            | tkea            | tkea

29 users found

4 home directories are shared.
```

4.4 STKYHDIR - Home directory NOT sticky

L

RISKS

If a directory is flagged as sticky, files in the directory can only be removed, renamed or unlinked by:
- the file owner
- the directory owner
- the super user.

Other users could modify or delete the data files or programs in the user's home directory.

ACTIONS

Ensure that all home directories have this set.

L

RESULTS

```
0 users found
```

4.5 WRITEHDIR - Writeable home directory

M

RISKS

If a user's home directory is world or even group writeable, other people can modify the files.
This is an easy way of for a hacker to gain the password of a user by inserting a password capturing program into the user's home directory, for example masquerading as the ls command.

ACTIONS

Remove the write permission from the directory.Suggested permissions are:owner:rwx group:r-x world:--- (e.g. drwxr-x---)Use chmod a-w HomeDirName or chmod 750 HomeDirName

L

RESULTS

```
0 users found
```

4.6 SUSHDIR - Home directory contains suspicious files

H

RISKS

Users should not have 'system' files in their home directories.
If they are able to replace the 'real system' files with their own modified files, they could severely disrupt the system. They may be developing a new 'ls' command which corrupts files instead of listing directories.

ACTIONS

Examine these files and discover what they are and what they do.Ask the user why they are there and then remove them.

H

RESULTS

```
User bxxxx       /bin/shadow
User cxxxx       /bin/shadow
User dxxxx       /bin/shadow
User fxxxx       /bin/shadow
User gxxxx       /bin/shadow
User jcut2       /u/larr/cron
User kell        /u/larr/cron
User kxxxx       /bin/shadow
User larr        /u/larr/cron
User lxxxx       /bin/shadow
User nxxxx       /bin/shadow
User oxxxx       /bin/shadow
User pxxxx       /bin/shadow
User rgue        /u/tkea/passwd
User rxxxx       /bin/shadow
User shal        /u/larr/cron
User tkea        /u/tkea/passwd
User tkea        /u/tkea/passwd
User tkea        /u/tkea/passwd
User txxxx       /bin/shadow
User uxxxx       /bin/shadow
User vxxxx       /bin/shadow
User wais        /bin/shadow
User wxxxx       /bin/shadow
User yxxxx       /bin/shadow
User yxxxx       /bin/shadow
User zxxxx       /bin/shadow

27 Files found
```

5 USHELLS - User Shells

RISKS

Shells are a means of providing the user with an operating system language which lets them perform a number of tasks easily.
Common shells are sh, ksh, and csh.

5.1 NOSHELL - No shell shown

L

RISKS

Every user should have a shell defined. This file should exist, be valid, and ideally should be a compiled program.
- o A binary (compiled) file only needs EXECUTE permission.
- o A script file will need READ permission.
- o The shell should not have the SUID/SGID bit set.

On some systems, the user cannot login if they do not have a shell.
On other systems, the account will be admitted onto the system using the default shell which is usually the Bourne shell.
The message produced will be:
Using /bin/sh

ACTIONS

Ensure that every user has a shell defined.This file should be a compiled program and should not have SUID/SGID set.

H

RESULTS

```
The following users do NOT have a shell set:

adm             | baduser2        | baduser3        | bin
cgia            | daemon          | dgol            | fxxxx
guest           | hxxxx           | ixxxx           | jcut
jste            | lbro            | lpd             | lxxxx
MrLongName      | mxxxx           | MyLongerName    | nobody
rden            | root            | sxxxx           | sys
tkea            | tkea            | uucp            | vsor
xxxxx

29 users found
```

5.2 INVSHELL - Invalid shells

L

RISKS

Every user should have a shell defined. This file should exist, be valid, and ideally should be a compiled program.

- A binary (compiled) file only needs EXECUTE permission.
- A script file will need READ permission.
- The shell should not have the SUID/SGID bit set.

On some systems, the user cannot login if they do not have a shell.
On other systems, the account will be admitted onto the system using the default shell which is usually the Bourne shell.
Some of these could still be valid if they are symbolic links to real files.

ACTIONS

Ensure that every user has a shell defined.If this file has been chosen to prevent the user from logging in, then decide whether this user still needs to be registered on the system.Delete them completely from the password file if they are no longer required.Do NOT delete any system accounts such as root,bin,sys,uucp,nobody or daemon.This file should be a compiled program and should not have SUID/SGID set.

H

RESULTS

```
User             Shell
---------------------
exxxx            /bin/myshell
gopher           /bin/gophshell
gopher7          /*
gopher9          /bin/ksh1
gopherr          /*
jcut2            /bin/ksh2
ldix             /usr/sys
marvel           /usr/bin/gophshell
qxxxx            /bin/myshell
tllo             /bin/ksh2
yxxxx            /bin/ksh/test1
zxxxx            /bin/zxxxxshell

12 users found
```

5.3 SHARESHELL - Shared shells

L

RISKS

These users share shells. If one user changes a file he will have an impact on the other users which may have undesirable consequences.

ACTIONS

Provide each user with an individual shell which can only be amended by them (or ROOT).

M

RESULTS

```
The following shell files are shared:

Shell file=/bin/file23
edel            | edel

Shell file=/bin/ksh
larr            | larr            | dup1            | gopher8
anonymou        | wwwa            | vdor            | dup1
jlee            | rerw            | wais            | ldru
i1xxx           | yxxxx           | wxxxx           | vxxxx
uxxxx           | txxxx           | rxxxx           | pxxxx
oxxxx           | nxxxx           | kxxxx           | i2xxx
emil            | tkea            | cgra            | tjab
rgue            | cbea            | tlit            | cbea
dxxxx

Shell file=/bin/ls
kell            | kell

Shell file=/bin/sh
bxxxx           | bxxxx           | axxxx           | cxxxx

Shell file=/binx/myshell
gophera         | gophera

38 users found
```

5.4 SUIDSHELL - Shells which are SUID/SGID

M

RISKS

A shell with SUID/SGID set could give the user the ability to execute privileged commands.

ACTIONS

Find out and justify the need for the SUID/SGID bit setting. Remove this bit from the permissions.

H

RESULTS

