AZScan Documentation

Introduction

Summary

AZScan runs on a standalone PC and reviews the security of Unix, OS400 and VMS operating systems and Oracle databases. Key files are copied from the mid-range system to the PC and AZScan reviews them and writes reports in various formats which show the current weaknesses in the system.

What is AZScan?

AZScan is a vulnerability assessment tool for mid-range computer systems. It runs on a standalone PC and reviews key files copied from the computer being reviewed, to produce a range of reports which show the system's problems. Reports are produced on screen as well as in HTML, plain text and MSWord format. The reports show the Risks and Implications of the problem, followed by the results found on your system and makes recommendations on how to fix the problem.

Philosophy and Objectives

AZScan is designed with the following objectives:

- The software runs on a low-spec standalone PC and even a basic laptop.
- The product will be portable for users who travel.
- Interaction with the system being reviewed will be minimal.
- The software cannot damage or impair the system being reviewed.
- The results must be comprehensive but understandable by all levels of users including business managers.
- The results should not only identify issues but also identify recommended solutions.
- The results should be in the format Risk – Results – Recommendations.
- A scoring system will provide a numerical means of seeing system improvements.

How does it work?

Most mid-range systems contain user profiles and system settings, in certain important system files. By examining these files, AZScan can identify problems and weaknesses which represent security risks to the system. Highlighting risks in these systems impacts the System Manager, Security Administration and the Auditors (both Internal and external). Each group may have different functions but their common aim is to improve security. AZScan does this for you.

AZScan works by reviewing copies of these key files, analysing and cross referencing the data to produce reports which can be used by you to report on and improve, system security.

Copying the files from the mid-range system to a PC, instead of loading software onto the system, means that the review can be performed without stopping the system. AZScan also cannot damage your business critical system or even impair its performance.

Installation

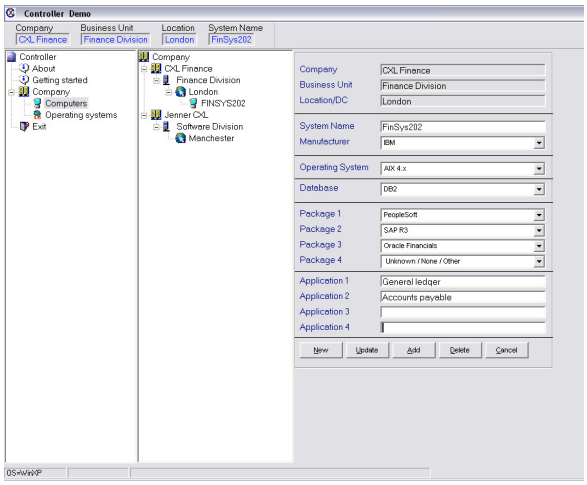
Installation of AZScan simply requires copying the demonstration file from our website at www.cxlsecure.com. The file is a self-installing executable. Simply follow the instructions and the software will install itself, usually in the 'c:\program files\cxl\azscan\' directory. The main executable can be accessed from desktop icon.

Controller

Introduction

This program is the starting point for AZScan. It allows you to provide details for your reviews such as which company, location and computer systems you are reviewing.

The controller program lets you select the name of the company, systems and software running on the computer system being reviewed. The next stage is to select the type of review you want to do – OS/400, Unix, OpenVMS or Oracle.



You can enter details of the company location and the various systems being reviewed including the operating systems, databases and applications.

This acts as a reminder for future reviews and some of the data is used in the cover pages of the reports.

It is not essential that you use the controller program. Expert users tend to go straight to the review type they wish to use such as Unix etc.

OS/400 Reviews

Introduction

AZScan is designed to review IBM **AS/400** systems running the **OS/400** operating system. Following name changes by IBM, these are now known as **eServer** systems running the **iSeries** operating system.

These systems can be very secure but have great flexibility in terms of security settings. The settings will determine just how secure your system is. There are many system wide security settings which, in some instances, can over-ride the settings of individual users making a manual review of security, a very difficult task.

Obtaining the OS/400 files

To enable AZScan to review OS/400, you have to give it two files from the iSeries system being reviewed. These files are produced using two very simple commands which generate the required input files. These two files are then copied to the PC running AZScan by disk, ftp or any other available means.

The first command generates the 'System Profile File':-

WRKSYSVAL SYSVAL(*ALL) OUTPUT(*OUTFILE) OUTFILE(QTEMP/SYSTEMLIST1)

If you examine the system profile file produced, it will look something like this:

```
System Values Page 1        5722SS1  V5R1M0 010525 CXLAS1 04-03-27 01:52:28

Name          Current       Shipped       Description
              Value         Value
QABNORMSW     0             0             Previous end of system indicator
QACGLVL >     *JOB          *NONE         Accounting level
QACTJOB >     200           20            Initial number of active jobs
QADLACTJ >    50            10            Additional number of active jobs
QADLSPLA      2048          2048          Spooling control block additional
Etc…
```

The second command generates the 'User Profile File'.

DSPUSRPRF USRPRF(*All) OUTPUT(*OUTFILE) OUTFILE(QTEMP/USERLIST2)