```
User              Permission       Shell
-----------------------------------------
akel              ---X-WSRWX       /bin/file23
anonymou          ---X-WSRWX       /bin/ksh
axxxx             ---X-WSRWX       /bin/sh
bxxxx             ---X-WSRWX       /bin/sh
cbea              ---X-WSRWX       /bin/ksh
cbea              ---X-WSRWX       /bin/ksh
cgra              ---X-WSRWX       /bin/ksh
cxxxx             ---X-WSRWX       /bin/sh
dup1              ---X-WSRWX       /bin/ksh
dup1              ---X-WSRWX       /bin/ksh
dxxxx             ---X-WSRWX       /bin/ksh
edel              ---X-WSRWX       /bin/file23
emil              ---X-WSRWX       /bin/ksh
gopher8           ---X-WSRWX       /bin/ksh
gxxxx             ---X-WSRWX       /bin/sh
i1xxx             ---X-WSRWX       /bin/ksh
i2xxx             ---X-WSRWX       /bin/ksh
jlee              ---X-WSRWX       /bin/ksh
kpit              ---X-WSRWX       /bin/ksh
kxxxx             ---X-WSRWX       /bin/ksh
larr              ---X-WSRWX       /bin/ksh
ldru              ---X-WSRWX       /bin/ksh
nxxxx             ---X-WSRWX       /bin/ksh
oxxxx             ---X-WSRWX       /bin/ksh
pxxxx             ---X-WSRWX       /bin/ksh
rerw              ---X-WSRWX       /bin/ksh
rgue              ---X-WSRWX       /bin/ksh
rxxxx             ---X-WSRWX       /bin/ksh
shal              ---X-WSRWX       /bin/jxjx2
tjab              ---X-WSRWX       /bin/ksh
tkea              ---X-WSRWX       /bin/ksh
tlit              ---X-WSRWX       /bin/ksh
txxxx             ---X-WSRWX       /bin/ksh
uxxxx             ---X-WSRWX       /bin/ksh
vdor              ---X-WSRWX       /bin/ksh
vxxxx             ---X-WSRWX       /bin/ksh
wais              ---X-WSRWX       /bin/ksh
wwwa              ---X-WSRWX       /bin/ksh
wxxxx             ---X-WSRWX       /bin/ksh
yxxxx             ---X-WSRWX       /bin/ksh

40 users found
```

5.5 WRITESHELL - Shells which are writeable

M

RISKS

Where a binary file is being used the correct permissions are - --x --x --x
With a script file, READ permission is also required. This means that other users can read and copy the file.
A copy of a shell could be modified to cause serious user/system problems.

ACTIONS

Make sure the shells are binary files and have the permissions shown above.

RESULTS

```
User             Permission  Shell
---------------------------------
akel             ---x-wsrwx  /bin/file23
anonymou         ---x-wsrwx  /bin/ksh
axxxx            ---x-wsrwx  /bin/sh
bxxxx            ---x-wsrwx  /bin/sh
cbea             ---x-wsrwx  /bin/ksh
cbea             ---x-wsrwx  /bin/ksh
cgra             ---x-wsrwx  /bin/ksh
cxxxx            ---x-wsrwx  /bin/sh
dup1             ---x-wsrwx  /bin/ksh
dup1             ---x-wsrwx  /bin/ksh
dxxxx            ---x-wsrwx  /bin/ksh
edel             ---x-wsrwx  /bin/file23
emil             ---x-wsrwx  /bin/ksh
gopher8          ---x-wsrwx  /bin/ksh
gophera          -rw-rw-r--  /binx/myshell
gxxxx            ---x-wsrwx  /bin/sh
i1xxx            ---x-wsrwx  /bin/ksh
i2xxx            ---x-wsrwx  /bin/ksh
jlee             ---x-wsrwx  /bin/ksh
kpit             ---x-wsrwx  /bin/ksh
kxxxx            ---x-wsrwx  /bin/ksh
larr             ---x-wsrwx  /bin/ksh
ldru             ---x-wsrwx  /bin/ksh
nxxxx            ---x-wsrwx  /bin/ksh
oxxxx            ---x-wsrwx  /bin/ksh
pxxxx            ---x-wsrwx  /bin/ksh
rerw             ---x-wsrwx  /bin/ksh
rgue             ---x-wsrwx  /bin/ksh
rxxxx            ---x-wsrwx  /bin/ksh
shal             ---x-wsrwx  /bin/jxjx2
tjab             ---x-wsrwx  /bin/ksh
tkea             ---x-wsrwx  /bin/ksh
tlit             ---x-wsrwx  /bin/ksh
txxxx            ---x-wsrwx  /bin/ksh
uxxxx            ---x-wsrwx  /bin/ksh
vdor             ---x-wsrwx  /bin/ksh
vxxxx            ---x-wsrwx  /bin/ksh
wais             ---x-wsrwx  /bin/ksh
www              -rw-rw-r--  /binx/myshell
wwwa             ---x-wsrwx  /bin/ksh
wxxxx            ---x-wsrwx  /bin/ksh
yxxxx            ---x-wsrwx  /bin/ksh

42 users found
```

6 GRPS - Groups

RISKS

Every user belongs to one or more groups. Groups are used to collect together users with similar jobs or access to the system.

6.1 DUPGRPNAME - Duplicate group names

L

RISKS

This could confuse the system and there is possibly something wrong if these exist. Problems will arise when you add or remove names from a group.

ACTIONS

Rename duplicate groups correctly. Only leave the correct one.

H

RESULTS

```
Group                Number
-------------------------
ftp                       2

1 group found
```

6.2 PWDGROUP - Password protected

L

RISKS

Groups rarely need passwords as the security is handled by the user-ID.

ACTIONS

Remove the passwords and replace with a '*'.

L

RESULTS

```
The following groups have a password:

lawmex

1 group found
```

6.3 BADFIELDS - Improper number of fields

L

RISKS

The group file should contain records whose fields are separated by three colons. If not, unpredictable results will occur depending on which is the missing field.

ACTIONS

Fix these group records and ensure that there are only four fields.

H

RESULTS

```
The following groups have the wrong number of fields:

lawlib          has too many fields - 5
ecs             has only 3 fields.

2 groups found
```

6.4 NOUSERGRP - No users

L

RISKS

The following groups do not have any VALID users in them.
If these groups do not contain any users, why do they exist.

ACTIONS

Delete any unused and therefore unnecessary groups.Reassign group ownership of files and directories to groups populated with the appropriate users.

H

RESULTS

```
The following groups do not have any valid users:

ecs             | gopheru         | groupA          | law2
test

5 groups found
```

6.5 BADUSER - Non-existent users

L

RISKS

The following groups have non-existent users i.e. they do not exist in the password file.

ACTIONS

Examine the GROUP file and remove those users who are not present in the PASSWORD file.

H

RESULTS

```
The following users in these groups do not exist in the password file:


Group:ftp
news1           | dkdkd

Group:gophera
prog1           | prog2

Group:law1
lawuser         | Sid22           | lawuser

Group:lawbraz
user25          | user26          | user27          | user25
user25

Group:news
news1           | dkdkd

Group:test1
t

Group:wwwa
jxxxx           | z

7 groups found
```

6.6 DUPUSER - Duplicate users

L

RISKS

A user is listed more than once in a group. If a user is deleted, they may still keep their privileges.

ACTIONS

Remove the duplicates, leaving only one user in the list.

H

RESULTS

```
The following users are duplicated in the group file:

Group = gophera
tlit              | tlit
Group = lawbraz
user25            | user25           | user25
Group = ftpa
rden              | rden             | rden
Group = news
news              | news
Group = ftp
news              | news
Group = law1
lawuser           | lawuser

6 groups found
```

6.7 USRSGRP - Users in each group

L

RISKS

This is a simple list of users in each group.
It is possible that users have been assigned to the wrong group.

ACTIONS

Examine each group and ensure that the members of that group are all valid and appropriate for the functions performed by the group.

L

RESULTS

```
Group=lawlib
Primary -   uxxxx           | jcut2           | edel
Primary -   emil             | lbro            | dgol
Primary -   cxxxx            | shal            | tjab
Secondary -   None

Group=groupA
Primary -   None
Secondary -   None

Group=test
Primary -   None
Secondary -   None

Group=lawmex
Primary -   ldru             | larr            | tlit
Primary -   rerw             | kpit            | gxxxx
Primary -   yxxxx
Secondary -   None

Group=test1
Primary -   None
Secondary -   None

Group=gophera
Primary -   dup1             | gophera         | gopher7
Primary -   gopher9          | dup1            | gopherr
Primary -   gopher8
Secondary - vsor             | gophera         | gopherr
Secondary - cxxxx            | tlit

Group=gopheru
Primary -   None
Secondary -   None

Group=lawbraz
Primary -   None
Secondary -   None

Group=ftp
Primary -   ftp
Secondary -   None

Group=ftpa
Primary -   tllo             | cbea            | jste
Primary -   ldix             | rden            | cbea
Primary -   cgia             | cgra
Secondary - tkea             | rgue            | tkea
Secondary - tkea             | jcut            | edel
Secondary - emil             | lbro            | shal
Secondary - tjab             | ldru            | larr
Secondary - rerw             | tllo            | cbea
Secondary - jste             | rden            | cbea
Secondary - cgia             | cgra

Group=ecs
Primary -   None
Secondary -   None

Group=wwwa
Primary -   i2xxx            | wxxxx           | vxxxx
Primary -   txxxx            | rxxxx           | qxxxx
Primary -   pxxxx            | oxxxx           | nxxxx
Primary -   mxxxx            | kxxxx           | exxxx
Primary -   bxxxx            | axxxx           | lxxxx
Secondary - dxxxx            | yxxxx           | xxxxx
Secondary - fxxxx            | sxxxx           | ixxxx
```

7 GRPGIDS - Group GIDs

RISKS

Every user belongs to one or more groups. Groups are used to collect together users with similar jobs or access to the system.
Like users, each group is given a unique number called a GID which the system recognises to extend the users access to files and directories.

7.1 ZEROGID - GID=0

L

RISKS

On many Unix systems only users within these groups are able to use the SU (Set UID) command. Thus only these users can become super users.

ACTIONS

Review any groups shown below and ensure that you are happy for the users to possibly become super users.

H

RESULTS

```
The following groups have a GID of 0:

lawmex          | test1

2 groups found
```

7.2 NOGID - No GID

L

RISKS

Groups without a GID will severely confuse the system.

ACTIONS

Every group should have a unique group number which is reflected in the user profiles.

H

RESULTS

```
The following groups do NOT have a GID:

lawlib          | groupA          | test

3 groups found
```

7.3 BADGID - Invalid GIDs

L

RISKS

Groups with invalid or non-numeric GIDs can give strange results and produce unpredictable permissions.

ACTIONS

Change the GID to a valid number.

H

RESULTS

```
The following groups have an invalid GID:

ecs             206s            | law1            222Lawyer

2 groups found
```

7.4 DUPGID - Duplicate GIDs

L

RISKS

Groups with different names but the same GID will confuse the system.

ACTIONS

Ensure that each group has a unique GID and name or else move users and files into a single group.

H

RESULTS

```
GID=
groupA | lawlib          | test

GID=0
lawmex | test1

GID=207
news | wwwa

4 groups found
```

8 FILES - Files

RISKS

Files may contain data or be executable programs. When they are created, they will have an owner and a group. A number of privileges determine whether they can be written to, read or executed and by whom.

8.1 UKNOWNR - Files - Unknown owners

L

RISKS

The following users own files but do not have records in the PASSWORD file i.e. the owner no longer exists.

ACTIONS

Examine these files and either remove them and their files or assign them to new owners.

H

RESULTS

```
The following files have unknown owners:

Owner           file
--------------------
MrLongerN       /fred/profileLonger
MyLongNam       /fred/profileLong
236             /pub/.names
kell2           /pub/INDEX
238             /pub/copyright/carp94
user26          /pub/exh.images/vat.exh/exh/g-nature/Nature.txt
user27          /pub/exh.images/vat.exh/exh/g-nature/nature01.jpg
fred            /u/ztest.pgm
fred            /usr/test.pgm

9 Files found
```

8.2 UKNGRPS - Files - Unknown groups

L

RISKS

The following groups own files but do not have records in the GROUP file i.e. the group no longer exists.

ACTIONS

Examine these files and either remove them and their files or assign them new group ownership.

H

RESULTS

The following files are owned by unknown groups:

Group	File
system	/filezz
sys	/bin/jxjx1
sys	/bin/jxjx2
sys	/bin/ksh
sys	/bin/ls
system	/bin/profile
system	/bin/shadow
system	/bin/passwd
sys	/bin/sh
system	/etc/filexx
system	/etc/group
system	/etc/hosts.equiv
system	/etc/passwd
system	/fred/.rhost
system	/fred/.netrc
system	/fred/groupx
system	/fred/passwdx
system	/fred/profile
system	/fred/profileLonger
system	/fred/profileLong
system	/lib/libc.a#
system	/lib/libcurses.a
fccc	/pub/client.software/popmail/pop3.0/loadpop.exe
fabc	/pub/exh.images/1492.exh/WARNING
ftpa22	/pub/exh.images/1492.exh/exh/Intro.wp
system	/u/ztest.pgm
system	/u/larr/passwd1.Z
system	/u/larr/passwd2.Z
system	/u/larr/passwd3.Z
system	/u/larr/cron
system	/u/tkea/passwd
system	/u/tkea/tpasswd1
system	/u/tkea/tpasswd2
system	/usr/test.pgm
system	/usr/binx/myshell

35 Files found

8.3 WLDWRITE - Files - WORLD writeable

M

RISKS

Anyone can modify or delete these files.
This can be a security problem if the file can be used to gain root access (e.g. the password file).
The following points should also be noted:
o If a file does not have 'read' rights it can still have data appended to the end or it can be deleted and replaced.
o If a file has read rights the contents can be modified.
o With execute rights, a compiled program can be run but shell scripts require read rights.
o To write to a file a user does not need write access to the directory.
o A user must have 'execute' permission on the directory to do anything to the files.
o Files in directories which are sticky have NOT been shown since it is assumed that these can only be renamed or removed by the owner of the file, the owner of the directory or the super user.

ACTIONS

Remove world write from these files unless it is actually needed.Use chmod a-w <filename>

H

RESULTS