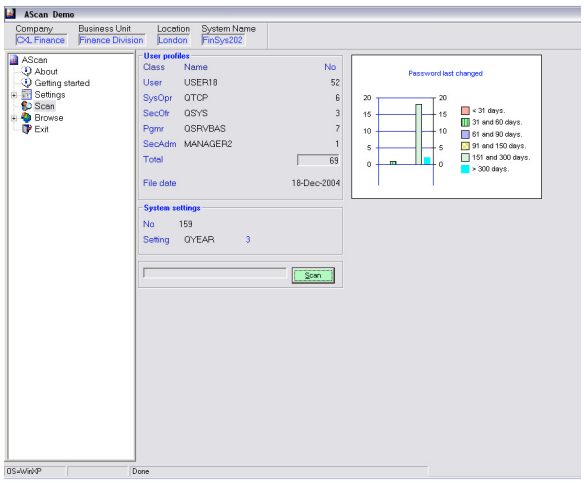
Examining the User Profile File will show a listing which looks like this:

```
1041029021706CXLSASP DAVID    *USER   *SYSVAL 1040413073938 *NO *YES *NO      *NONE
1041029021706CXLSASP MANAGER1 *PGMR   *SYSVAL 1040513073938 *NO *YES *YES     *NONE
1041029021706CXLSASP MANAGER2 *SECADM *SYSVAL 1040313073938 *NO *NO
1041029021706CXLSASP MANAGER3 *PGMR   *SYSVAL 1040413073938 *NO *YES *NO      *NONE
1041029021706CXLSASP MANAGER4 *SECOFR *SYSVAL 1040318134548 *NO *NO
1041029021706CXLSASP MANAGER5 *SYSOPR *SYSVAL 1020413012415 *NO *NO
1041029021706CXLSASP MANAGER6 *USER   *SYSVAL 1040313073938 *NO *YES *SYSVAL *NONE
1041029021706CXLSASP QBRMS    *USER   *SYSVAL 1040413073938 *NO *YES *SYSVAL *NONE
1041029021706CXLSASP QCLUMGT  *USER   *SYSVAL 1040313012415 *NO *YES *YES     *IOSYSCFG
1041029021706CXLSASP QCLUSTER *USER   *SYSVAL 1040813012415 *NO *YES *YES     *IOSYSCFG
```

It is important that the files are transferred to the PC using simple FTP and you do not use IBM commands such as CRYTOIMPF or use Client Access data transfer with tab delimited set. (These will reformat the output files).

OS/400 Scanning

AZScan will review the files very quickly and progress can be watched on screen. Producing the reports is also fast too although if you have selected MS Word format, the production of this report can be slow due to the way Word works.



Tip

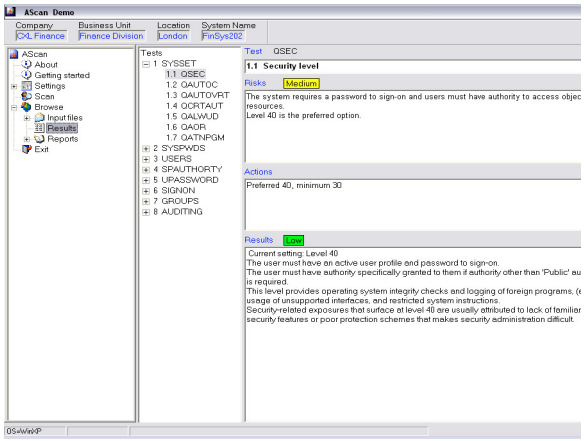
It is suggested that you only produce the Word format report after the text and HTML versions have been produced and checked.

Tip

The Word format report is great for importing straight into your written report on the system.

Results

Results can either be reviewed on screen or in printed format. The RESULTS screen is shown here.



The tests have been grouped together into sections and you navigate through each one using the middle treeview.

Reports can either be viewed on screen or printed out but be warned, some reports can be very large.

Tip

If you have produced a Word report, use the Heat Map to identify problem areas and then pull the Word format report into MSWord and just print the sections you think are important.

Reports are produced in various formats:

- Plain text formatted with page breaks.
- MS Word format
- HTML

In addition, reports are either Full, Summary or Heatmaps.

It should be noted that the Word format version should not be read using MS Wordpad. Please use MS Word as Wordpad has a number of problems which change the formatting of reports.

OS/400 Systems

AZScan will review 15 versions of OS/400

1	OS\400	v5r3	9	OS\400	v3r7
2	OS\400	v5r2	10	OS\400	v3r6
3	OS\400	v5r1	11	OS\400	v3r5
4	OS\400	v4r5	12	OS\400	v3r4
5	OS\400	v4r4	13	OS\400	v3r3
6	OS\400	v4r3	14	OS\400	v3r2
7	OS\400	v4r2	15	OS\400	v3r1
8	OS\400	v4r1			

OS/400 Tests

Shown below is a table of tests which AZScan performs based on the system settings and the user profiles.

No	Code	Description	**Risk**
1	SYSSET	System settings	
1 1.1	QSEC	Security level	**Medium**
2 1.2	QAUTOC	Auto configuration	**Low**
3 1.3	QAUTOVRT	Auto virtual	**Low**
4 1.4	QCRTAUT	Default public authority	**Medium**
5 1.5	QALWUD	Allow user domain	**Low**
6 1.6	QAOR	Allow object restore	**Low**
7 1.7	QATNPGM	Attention program	**Medium**
2	SYSPWDS	System passwords	
8 2.1	QPWDLVL	Password level	**Low**
9 2.2	QPWDEXPITV	Password expiration interval	**High**
10 2.3	QPWDLMTAJC	Password limit adjacent digits	**Low**
11 2.4	QPWDLMTCHR	Password limit characters	**Low**
12 2.5	QPWDLMTREP	Password limit repetition	**Low**
13 2.6	QPWDMINLEN	Password minimum length	**High**
14 2.7	QPWDMAXLEN	Password maximum length	**Low**
15 2.8	QPWDPOSDIF	Password position different	**Low**
16 2.9	QPWDRQDDGT	Password does not require digits	**Medium**
17 2.10	QPWDRQDDIF	Password required to be different	**High**
18 2.11	QPWDVLDPGM	Password validation program	**Low**
3	USERS	Users	
19 3.1	UCLASS	User Classes	**High**
20 3.2	DISPROF	Users with disabled profiles	**Low**
21 3.3	CURLIB	Users current library	**Low**
22 3.4	INLPGM	Users initial programs	**Low**
23 3.5	INLMNU	Users initial menu	**Low**
24 3.6	DSPSGNINF	Users display sign-on information	**Medium**
25 3.7	LMTCPB	Users limit capability	**Low**
26 3.8	QLMTDEVSSN	Users with limited device sessions	**Low**
27 3.9	SPCENV	Users with special environments	**Low**
4	SPAUTHORTY	Special Authorities	
28 4.1	ALLOBJ	Users with all objects authority	**High**
29 4.2	SECADM	Users with security administration authority	**High**
30 4.3	JOBCTL	Users with job control authority	**Medium**
31 4.4	SPLCTL	Users with spool control Authority	**Medium**

32 4.5	SAVSYS	Users with save system authority	**Medium**
33 4.6	SERVICE	Users with service authority	**Medium**
34 4.7	AUDIT	Users with audit authority	**Low**
35 4.8	IOSYSCFG	Users with system configuration authority	**Low**
5	UPASSWORD	User passwords	
36 5.1	PWDEXPITV	Users password expiry interval	**Medium**
37 5.2	PWDEXPD	Users with password set to expired	**Medium**
38 5.3	PWDLCHG	Users password last changed	**Medium**
39 5.4	PWDIBMPRO	IBM system profiles where password <> *NONE	**Low**
6	SIGNON	Signon attempts allowed	
40 6.1	QMAXSIGN	Maximum sign-on attempts	**Medium**
41 6.2	QMAXSGNACN	Maximum sign-On attempt action	**Low**
42 6.3	QRMTSIGN	Remote sign-on	**Medium**
43 6.4	QLMTESCOFR	Limit security officer	**Low**
44 6.5	QDSPSGNINF	Display sign-on information	**Medium**
45 6.6	QLMTDEVSSN	Limit device sessions	**Low**
46 6.7	QINACTITV	Inactive Interval	**Medium**
47 6.8	QINACTMSGQ	Inactive Message Queue	**Low**
7	GROUPS	Groups	
48 7.1	GROUPS	Users in each group	**Low**
8	AUDITING	Auditing	
49 8.1	QAUDCTL	Audit control	**Low**
50 8.2	QAUDLVL	Audit level	**Medium**
51 8.3	QAEA	Audit end action	**Low**
52 8.4	QAFREQ	Audit frequency level	**Low**
53 8.5	QCRTOBJAUD	Create object audit	**Low**

Unix Reviews

Introduction

AZScan is designed to review a wide variety of Unix systems. Almost every software and hardware vendor has a version of Unix and despite the standard name, many of them vary considerably.

Unix has been a notoriously insecure operating system which seems to have been designed with a 'trust everyone' approach to security. In recent years, many manufacturers have bolted on additional security systems which have further extended the differences between Unix versions.

Obtaining the input files

To enable AZScan to work, you have to give it copies of 4 files from the Unix system being reviewed. Three files are simply copied to your PC and fed into the software for review and a fourth file is a created directory listing.

Simply copy the password, shadow and group files to the PC running AZScan.

1. The password file

This file is normally called /etc/passwd and looks something like this:

```
root:x:0:1:Superuser:/:
daemon:x:1:1:System daemons:/etc:
bin:x:2:2:Owner of system commands:/bin:
sys:x:3:3:Owner of system files:/usr/sys:
uucp:x:5:5:UUCP administrator:/usr/lib/uucp:
```

2. The shadow file

This file is normally called /etc/shadow and looks like this:

```
acdrm:WxWe0sfymi/J8:9694::
lch:0.vsmJYWoUCx.:9682::
accwa:DFfv7O3HPguLi:9700::
aod:GwY6jJSZzhQH.:9688::
sad:doeG9VoauA2Pw:9701::
```

On some operating systems, the location of the shadow file can change. Below are some alternative locations and names.

BSD4.3-Reno	/etc/master.passwd
ConvexOS 10	/etc/shadpw *
HP-UX	/.secure/etc/passwd *
OSF/1	/etc/passwd[.dir|.pag] *
SunOS 4.1+c2	/etc/security/passwd.adjunct ##username
Ultrix 4	/etc/auth[.dir|.pag] *
UNICOS	/etc/udb *

Some versions of Unix have very different shadow files, often stored in databases. These are discussed lower down in the section called 'Exceptions'.

3. The group file

This file is normally called /etc/group and looks like this:-

```
bin::2:bin,daemon
adm::4:adm,daemon,listen
asg::8:asg
network::10:network
```

4. The directory file

This file does not normally exist on the system and is the one file that has to be created using the ls command. (On a PC this is the dir command.)

First go to the root directory using the command: cd . (Note the '.')

This is the very top level directory. (On a PC it would be CD C:\)

Next issue the ls command with extra parameters: ls -laRF > mydirfile.txt

This command produces a complete directory listing of the system with dates, file sizes and permissions. Note the upper and lower cases of the laRF parameters. A sample of this output is shown here:

```
drwxr-xr-x  18  root   bin      640  Jul 29 11:31  ./
drwxr-xr-x  18  root   bin      640  Jul 29 11:31  ../
-rw-------   1  root   other      3  Aug 09 1994   .defprint
-rw-------   1  root   other     59  Sep 20 1994   .desked_pref
-r--------   1  root   auth       0  Jul 23 15:54  .lastlogin
-rw-------   1  root   root      15  Dec 14 1991   .mailrc
-rwxrwxrwx   1  root   root     751  Dec 14 1991   .profile*
-rw-r--r--   1  root   root     833  Mar 21 1994   .utillist2
drwxr-xr-x   2  bin    bin     2032  Jan 12 1994   bin/
-r--------   1  bin    bin    77981  Jun 05 1992   boot
drwx------   2  root   other     32  Jan 07 1970   clipdir/
-rw-------   1  root   other   1641  Jan 14 1994   date
```

The output of this command is fed into a newly created file called mydirfile.txt (or any name you choose). The resultant file is copied to the PC for AZScan to review and is referred to as the 'directory file'.

Exceptions

Although Unix has been hailed as an 'Open System' meaning 'not proprietary' and 'not hardware specific', there are many variations and complexities which have been added, as different hardware and software vendors struggle to make Unix more secure.

One 'standard' has been the introduction of the Trusted Computer Base (TCB) which holds the shadow password file in a database. AZScan can handle this and details of obtaining a useable shadow password file are shown later.

Two manufacturers who have very different versions of Unix are Compaq and IBM. With IBM's AIX systems, the security parameters are much more extensive than on most Unix systems and this makes their shadow file very different to all the others.