```
Attribute   File
----------------
-rw-rw-rw- /bin/profile
-rw-rw-rw- /bin/shadow
-rw-rw-rw- /bin/passwd
-rw-r--rw- /etc/filexx
-rw-r--rw- /etc/hosts.equiv
-rw-r--rw- /etc/passwd
-rw-rw-rw- /fred/.rhost
-rw-r--rw- /fred/.netrc
-rw-rw-rw- /fred/profile
-rw-rw-rw- /fred/profileLonger
-rw-rw-rw- /fred/profileLong
-rw-r--rw- /pub/client.software/gopher/dos/gophftp.exe
-r--rw-rw- /pub/client.software/gopher/dos/readme.ftp
-rw-rw-rwx /pub/exh.images/vat.exh/exh/g-nature/nature03.jpg

14 Files found
```

8.4 WLDEXEC - Files - WORLD executable

M

RISKS

Anyone can run the files here which are world executable.
Many of them are system commands designed to be used by everyone. (e.g. ls)
The following points should also be noted:
o With execute rights, a compiled program can be run but shell scripts require read rights.
o To write to a file a user does not need write access to the directory.
o A user must have execute permission on the directory to do anything to the files.
o In order to examine only the more important files, we have ignored files in directories whose path contains the word /bin/ or /sbin/.

ACTIONS

Examine the list of files and ensure that it is intended that everyone can run them. Remove world execute from these files unless it is actually needed.

L

RESULTS

```
Attribute  File
---------------
-r-xr-xr-x /lib/libc.a#
-rw-rw-r-x /pub/exh.images/vat.exh/exh/g-nature/nature02.jpg
-rw-rw-rwx /pub/exh.images/vat.exh/exh/g-nature/nature03.jpg

3 Files found
```

8.5 GRPWRIT - Files - GROUP writeable

L

RISKS

Any member of this file's group can modify or delete these files.
This can be a security problem if the file can be used to gain root access.
(e.g. the password file).
The following points should also be noted:
o If a file does not have read rights it can still have data appended to the end or it can be deleted and replaced.
o If a file has read rights the contents can be modified.
o With execute rights, a compiled program can be run but shell scripts require read rights.
o To write to a file a user does not need write access to the directory.
o A user must have execute permission on the directory to do anything to the files.
o Files in directories which are sticky have NOT been shown since it is assumed that these can only be renamed or removed by the owner of the file, the owner of the directory or the super user.

ACTIONS

Remove group write access from these files unless it is actually needed.

H

RESULTS

```
Attribute       Group           file
-------------------------------------
---x-wsrwx      sys             /bin/jxjx1
---x-wsrwx      sys             /bin/jxjx2
---x-wsrwx      sys             /bin/ksh
-rw-rw-rw-      system          /bin/profile
-rw-rw-rw-      system          /bin/shadow
-rw-rw-rw-      system          /bin/passwd
---x-wsrwx      sys             /bin/sh
-rw-rw-rw-      system          /fred/.rhost
-rw-rw-r--      system          /fred/passwdx
-rw-rw-rw-      system          /fred/profile
-rw-rw-rw-      system          /fred/profileLonger
-rw-rw-rw-      system          /fred/profileLong
-rw-rw-r--      ftpa            /pub/.rhostsx25
-rw-rw-r--      ftpa            /pub/README
-rw-rw-r--      ftpa            /pub/client.software/gopher/dos/README
-r--rw-rw-      ftpa            /pub/client.software/gopher/dos/readme.ftp
-rw-rw-r--      ftpa            /pub/client.software/gopher/dos/readme.v3#
-rw-rw-r--      ftpa            /pub/client.software/gopher/os2/goph1_61.txt
-rw-rw-r--      ftpa            /pub/client.software/gopher/os2/goph1_61.zip
-rw-rw-r--      ftpa            /pub/client.softwar..../os2/os2goph1_04.zip
-rw-rw-r--      ftpa            /pub/client.software/gopher/os2/README
-rw-rw-r--      ftpa            /pub/client.software/gopher/os2/gopher
-rw-rw-r--      ftpa            /pub/client.softwar....ndows/hgopher2.4.zip
-rw-rw-r--      ftpa            /pub/client.software/popmail/read.me
-rw-rw-r--      fccc            /pub/client.softwar....l/pop3.0/loadpop.exe
-rw-rw-r--      ftpa            /pub/client.softwar....l/pop3.0/poptips.txt
-rw-rw-r--      ftpa            /pub/client.software/popmail/pop3.0/read.me
-rw-rw-r--      news            /pub/client.softwar....pop3.2.3/loadpop.exe
-rw-rw-r--      ftpa            /pub/client.softwar....pop3.2.3/poptips.txt
-rw-rw-r--      ftpa            /pub/client.software/popmail/pop3.2.3/read.me
-rw-rw-r--      ftpa            /pub/collections.services/catup
-rw-rw-r--      ftpa            /pub/exh.images/1492.exh/Biblio.text
-rw-rw-r--      ftpa            /pub/exh.images/1492.exh/Biblio.wp
-rw-rw-r--      ftpa            /pub/exh.images/1492.exh/FILELIST
-rw-rw-r--      ftpa            /pub/exh.images/1492.exh/Imaglist.text
-rw-rw-r--      fabc            /pub/exh.images/1492.exh/WARNING
-rw-rw-r--      ftpa            /pub/exh.images/1492.exh/exh/Intro.text
-rw-rw-r--      ftpa22          /pub/exh.images/1492.exh/exh/Intro.wp
-rw-rw-r--      ftpa            /pub/exh.images/149....a-America/Americ.gif
-rw-rw-r--      ftpa            /pub/exh.images/1492.exh/exh/a-America/n.gif
-rw-rw-r--      ftpa            /pub/exh.images/1492.exh/exh/b-Med/Meditr.gif
-rw-rw-r--      ftpa            /pub/exh.images/149....h/b-Med/Meditr.text#
-rw-rw-r--      ftpa            /pub/exh.images/1492.exh/exh/b-Med/world.gif
-rw-rw-r--      ftpa            /pub/exh.images/149....-Columbus/Columb.gif
-rw-rw-r--      ftpa            /pub/exh.images/149....Columbus/Columb.text
-rw-rw-r--      ftpa            /pub/exh.images/149....ting.Amer/Invent.gif
-rw-rw-r--      ftpa            /pub/exh.images/149....aims.Amer/Claims.gif
-rw-rw-r--      ftpa            /pub/exh.images/149....ims.Amer/Claims.text
-rw-rw-r--      ftpa            /pub/exh.images/149....Epilogue/Epilog.text
-rw-rw-r--      ftpa            /pub/exh.images/149....f-Epilogue/Epilog.wp
-rw-rw-r--      ftpa            /pub/exh.images/149....-Epilogue/winter.gif
-rw-rw-r--      ftpa            /pub/exh.images/149....ewers/README.viewers
-rw-rw-r--      ftpa            /pub/exh.images/1492.exh/viewers/dvpeg24a.zip
-rw-rw-r--      ftpa            /pub/exh.images/1492.exh/viewers/qextract.exe
-rw-rw-r--      ftpa            /pub/exh.images/1492.exh/viewers/vpic60.zip
-rw-rw-r--      ftpa            /pub/exh.images/dss/Article.txt
-rw-rw-r--      ftpa            /pub/exh.images/dss/Article.wp
-rw-rw-r--      ftpa            /pub/exh.images/dss/Explain.txt
-rw-rw-r--      ftpa            /pub/exh.images/dss/WARNING
-rw-rw-r--      ftpa            /pub/exh.images/dss/exh/Biblio.txt
-rw-rw-r--      ftpa            /pub/exh.images/dss/exh/Biblio.wp
-rw-rw-r--      ftpa            /pub/exh.images/dss....roduction/Deadsea.wp
-rw-rw-r--      ftpa            /pub/exh.images/dss....ntroduction/tabs.gif
-rw-rw-r--      ftpa            /pub/exh.images/dss....roduction/thongs.gif
-rw-rw-r--      ftpa            /pub/exh.images/dss....mmunity/Communit.gif
-rw-rw-r--      ftpa            /pub/exh.images/dss....ommunity/torah-a.gif
```

8.6 GRPEXEC - Files - GROUP executable

L

RISKS

Any member of this file's group can run the files here which are group executable.
The following points should also be noted:
- o With execute rights, a compiled program can be run but shell scripts require read rights.
- o To write to a file a user does not need write access to the directory.
- o A user must have execute permission on the directory to do anything to the files.
- o Many of them are system commands designed to be used by everyone. (e.g. ls)

In order to examine only the more important files, we have ignored files in directories whose path contains the word /bin/ or /sbin/.

ACTIONS

Examine the list of files and ensure that it is intended that members of the group can run them.Remove group execute access from these files unless it is actually needed.

L

RESULTS