Unix Trusted Computer Base Systems (TCB) Shadow File

When a Trusted Computer Base system is being employed, details of the user's password, audit flags and UID are held in a database in a series of files in the /tcb/files/auth directory. To obtain a composite "shadow" file by concatenating the TCB files under /tcb/files/auth we use the command:

/bin/cat /tcb/files/auth/?/* > /merged.tcb

When working with DEC/Compaq Unix TCB systems, the correct command is:

usr/tcb/bin/edauth -g > /merged.tcb

This generates a file called **merged.tcb** in the root directory. The file contents looks like this:

```
adm:u_name=adm:u_id#4:\
:u_pwd=*:\
:u_auditid#4:\
:u_auditflag#1:\
:u_pswduser=adm:u_lock@:chkent:
atstmos:u_name=atstmos:u_id#302:\
:u_pwd=OiXjiZ/S6.HZI:\
:u_auditid#96:\
:u_auditflag#1:\
:u_succhg#836990202:u_unsucchg#836919995:u_suclog#841327822:u_suctty=ttypc:\
:u_unsuclog#838289307:u_unsuctty=ttyq4:u_lock@:chkent:
bin:u_name=bin:u_id#2:\
:u_pwd=*:\
:u_auditid#2:\
:u_auditflag#1:\
:u_pswduser=bin:u_lock@:chkent:
```

A record is created for every user adm, atstmos, bin etc. The file **merge.tcb** is used as the shadow file for AZScan.

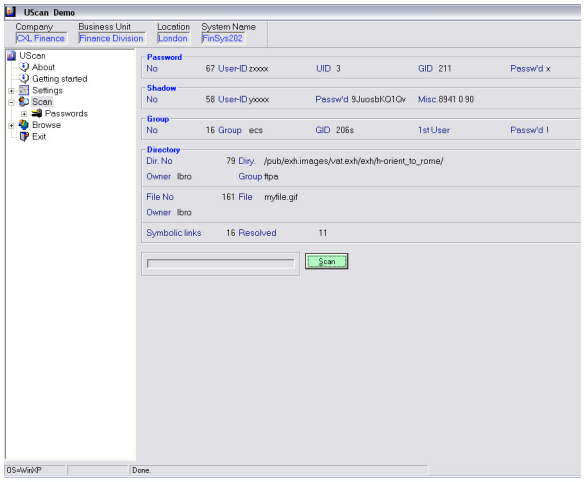
AIX Systems Shadow File

This file is normally called /etc/security/passwd and looks like this:

```
guest:
password = *

nobody:
password = *

lpd:
password = *

paul:
password = eacVScDKri4s6
lastupdate = 1026394230
flags = ADMCHG
```

Unix Scanning

When the correct files have been collected and fed into AZScan, the system will begin reviewing them. The time taken to perform the review will mainly be dependant on the size of the directory file. These can run to many megabytes and the storing and processing of this data can take some time.



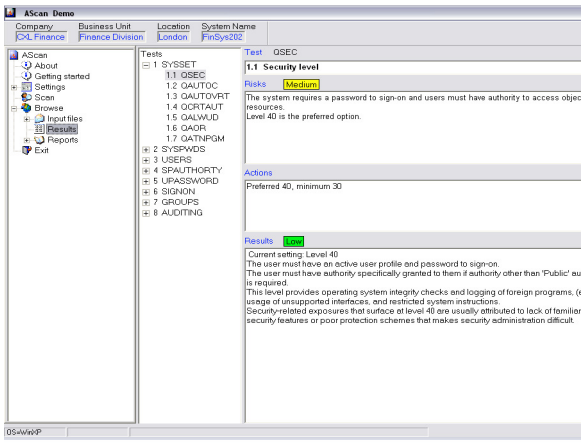
An added complexity which is handled by the software are ‘symbolic links’ where one directory entry is not actually a file but just a link to another file which in turn could be a real file or just another link

Passwords

The usual method for encrypting passwords on many Unix systems is a complex, one-way algorithm which creates passwords which cannot be decrypted. However, the code for this algorithm is readily available and can be used to try to guess passwords. The shadow password file holds the user passwords in this encrypted form and AZScan employs its own version of the algorithm to guess the passwords held in the shadow file. AZScan uses a dictionary of about common 40,000 words and also tries the user names, and sections from the GCOS field of the password file. On large systems, it always manages to guess some of them. In addition, you can also add your own favourite words which may be common where you live (local sports teams, city names etc).

As this is a very sensitive area, guessed passwords are not produced as part of the normal reports but they can be seen on screen as AZScan tries to guess them.

Unix Results



Results can either be reviewed on screen or in printed format. The RESULTS screen is shown here.

The tests have been grouped together into sections and you navigate through each one using the middle treeview.

Reports can either be viewed on screen or printed out but be warned, some reports can be very large.

Tip

If you have produced a Word report, use the Heat Map to identify problem areas and then pull the Word format report into MSWord and just print the sections you think are important.

Reports are produced in various formats:

- Plain text formatted with page breaks.
- MS Word format
- HTML

In addition, reports are either Full, Summary or Heatmaps.

It should be noted that the Word format version should not be read using MS Wordpad. Please use MS Word as Wordpad has a number of problems which change the formatting of reports.

Unix Operating Systems Versions

Shown below are the 118 versions of Unix which AZScan is capable of reviewing. If you don't see the version you want, just email CXL and we will work on it.

1 AIX 1.x
2 AIX 2.x
3 AIX 3.x
4 AIX 4.x
5 AIX 5L
6 AIX PS2
7 AIX/370
8 AIX/6000
9 AOS
10 Arix
11 AUX 3.x
12 BOS V1.x
13 BOS V2.x
14 BOS V3.x
15 BSD 1.x
16 BSD 2.x
17 BSD 3.x
18 BSD 4.x
19 BSD 5.x
20 Chorus
21 Coherent 3.x
22 Coherent 4.x
23 Consensys
24 ConvexOS 10
25 ConvexOS 11
26 Cromix
27 CTIX
28 DELL UNIX
29 DGUX 4.x
30 DGUX 5.x
31 Digital 3 TCB
32 Digital 4 TCB
33 Digital Unix 3
34 Digital Unix 4
35 DOMAINIX
36 DOMAINOS 10.x
37 DVIX
38 DYNIX 1.x ptx
39 DYNIX 2.x ptx
40 DYNIX 3.x ptx
41 DYNIX 4.x ptx
42 DYNIX 5.x ptx
43 EP/IX
44 ESIX
45 EuNIX
46 FreeBSD 1.x
48 FreeBSD 3.x
49 FreeBSD 4.x
50 FreeBSD 5.x
51 HP-UX 10 TCB
52 HP-UX 10.x
53 HP-UX 11.x
54 HP-UX 5.x
55 HP-UX 6.x
56 HP-UX 7.x
57 HP-UX 8.x
58 HP-UX 9.x
59 ICL Unix NX5
60 ICL Unix NX6
61 ICL Unix NX7
62 IDRIS
63 IRIX 3.x
64 IRIX 4.x
65 IRIX 5.x
66 IRIX 6.x
67 LINUX
68 LINUX Red Hat
69 NCR Unix
70 NetBSD
71 NeXT 1.x
72 NeXT 2.x
73 NeXT 3.x
74 OSF/1 1.x
75 OSF/1 2.x
76 OSF/1 3.x
77 OSx
78 RiscIX
79 Riscos 4.x
80 Riscos 5.x
81 SCO 2.x
82 SCO 3.x
83 SCO 3.x TCB
84 SCO 4.x
85 SCO 4.x TCB
86 SCO 5.x
87 SCO 5.x TCB
88 SINIX 5.x
89 Solaris 1.x
90 Solaris 10
91 Solaris 2.x
92 Solaris 7
93 Solaris 8
95 SunOS 4.x
96 SunOS 5.x
97 SVR3
98 SVR4
99 System V.3
100 System V.4
101 Tru64 4
102 Tru64 5
103 Ultrix 2.x
104 Ultrix 3.x
105 Ultrix 4.x
106 Unicos 5.x
107 Unicos 6.x
108 Unicos 7.0
109 Unicos 8.0
110 Unicos 9.0
111 Unixware 1.x
112 Unixware 2.x
113 Unixware 7.x
114 UTS
115 Xenix 1
116 Xenix 2
117 Xenix 3
118 Zeus

47 FreeBSD 2.x 94 Solaris 9

Unix Tests

The tests performed by AZScan on Unix systems are shown below. They have been grouped together into logical sections and the risk that each presents is marked and colour coded as high, medium and low. At present there are over 70 tests.

No	Code	Description	Risk
1	UPWDS	User Passwords	
1 1.1	DUPPWD	Duplicate names in password file	Low
2 1.2	NOPWD	Users without passwords	High
3 1.3	DISPWD	Disabled accounts	Low
4 1.4	BADFIELD	Incorrect number of fields	Medium
5 1.5	UNMATCH	Unmatched password file entries	Medium
6 1.6	PWDLIFE	Password lifetimes	Medium
7 1.7	ACCTINFO	Account information	Low
2	UUIDS	User UIDs	
8 2.1	ZEROUID	UID=0	Medium
9 2.2	NOUID	No UID	High
10 2.3	BADUID	Invalid UIDs	High
11 2.4	DUPUID	Duplicate UIDs in the password file	Medium
3	UGIDS	User GIDs	
12 3.1	ZEROGID	Users with GID=0	Low
13 3.2	NOGID	Users with no GID	Medium
14 3.3	BADGID	Users with an invalid GID	Medium
15 3.4	DUPGID	Duplicate GIDs in the password file	Low
16 3.5	EXSTGID	Non-existent GIDs	Low
4	UHDIRS.	User Home dirs.	
17 4.1	NOHDIR	No home directory	Low
18 4.2	INVHDIR	Invalid home directory	Medium
19 4.3	SHAREHDIR	Shared home directory	Low
20 4.4	STKYHDIR	Non-Sticky home directory	Low
21 4.5	WRITEHDIR	Writeable home directory	Medium
22 4.6	SUSHDIR	Home directory contains suspicious files	High
5	USHELLS	User Shells	
23 5.1	NOSHELL	No shell shown	Low
24 5.2	INVSHELL	Invalid shells	Low
25 5.3	SHARESHELL	Shared shells	Low
26 5.4	SUIDSHELL	Shells which are SUID/SGID	Medium
27 5.5	WRITESHELL	Shells which are writeable	Medium
6	GRPS	Groups	
28 6.1	DUPGRPNAME	Duplicate group names	Low
29 6.2	PWDGROUP	Password protected	Low
30 6.3	BADFIELDS	Improper number of fields	Low
31 6.4	NOUSERGRP	No users	Low
32 6.5	BADUSER	Non-existent users	Low
33 6.6	DUPUSER	Duplicate users	Low
34 6.7	USRSGRP	Users in each group	Low
7	GRPGIDS	Group GIDs	
35 7.1	ZEROGID	GID=0	Low
36 7.2	NOGID	No GID	Low
37 7.3	BADGID	Invalid GIDs	Low
38 7.4	DUPGID	Duplicate GIDs	Low
8	FILES	Files	
39 8.1	UKNOWNR	Files - Unknown owners	Low
40 8.2	UKNGRPS	Files - Unknown groups	Low
41 8.3	WLDWRITE	Files - WORLD writeable	Medium
42 8.4	WLDEXEC	Files - WORLD executable	Medium
43 8.5	GRPWRIT	Files - GROUP writeable	Low
44 8.6	GRPEXEC	Files - GROUP executable	Low
45 8.7	BADPRIV	Files - Uneven privileges	Medium
46 8.8	SUID	Files - SUID	Low
47 8.9	SGID	Files - SGID	Low
48 8.10	STICKY	Files - Sticky	Low
49 8.11	SUID+WW	Files - SUID/SGID and WORLD executable/writeable	Medium
50 8.12	HOSTINFO	Files likely to contain host information	Medium
51 8.13	SUWW	Startup files which are world writeable	High
52 8.14	FILUS	File has an unusual name	Low
9	DIRS	Directories	
53 9.1	UNKOWN	Dir - Unknown owners	Medium
54 9.2	UNKGRP	Dir - Unknown groups	Low
55 9.3	WRLDWRT	Dir - WORLD writeable	Medium
56 9.4	WRLDEXE	Dir - WORLD executable	Medium
57 9.5	GRPWRT	Dir - GROUP writeable	Medium
58 9.6	GRPEXE	Dir - GROUP executable	Medium
59 9.7	BADPRIV	Dir - Uneven privileges	Medium
60 9.8	SGID	Dir - SGID	Low