```
Attribute       Group           file
-------------------------------------
-r-xr-xr-x      system          /lib/libc.a#
-rw-rwxr-T      ftpa            /pub/exh.images/vat....-nature/nature05.jpg

2 Files found
```

8.7 BADPRIV - Files - Uneven privileges

M

RISKS

These file permissions have:
- o GROUP higher than OWNER or
- o WORLD higher than GROUP or
- o WORLD higher than OWNER.

This makes nonsense of the permissions set on these files.

ACTIONS

The file permissions should be adjusted accordingly.

H

RESULTS

```
Problem       Attribute       File
-----------------------------------
Grp W > Own W ---x-wsrwx /bin/jxjx1
Grp W > Own W ---x-wsrwx /bin/jxjx2
Grp W > Own W ---x-wsrwx /bin/ksh
Grp W > Own W ---x-wsrwx /bin/sh
Wld W > Grp W -rw-r--rw- /etc/filexx
Wld W > Grp W -rw-r--rw- /etc/hosts.equiv
Wld W > Grp W -rw-r--rw- /etc/passwd
Wld W > Grp W -rw-r--rw- /fred/.netrc
Wld W > Grp W -rw-r--rw- /pub/client.software/gopher/dos/gophftp.exe
Grp W > Own W -r--rw-rw- /pub/client.software/gopher/dos/readme.ftp
Wld X > Grp X -rw-rw-r-x /pub/exh.images/vat.exh/exh/g-nature/nature02.jpg
Wld X > Grp X -rw-rw-rwx /pub/exh.images/vat.exh/exh/g-nature/nature03.jpg
Grp X > Own X -rw-rwxr-T /pub/exh.images/vat.exh/exh/g-nature/nature05.jpg

13 Files found
```

8.8 SUID - Files - SUID

RISKS

When applied to an executable file, the person who executes this program will do so under the UID of the OWNER - in many instances this will be ROOT.
It is a standard hacking technique to SUID some common commands
(e.g.) to allow root access with an ordinary account.

ACTIONS

Ask the owner of the files to justify the need for SUID and ensure that you are happy for these files to be SUID.

RESULTS

```
Attribute   File
----------------
-rwsrw-r--  /pub/exh.images/vat.exh/exh/g-nature/Nature.txt

1 file found
```

8.9 SGID - Files - SGID

RISKS

If an executable file has the SGID bit set then when someone executes the file, his group will temporarily change to that of the file's group.
In some instances this will cause problems if the group has special privileges.

ACTIONS

Ask the owner of the files to justify the need for SGID and ensure that you are happy for these files to be SGID.

L

RESULTS

```
Attribute   File
----------------
-rw-rwsr--  /pub/exh.images/vat.exh/exh/g-nature/nature01.jpg

1 file found
```

8.10 STICKY - Files - Sticky

L

RISKS

If the sticky bit is set on a program file it will not be removed from memory after it has finished executing. This makes it useful if the program is run often. Improved memory management has made this unnecessary but very useful when applied to directories.

ACTIONS

None.

L

RESULTS

```
Attribute   File
----------------
-rw-rwxr-T  /pub/exh.images/vat.exh/exh/g-nature/nature05.jpg

1 file found
```

8.11 SUID+WW - Files - SUID/SGID and WORLD executable/writeable

M

RISKS

This test has been included to assist you in finding the most high risk files i.e. those which are SUID or SGID and are world WRITEABLE/EXECUTABLE.
Anyone with access to these files will be able to execute (programs) under the UID of the owner.

ACTIONS

Ask the owner of the files to justify the need for these high privileges.

M

RESULTS

```
Attribute   File
----------------
---x-wsrwx  /bin/jxjx1
---x-wsrwx  /bin/jxjx2
---x-wsrwx  /bin/ksh
---x-wsrwx  /bin/sh

4 Files found
```

8.12 HOSTINFO - Files likely to contain host information

M

RISKS

These files are likely to contain information about other computers and users which can connect to the system being reviewed.
If someone breaks into just one of these systems it is possible for them to gain access to all the others in which there is a host.equiv file. Similarly, the .rhosts file will show external systems and users who can login to a local account without a password.
DO NOT TRUST ANY SYSTEM WHICH YOU DO NOT CONTROL ACCESS TO.
Note: Some of the files listed below may be executable programs rather than data files and will therefore be likely to be needed by the system.

ACTIONS

Try to avoid using these files unless absolutely necessary.Obtain a printout of each of these files or use the CAT command. Then:o Examine the names of the other systems which can connect to this computer and ensure that they are permitted and actually needed.o Examine any .rhosts files and check that the users contained in them are authorised to access this systemEnsure that the files are not writeable.

M

RESULTS

```
Attribute   File
----------------
-rw-r--rw-  /etc/hosts.equiv
-rw-rw-rw-  /fred/.rhost
-rw-r--rw-  /fred/.netrc
-rw-rw-r--  /pub/.rhostsx25