61 9.9	NSTICKY	Dir - Not Sticky	**Low**
10	FTP	FTP	
62 10.1	FTPOWNBIN	Anonymous FTP bin directory has wrong owner	**Low**
63 10.2	FTPOWNETC	Anonymous FTP etc directory has wrong owner	**Medium**
64 10.3	FTPHDIROWN	Anonymous FTP home directory has wrong owner	**Medium**
11	/ETC	/etc	
65 11.1	ETCWW	Directories under /etc has world write access	**Medium**
66 11.2	ETCPWD	File /etc/default/passwd has insecure permissions	**Medium**
67 11.3	ETCPROF	File /etc/profile has insecure permissions	**Medium**
12	LOG FILES	Log files	
68 12.1	LOGLOGEX	The login log file does not exist	**Medium**
69 12.2	LOGLOGOWN	Login log not owned by user root and group root or sys	**Medium**
13	TCB	TCB	
70 13.1	PARAMS	Trusted Computing Base parameters	**Low**
71 13.2	USERLIST	TCB User list - owners and audit flags	**Low**
72 13.3	TCBLOGIN	TCB User login details	**Low**
14	NIS	NIS	
73 14.1	NISUSED	Is NIS being used	**Low**

OpenVMS Reviews

Introduction

AZScan is designed to review VMS based systems. Originally, this was the proprietary operating system of DEC who are now owned by Compaq. The operating system is now called OpenVMS and the hardware has also undergone name changes (Alphas).

VMS is a very secure operating system and each user can be individually set up with as many or as few security facilities as they need to do their job. Similarly, incorrect settings can make this a very insecure system.

Obtaining the files

To enable AZScan to work, you have to give it a file from the Alpha/VAX system being reviewed. This file is produced using a very simple command issued by a System Manager. The file produced is then copied to the PC running AZScan. Ask the system manager to produce the file for you by issuing the following command:

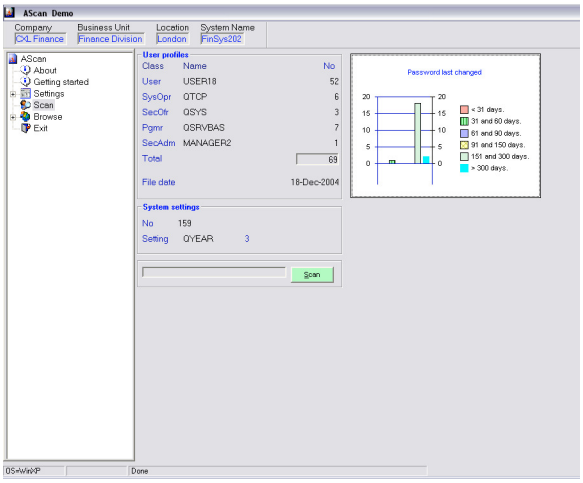
$ mc authorize list */full

The command generates a SysUAF file called 'sysuaf.lis'. The '/full' is very important. If you examine the file, it will look like this:-

```
Username: GEN_PM                                    Owner: DEP - P.SMITH
Account: GENX                                       UIC: [100,10] ([GEN,BBL])
CLI:   DCL                                          Tables: DCLTABLES
Default: GEN_DISK:[GEN]                             LGICMD: LOG$:LOGIN
Flags: DisPwdDic Captive
Primary days: Mon Tue Wed Thu Fri                   Secondary days: Sat Sun
No access restrictions
Expiration: 47 00:00          Pwdminimum: 2         Login Fails: 17   etc….
```

Copy this file using a disk or via a network/email to the PC running AZScan. Rename the file carefully when you copy it to the PC as it is usually called sysuaf.lis on the Alpha/Vax system.

Scanning



AZScan will review the files very quickly and progress can be watched on screen. Producing the reports is also fast too although if you have selected MS Word format, the production of this report can be slow due to the way Word works.

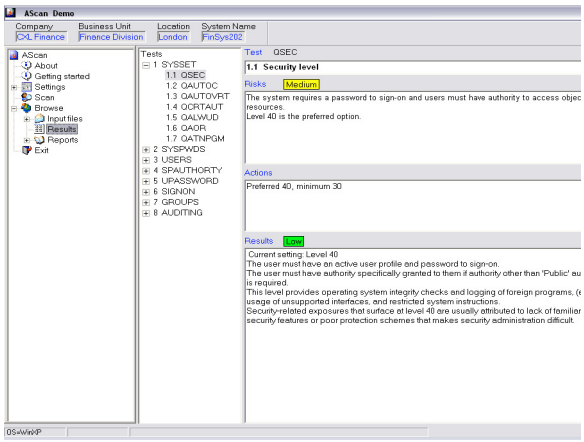
Tip

It is suggested that you only produce the Word format report after the text and HTML versions have been produced and checked.

Tip

The Word format report is great for importing straight into your written report on the system.

OpenVMS Results



Results can either be reviewed on screen or in printed format. The RESULTS screen is shown here.

The tests have been grouped together into sections and you navigate through each one using the middle treeview.

Reports can either be viewed on screen or printed out but be warned, some reports can be very large.

Tip

If you have produced a Word report, use the Heat Map to identify problem areas and then pull the Word format report into MSWord and just print the sections you think are important.

Reports are produced in various formats:

- Plain text formatted with page breaks.
- MS Word format
- HTML

In addition, reports are either Full, Summary or Heatmaps.

It should be noted that the Word format version should not be read using MS Wordpad. Please use MS Word as Wordpad has a number of problems which change the formatting of reports.

OpenVMS Systems

Shown below are the versions of VMS which AZScan is capable of reviewing.

No	Name
1	VMS 5.4
2	VMS 5.3
3	VMS 5.2
4	VMS 5.1
5	VMS 5.0
6	VMS 4.7
7	VMS 4.6
8	VMS 4.5
9	VMS 4.4
10	VMS 4.3
11	VMS 4.2
12	VMS 4.0
13	OpenVMS 8.1
14	OpenVMS 8.0
15	OpenVMS 7.3
16	OpenVMS 7.2
17	OpenVMS 7.1
18	OpenVMS 6.2
19	OpenVMS 6.1
20	OpenVMS 5.5

OpenVMS Tests

Shown below are the 93 VMS tests performed by AZScan.