4 Files found
```

8.13 SUWW - Startup files which are world writeable

H

RISKS

The following files are likely to be the start-up files of users. Where they are script files, they will be run soon after the user has logged in.
Anyone who can write to these files can insert malicious commands which will then be executed by the legitimate user.

ACTIONS

Ensure that these files are owned by the system administrator (NOT the user).Ensure they are not writeable by other people.

M

RESULTS

```
Attribute   File
----------------
-rw-rw-rw-  /bin/profile
-rw-rw-rw-  /fred/profile
-rw-rw-rw-  /fred/profileLonger
-rw-rw-rw-  /fred/profileLong

4 Files found
```

9 DIRS - Directories

RISKS

Directories are used to group files together. When they are created, they will have an owner and a group.
A number of privileges determine whether they can be written to or read and by whom.

9.1 UNKOWN - Dir - Unknown owners

M

RISKS

The following users own directories but they are not present in the PASSWORD file i.e. the owner no longer exists.

ACTIONS

Examine these directories and either remove them and their files or assign them new owners.

M

RESULTS

```
Owner           Directory
-----------------------
238              /pub/copyright/
lbro1            /pub/exh.images/vat.exh/exh/g-nature/
fred             /pub/exh.images/vat.exh/exh/h-orient_to_rome/

3 directories found
```

9.2 UNKGRP - Dir - Unknown groups

L

RISKS

The following groups own directories but do not have records in the GROUP file i.e. the group no longer exists.

ACTIONS

Examine these directories and either remove them and their files or assign them new group ownership.

H

RESULTS

```
Group            Directory
-------------------------
system           /
system           /bin/
system           /etc/
system           /fred/
system           /lib/
system           /u/
system           /usr/
fccc             /pub/client.software/usenet/windows/
groupX           /pub/exh.images/vat.exh/exh/g-nature/
groupZ           /pub/exh.images/vat.exh/exh/h-orient_to_rome/
system           /u/larr/
system           /u/tkea/
system           /u/www/
system           /u/wwwa/
system           /usr/binx/

15 directories found
```

9.3 WRLDWRT - Dir - WORLD writeable

Ⓜ

RISKS

A user must also have 'execute' rights in order to cd to that directory or any directory underneath it. A user must also have 'read' rights to list files but can run programs if they know the file name.
Sub-directories, in directories which are sticky, have NOT been shown since it is assumed that these can only be renamed or removed by the owner of the file, the owner of the directory or the super user.
Anyone can delete these directories and any files or subdirectories in them.

ACTIONS

Remove world write from these directories unless it is actually needed. Use chmod a-w <directory>

Ⓗ

RESULTS

```
Attribute  Directory
-------------------
dr-xr-srwt /bin/
drw-rw-rwx /u/
drw-rw-rwx /usr/
drwsrwsrwt /u/larr/
drwsrwsrwt /u/tkea/
dr--rw-rwt /u/www/
dr--rw-rwt /u/wwwa/
drw-rw-rwx /usr/binx/

8 directories found
```

9.4 WRLDEXE - Dir - WORLD executable

M

RISKS

Directories which are 'executable' can be accessed by everyone. If users also have write permission on the directory they can delete files from here.
If users do NOT have read access they can only delete files which they know to exist; they cannot list the directory.
Directories which need to be protected should not have this permission.
Unauthorised access to data.

ACTIONS

Ensure that most directories do not have this permission. Where they do, ensure that this access is actually intended.

L

RESULTS

```
Attribute  Directory
--------------------
drw-rw-rwx /usr/binx/

1 directory found
```

9.5 GRPWRT - Dir - GROUP writeable

M

RISKS

Any member of the group can delete these directories and any files or subdirectories in them.
A user must also have 'execute' rights in order to cd to that directory or any directory underneath it. A user must also have 'read' rights to list files but can run programs if they know the file name.
Sub-directories, in directories which are sticky, have NOT been shown since it is assumed that these can only be renamed or removed by the owner of the file, the owner of the directory or the super user.
Unauthorised access to data.

ACTIONS

Remove group write access from these directories unless it is actually needed.

H

RESULTS

```
Attribute  Directory
---------------------
drwxrwsr-x /pub/
drw-rw-rwx /u/
drw-rw-rwx /usr/
drwxrwxr-x /pub/client.software/
drwxrwsr-x /pub/collections.services/
drwxrwsr-x /pub/copyright/
drwxrwsr-x /pub/ww/
drwxrwsr-x /pub/ww1/
drwxrwsr-x /pub/ww2/
drwxrwxr-x /pub/client.software/gopher/
drwxrwsr-x /pub/client.software/popmail/
drwxrwsr-x /pub/client.software/gopher/dos/
drwxrwsr-x /pub/client.software/gopher/os2/
drwxrwsr-x /pub/client.software/gopher/seq1/
drwxrwsr-x /pub/client.software/gopher/windows/
drwxrwsr-x /pub/client.software/popmail/pop3.0/
drwxrwsr-x /pub/client.software/popmail/pop3.2.3/
drwxrwsr-x /pub/exh.images/
drwxrwsr-x /pub/exh.images/russian.archive.exh#/
drwxrwsr-x /pub/exh.images/vat.exh/
drwxrwsr-x /pub/exh.images/1492.exh/
drwxrwsr-x /pub/exh.images/1492.exh/exh/
drwxrwsr-x /pub/exh.images/1492.exh/viewers#/
drwxrwsr-x /pub/exh.images/1492.exh/exh/a-America/
drwxrwsr-x /pub/exh.images/1492.exh/exh/b-Mediterranean/
drwxrwsr-x /pub/exh.images/1492.exh/exh/c-Columbus/
drwxrwsr-x /pub/exh.images/1492.exh/exh/d-Inventing.Amer/
drwxrwsr-x /pub/exh.images/1492.exh/exh/e-Eur.claims.Amer/
drwxrwsr-x /pub/exh.images/1492.exh/exh/f-Epilogue/
drwxrwsr-x /pub/exh.images/1492.exh/exh/b-Med/
drwxrwsr-x /pub/exh.images/dss/
drwxrwsr-x /pub/exh.images/dss/.exh/
drwxrwsr-x /pub/exh.images/dss/viewers#/
drwxrwsr-x /pub/exh.images/dss/exh/
drwxrwsr-x /pub/exh.images/dss/exh/a-introduction/
drwxrwsr-x /pub/exh.images/dss/exh/b-community/
drwxrwsr-x /pub/exh.images/dss/exh/c-library#/
drwxrwsr-x /pub/exh.images/dss/exh/d-today/
drwxrwsr-x /pub/exh.images/dss/exh/a-introduction/Deadsea.txt/
drwxrwsr-x /pub/exh.images/dss/exh/c-library/
drwxrwsr-x /pub/exh.images/dss/viewers/
drwxrwsr-x /pub/exh.images/russian.archive.exh/
drwxrwsr-x /pub/exh.images/russian.archive.exh/README/
drwxrwsr-x /pub/exh.images/russian.archive.exh/images_gif/
drwxrwsr-x /pub/exh.images/russian.archive.exh/text.english/
drwxrwsr-x /pub/exh.images/vat.exh/.exh/
drwxrwsr-x /pub/exh.images/vat.exh/viewers/
drwxrwsr-x /pub/exh.images/vat.exh/exh/
drwxrwsr-t /pub/exh.images/vat.exh/exh/a-vat_library#/
drwxrwsr-x /pub/exh.images/vat.exh/exh/b-archeology/
drwxrwsr-x /pub/exh.images/vat.exh/exh/c-humanism/
drwxrwsr-x /pub/exh.images/vat.exh/exh/d-mathematics/
drwxrwsr-x /pub/exh.images/vat.exh/exh/e-music/
drwxrwsr-x /pub/exh.images/vat.exh/exh/f-medicine_bio/
drwxrwsr-x /pub/exh.images/vat.exh/exh/g-nature/
drwxrwsr-x /pub/exh.images/vat.exh/exh/h-orient_to_rome/
drwxrwsr-x /pub/exh.images/vat.exh/exh/i-rome_to_china/
drwxrwsr-t /pub/exh.images/vat.exh/exh/a-vat_library/
drwxrwsr-x /pub/exh.images/vat.exh/exh/i-rome_to_china:#/
drwsrwsrwt /u/larr/
drwsrwsrwt /u/tkea/
dr--rw-rwt /u/www/
dr--rw-rwt /u/wwwa/
drw-rw-rwx /usr/binx/

64 directories found
```

9.6 GRPEXE - Dir - GROUP executable

M

RISKS

Directories which are 'executable' can be accessed by members of the group.
If everyone in the group also has write permission on the directory they can delete files from here. If everyone does NOT have read access they can only delete files which they know to exist; they cannot list the directory.
Directories which need to be protected should not have this permission.
Unauthorised modification and deletion of data.

ACTIONS

Ensure that most directories do not have this permission.Where they do, ensure that this access is actually intended.

M

RESULTS

```
Attribute  Directory
--------------------
drwxrwxr-x /pub/client.software/
drwxrwxr-x /pub/client.software/gopher/

2 directories found
```

9.7 BADPRIV - Dir - Uneven privileges

M

RISKS

Permissions must logically be in the correct order i.e.
Group permissions should be lower than OWNER permissions and
WORLD permissions should be lower than GROUP permissions.
These directory permissions have:
GROUP higher than OWNER or
WORLD higher than GROUP or
WORLD higher than OWNER.
This makes nonsense of the permissions set on these directories.

ACTIONS

These directory permissions should be adjusted accordingly.

H

RESULTS

```
Problem               Attribute       Directory
-----------------------------------------------
Wld W > Grp W         dr-xr-srwt /bin/
Wld X > Grp X         drw-rw-rwx /u/
Grp W > Own W         dr--rw-rwt /u/www/
Grp W > Own W         dr--rw-rwt /u/wwwa/
Wld X > Grp X         drw-rw-rwx /usr/
Wld X > Grp X         drw-rw-rwx /usr/binx/

6 directories found
```

9.8 SGID - Dir - SGID

L

RISKS

On some versions of Unix, the SGID bit on a directory determines the way the system handles groups, either:
With the SGID bit set, files created inside the directory have the same group as the directory.
With the SGID bit NOT set, files in these directories have the same group as the primary group of the user.
or
With the SGID bit set or NOT set, files created in these directories have the same group as the primary group of the user.

ACTIONS

None.

H

RESULTS

```
Attribute   Directory
----------------------
dr-xr-sr-x /
dr-xr-srwt /bin/
dr-xr-sr-x /etc/
dr-xr-sr-x /fred/
dr-xr-sr-x /lib/
drwxrwsr-x /pub/
drwxrwsr-x /pub/collections.services/
drwxrwsr-x /pub/copyright/
drwxrwsr-x /pub/ww/
drwxrwsr-x /pub/ww1/
drwxrwsr-x /pub/ww2/
drwxrwsr-x /pub/client.software/popmail/
drwxr-sr-x /pub/client.software/usenet/
drwxr-sr-x /pub/client.software/wais#/
drwxr-sr-x /pub/client.software/www/
drwxrwsr-x /pub/client.software/gopher/dos/
drwxrwsr-x /pub/client.software/gopher/os2/
drwxrwsr-x /pub/client.software/gopher/seq1/
drwxrwsr-x /pub/client.software/gopher/windows/
drwxrwsr-x /pub/client.software/popmail/pop3.0/
drwxrwsr-x /pub/client.software/popmail/pop3.2.3/
drwxr-sr-x /pub/client.software/usenet/dos/
drwxr-sr-x /pub/client.software/usenet/windows/
drwxr-sr-x /pub/client.software/wais/
drwxr-sr-x /pub/client.software/wais/windows/
drwxr-sr-x /pub/client.software/www/windows/
drwxrwsr-x /pub/exh.images/
drwxrwsr-x /pub/exh.images/russian.archive.exh#/
drwxrwsr-x /pub/exh.images/vat.exh/
drwxrwsr-x /pub/exh.images/1492.exh/
drwxrwsr-x /pub/exh.images/1492.exh/exh/
drwxrwsr-x /pub/exh.images/1492.exh/viewers#/
drwxrwsr-x /pub/exh.images/1492.exh/exh/a-America/
drwxrwsr-x /pub/exh.images/1492.exh/exh/b-Mediterranean/
drwxrwsr-x /pub/exh.images/1492.exh/exh/c-Columbus/
drwxrwsr-x /pub/exh.images/1492.exh/exh/d-Inventing.Amer/
drwxrwsr-x /pub/exh.images/1492.exh/exh/e-Eur.claims.Amer/
drwxrwsr-x /pub/exh.images/1492.exh/exh/f-Epilogue/
drwxrwsr-x /pub/exh.images/1492.exh/exh/b-Med/
drwxr-sr-x /pub/exh.images/1492.exh/viewers/
drwxr-sr-x /pub/exh.images/african.american.exh/
drwxrwsr-x /pub/exh.images/dss/
drwxrwsr-x /pub/exh.images/dss/.exh/
drwxrwsr-x /pub/exh.images/dss/viewers#/
drwxrwsr-x /pub/exh.images/dss/exh/
drwxrwsr-x /pub/exh.images/dss/exh/a-introduction/
drwxrwsr-x /pub/exh.images/dss/exh/b-community/
drwxrwsr-x /pub/exh.images/dss/exh/c-library#/
drwxrwsr-x /pub/exh.images/dss/exh/d-today/
drwxrwsr-x /pub/exh.images/dss/exh/a-introduction/Deadsea.txt/
drwxrwsr-x /pub/exh.images/dss/exh/c-library/
drwxrwsr-x /pub/exh.images/dss/viewers/
drwxrwsr-x /pub/exh.images/russian.archive.exh/
drwxrwsr-x /pub/exh.images/russian.archive.exh/README/
drwxrwsr-x /pub/exh.images/russian.archive.exh/images_gif/
drwxrwsr-x /pub/exh.images/russian.archive.exh/text.english/
drwxrwsr-x /pub/exh.images/vat.exh/.exh/
drwxrwsr-x /pub/exh.images/vat.exh/viewers/
drwxrwsr-x /pub/exh.images/vat.exh/exh/
drwxrwsr-t /pub/exh.images/vat.exh/exh/a-vat_library#/
drwxrwsr-x /pub/exh.images/vat.exh/exh/b-archeology/
drwxrwsr-x /pub/exh.images/vat.exh/exh/c-humanism/
drwxrwsr-x /pub/exh.images/vat.exh/exh/d-mathematics/
drwxrwsr-x /pub/exh.images/vat.exh/exh/e-music/
drwxrwsr-x /pub/exh.images/vat.exh/exh/f-medicine_bio/
drwxrwsr-x /pub/exh.images/vat.exh/exh/g-nature/
```

9.9 NSTICKY - Dir - Not Sticky

L

RISKS

These directories do not have the sticky bit set. In many versions of Unix only the file owner, the directory owner and the super user can rename or remove files in these directories.
Unauthorised modification of data.

ACTIONS

This is a useful feature which should be employed whenever possible.

H

RESULTS