No	Code	Description	Risk
1	SUMMARY	Summary	
1 1.1	PRIVS	Privileges	High
2 1.2	LEVELS	Levels	High
3 1.3	FLAGS	Flags	High
4 1.4	NETLI	Network Logins	Medium
2	PWDS	Passwords	
5 2.1	PWDLIFE	Password life	Medium
6 2.2	PWDLENU	Users password length	Medium
7 2.3	PWDCHANGES	Distribution of password changes	Medium
8 2.4	PWDLEN	Password length	Medium
3	A/C	Accounts	
9 3.1	UNA/C	Unused accounts	Medium
10 3.2	NOOWN	No owners	Low
4	SPAC	Specific accounts	
11 4.1	AC-SYSTEM	SYSTEM Account	High
12 4.2	AC-FIELD	FIELD Account	High
13 4.3	AC-DEFAULT	DEFAULT Account	High
5	LOGINS	Logins	
14 5.1	LINOI	Non-interactive Logins	Low
15 5.2	LIBOT	Both types of login	Low
16 5.3	LIINT	Interactive logins	Low
17 5.4	LLOGINS	Last logins	Low
18 5.5	LIFAIL	Login failures	Low
19 5.6	DEFDIR	Default Directories	Low
20 5.7	CLI	CLI	Low
21 5.8	LGICMD	LGICMD	Low
22 5.9	NCAPTIVE	Non-Captive	Medium
6	UICS	UICs	
23 6.1	SHUICS	Shared UICs	Medium
24 6.2	LOWUICS	Low value UICs	Medium
7	SYSSET	System settings	
25 7.1	UNLCPU	Unlimited cpu	Medium
26 7.2	PRCLM	PRCLM	Low
27 7.3	MXDETACH	Max Detached	Medium
8	FLAGS	Flags	
28 8.1	CAPTIVE	Captive	Low
29 8.2	DISWELCOME	Diswelcome	Medium
30 8.3	DISNEWMAIL	Disnewmail	Low
31 8.4	DISMAIL	Flag - Dismail	Low
32 8.5	GENPWD	Flag - Genpwd	Medium
33 8.6	DISIMAGE	Flag - Disimage	Low
34 8.7	DISRECONNECT	Flag - Disreconnect	Low
35 8.8	DISREPORT	Flag - Disreport	High
36 8.9	DISUSER	Flag - Disuser	Low
37 8.10	LOCKPWD	Flag - Lockpwd	Medium
38 8.11	PWD_EXPIRED	Flag - Pwd_expired	Low
39 8.12	RESTRICTED	Flag - Restricted	Low
40 8.13	DISPWDDIC	Flag - Dispwddic	Medium
41 8.14	DEFCLI	Flag - Defcli	Medium
42 8.15	DISCTLY	Flag - Disctly	Low
43 8.16	AUDIT	Flag - Audit	Low
44 8.17	AUTOLOGIN	Flag - AutoLogin	Low
45 8.18	DISFORCE_PWD_CHANGE	Flag - Disforce_pwd_change	Medium
46 8.19	DISPWDHIS	Flag - Dispwdhis	Medium
47 8.20	PWD2_EXPIRED	Flag - Pwd2_Expired	Low
48 8.21	EXTAUTH	Flag - External authentication	Low
49 8.22	VMSAUTH	Flag - VMSauth	Low

50 8.23	PWDMIX	Flag - PwdMix	**Medium**
51 8.24	DISPWDSYNCH	Flag - DisPwdSynch	**Low**
9	LEVELS	Levels	
52 9.1	LEVELS4-6	Levels 4 to 6	**High**
10	PRIVS	Privileges	
53 10.1	ACNT	Privilege - Acnt	**Low**
54 10.2	ALLSPOOL	Privilege - Allspool	**Low**
55 10.3	ALTPRI	Privilege - Altpri	**Medium**
56 10.4	BUGCHK	Privilege - BugChk	**Medium**
57 10.5	BYPASS	Privilege - ByPass	**Medium**
58 10.6	CMEXEC	Privilege - Cmexec	**Low**
59 10.7	CMKRNL	Privilege - Cmkrnl	**Medium**
60 10.8	DETACH	Privilege - Detach	**Low**
61 10.9	DIAGNOSE	Privilege - Diagnose	**Low**
62 10.10	EXQUOTA	Privilege - Exquota	**Low**
63 10.11	GROUP	Privilege - Group	**Low**
64 10.12	GRPNAM	Privilege - Grpnam	**Low**
65 10.13	GRPPRV	Privilege - Grpprv	**Low**
66 10.14	LOGIO	Privilege - LogIO	**Low**
67 10.15	MOUNT	Privilege - Mount	**Medium**
68 10.16	NETMBX	Privilege - Netmbx	**Low**
69 10.17	OPER	Privilege - Oper	**Medium**
70 10.18	PFNMAP	Privilege - Pfnmap	**Low**
71 10.19	PHYIO	Privilege - Phyio	**Medium**
72 10.20	PRMCEB	Privilege - Prmceb	**Low**
73 10.21	PRMGBL	Privilege - Prmgbl	**Low**
74 10.22	PRMMBX	Privilege - Prmmbx	**Low**
75 10.23	PSWAPM	Privilege - Pswapm	**Low**
76 10.24	READALL	Privilege - Readall	**High**
77 10.25	PSECY	Privilege - Security	**High**
78 10.26	SETPRV	Privilege - Setprv	**Medium**
79 10.27	SHARE	Privilege - Share	**Low**
80 10.28	SHMEM	Privilege - Shmem	**Low**
81 10.29	SYSGBL	Privilege - Sysgbl	**Medium**
82 10.30	SYSLCK	Privilege - Syslck	**Medium**
83 10.31	SYSNAM	Privilege - Sysnam	**High**
84 10.32	SYSPRV	Privilege - Sysprv	**High**
85 10.33	TMPMBX	Privilege - Tmpmbx	**Low**
86 10.34	VOLPRO	Privilege - Volpro	**Low**
87 10.35	WORLD	Privilege - World	**Low**
88 10.36	AUDIT	Privilege - Audit	**Medium**
89 10.37	DGRADE	Privilege - Downgrade	**Medium**
90 10.38	PIMPT	Privilege - Import	**Low**
91 10.39	UGRADE	Privilege - Upgrade	**Low**
92 10.40	IPNATE	Privilege - Impersonate	**Medium**
93 10.41	OVERALL	Flags/Privilege - Overall	**Medium**

Oracle Database Reviews

Introduction

AZScan is designed to review Oracle database systems too.