```
Attribute  Directory
--------------------
dr-xr-srwt /bin/
drwxrwsr-t /pub/exh.images/vat.exh/exh/a-vat_library#/
drwxrwsr-t /pub/exh.images/vat.exh/exh/a-vat_library/
drwsrwsrwt /u/larr/
drwsrwsrwt /u/tkea/
dr--rw-rwt /u/www/
dr--rw-rwt /u/wwwa/

7 directories found
```

10 FTP - FTP

RISKS

The File Transfer Protocol (FTP) is a standard means of moving files from one system to another

10.1 FTPOWNBIN - Anonymous FTP bin directory has wrong owner

L

RISKS

Anonymous FTP allows people on the network who do not have an account on the computer, to deposit files in or retrieve files from the anonymous FTP account's pub directory.
The anonymous FTP account's bin and etc directories contain files and commands needed to support anonymous FTP.

ACTIONS

The owner of these directories should be the root account.

L

RESULTS

```
The /ftp/bin/ directory was not found in file directory listing.
```

10.2 FTPOWNETC - Anonymous FTP etc directory has wrong owner

M

RISKS

Anonymous FTP allows people on the network who do not have an account on the system to deposit files in or retrieve files from the anonymous FTP account's pub directory.

ACTIONS

The anonymous FTP account's bin and etc directories contain files and commands needed to support anonymous FTP. The owner of these directories should be the root account.

L

RESULTS

```
The /ftp/etc/ directory was not found in file directory listing.
```

10.3 FTPHDIROWN - Anonymous FTP home directory has wrong owner

M

RISKS

Anonymous FTP allows people on the network who do not have an account on the system to deposit files in or retrieve files from the anonymous FTP account's pub directory.
The anonymous FTP account's home directory should be owned by the root account to prevent users being able to write to or
modify its content.

ACTIONS

Change the ownership of the anonymous FTP account's home directory to root using the command 'chown root 'DIRECTORY-NAME".

L

RESULTS

```
The user 'ftp'was found in the password file.
The user's home directory is /anonftp/
The /anonftp/ directory was not found in file directory listing.
```

11 /ETC - /etc

RISKS

The /etc directory is one of the most important directories on a Unix system since it contains many of the computer's security files such as the password file.

11.1 ETCWW - Directories under /etc has world write access

M

RISKS

The directory /etc and its sub-directories normally contain files that are executed by the root account during system start-up and are critical for the running of the system.

ACTIONS

Permitting world write access to a directory allows all users on the system to modify the files it contains.

L

RESULTS

```
Directories under the /etc directory are not world writable.
```

11.2 ETCPWD - File /etc/default/passwd has insecure permissions

M

RISKS

If the file /etc/default/passwd exists, can it be only written too by its owner.

ACTIONS

Check the ownership and permissions of this file and its parent directories (i.e. /etc /etc/default).If necessary, use the chmod command to change permissions such that only root can write to the file.

H

RESULTS

```
The files /etc/passwd  and /etc/default/passwd were examined.

/etc/passwd  -rw-r--rw-  world writable.

/etc/default/passwd   not found.
```

11.3 ETCPROF - File /etc/profile has insecure permissions

M

RISKS

/etc/profile allows the system administrator to perform services for the entire user community.
Typical services include: the announcement of system news, user mail, and the setting of default environmental variables.
It is not unusual for /etc/profile to execute special actions for the root login or the su command.

ACTIONS

Ensure that the file /etc/profile can only be written to by root.

L

RESULTS

```
The Profile file not found.
```

12 LOG FILES - Log files

RISKS

Log files are used to record key events on the system such as the use of SU and failed logins etc
It is important to ensure that they cannot be amended by users.

12.1 LOGLOGEX - The login log file does not exist

M

RISKS

If the login log file does not exist then failed attempts to log in, such as those caused by a hacker repeatedly attempting to guess passwords, will not be logged.

ACTIONS

Create the login log file, ensuring it is owned by username root and group sys, and that it has read and write permissions granted solely to its owner.The login log file should exist and should be regularly monitored for such behaviour.Also, this file should not be a symbolic link, especially if the file linked to is not on the same partition as the link, as this could lead to login events being written to the wrong file or worse still discarded.Also, ensure that the file is not a symbolic link.

M

RESULTS

```
Login files found:

A login log file was not found on this system.

0 Files found
```

12.2 LOGLOGOWN - Login log not correctly owned

M

RISKS

If the login log file exists, is it owned by username root and group root or sys.

ACTIONS

Ensure that the login log file is owned by username root and group root or sys, and that only the owner has read and write permissions.

M

RESULTS

```
Login files found:

A login log file was not found on this system.

0 Files found
```

14 AIX - AIX

RISKS

AIX is a proprietary operating system from IBM. The structure of the password file is different to most other Unix versions and it has thus got its own section.

15 NIS - NIS

RISKS

NIS is a distributed system which enables other computers to share password files, group files and many other files over a network.

15.1 NISUSED - Is NIS being used.

RISKS

This section reports on whether NIS is being used for the control of user-IDs.
We have found a + sign in the password or group file which indicates that NIS is being used.
When obtaining user or group information, the Unix system will first look in the password file and if the user-ID is not present it will refer to the master password file on the NIS server.

ACTIONS

As part of your review, it is important that you examine this master system.Ensure that the line in the password file is +: and not +::0:0:::In the second instance, if the + were accidentally replaced with just a single character such a 'p' then typing in this character at login time would allow a user to connect without a password and be connected as a super-user.

RESULTS

NIS is not being used on this system.