Obtaining the Oracle Input file

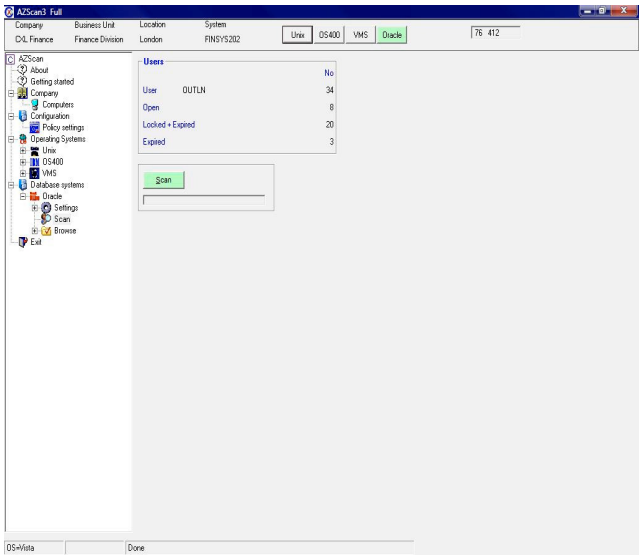
To enable AZScan to review Oracle systems, you have to give it a file from the system being reviewed. This file is produced using a simple script which we supply with the software. The script is run, usually by your system manager or database administrator, and an output file is produced. This file is then copied to the PC running AZScan.

This file can be very large (several gigabytes) but AZScan can read this fairly quickly.

Copy this file to the PC running AZScan and you are ready to begin scanning.

Oracle Scanning

AZScan will review the files very quickly and progress can be watched on screen. Producing the reports is also fast too although if you have selected MS Word format, the production of this report can be slow due to the way Word works.



Tip

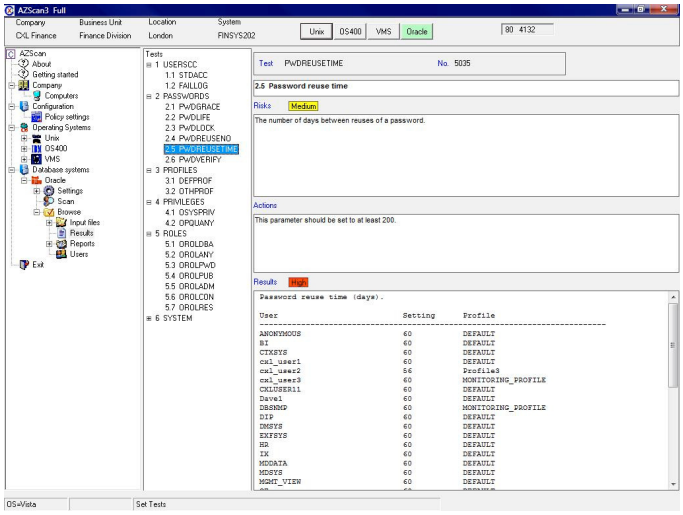
It is suggested that you only produce the Word format report after the text and HTML versions have been produced and checked.

Tip

The Word format report is great for importing straight into your written report on the system.

Oracle Results

Results can either be viewed on screen or in printed format. The RESULTS screen is shown here.



The tests have been grouped together into sections and you navigate through each one using the middle treeview.

Reports can either be viewed on screen or printed out but be warned, some reports can be very large.

Tip

If you have produced a Word report, use the Heat Map to identify problem areas and then pull the Word format report into MSWord and just print the sections you think are important.

Reports are produced in various formats:

- Plain text formatted with page breaks.
- MS Word format
- HTML

In addition, reports are either Full, Summary or Heatmaps.

It should be noted that the Word format version should not be read using MS Wordpad. Please use MS Word as Wordpad has a number of problems which change the formatting of reports.

Oracle Versions

The following versions of Oracle databases are able to be reviewed:

1	Oracle 7	(1992)
2	Oracle 8I	(1997)
3	Oracle 9I	(2001)
4	Oracle 10g	(2003)

Oracle Tests

Shown below are the 22 Oracle tests performed by AZScan.

No	Code	Description	Risk
1	USERSCC	Users	
1 1.1	STDACC	Standard accounts	**High**
2 1.2	FAILLOG	Failed logins allowed	**Low**
2	PASSWORDS	Passwords	
3 2.1	PWDGRACE	Password grace time	**Low**
4 2.2	PWDLIFE	Password life time	**High**
5 2.3	PWDLOCK	Password lock time	**Low**
6 2.4	PWDREUSENO	Password reuse number	**Medium**
7 2.5	PWDREUSETIME	Password reuse time	**Medium**
8 2.6	PWDVERIFY	Password verify function	**Low**
3	PROFILES	User profiles	
9 3.1	DEFPROF	The DEFAULT profile	**Low**
10 3.2	OTHPROF	Other profiles	**Low**
4	PRIVILEGES	Privileges	
11 4.1	OSYSPRIV	User's system privileges	**Medium**
12 4.2	OPQUANY	Users with ANY privilege	**Medium**
5	ROLES	Roles	
13 5.1	OROLDBA	Users granted the DBA Role	**High**
14 5.2	OROLANY	Roles with ANY privilege	**Medium**
15 5.3	OROLPWD	Roles without passwords	**Low**
16 5.4	OROLPUB	Roles granted to PUBLIC	**Medium**
17 5.5	OROLADM	Roles granted with ADMIN	**Medium**
18 5.6	OROLCON	Users with the CONNECT role	**Medium**
19 5.7	OROLRES	Users with the RESOURCE role	**Medium**
6	SYSTEM	System settings	
20 6.1	SYSLOGPWDFILE	Remote login password file	**Medium**
21 6.2	SYSOSAUTH	Remote OS authentication	**High**
22 6.3	SYSDATADIC	Data dictionary Accessibility	**Medium**