UNIX SECURITY AUDITOR

FOR IDEA 10

Comprehensive and easy to use.

Provides a wealth of detail to provide key information about the security of UNIX boxes

50 plus scripts that integrate flawlessly into IDEA

WHY DO YOU NEED TO AUDIT UNIX BOXES ANYWAY?

- UNIX is inherently unsecure;
- Security may not have been considered or implemented correctly;
- It may not have been a strategic purpose and may be administered by the end users.

HOWEVER, RUNNING AN UNIX AUDIT, WITHOUT A SPECIALISED TOOL, CAN CAUSE NUMEROUS PROBLEMS.

These include:

1. Testing becomes complicated very quickly, even with just a small number of users on the system.
2. Within UNIX, it is very easy to get the user and file/directory security horribly wrong.
3. There may not be central IT control over the UNIX environment.
4. UNIX is traditionally used in a network environment, often for internet and intranet connectivity.
5. Many database systems use UNIX as the underlying operating system – the database is well controlled but no review is undertaken of the UNIX system that the database resides upon.

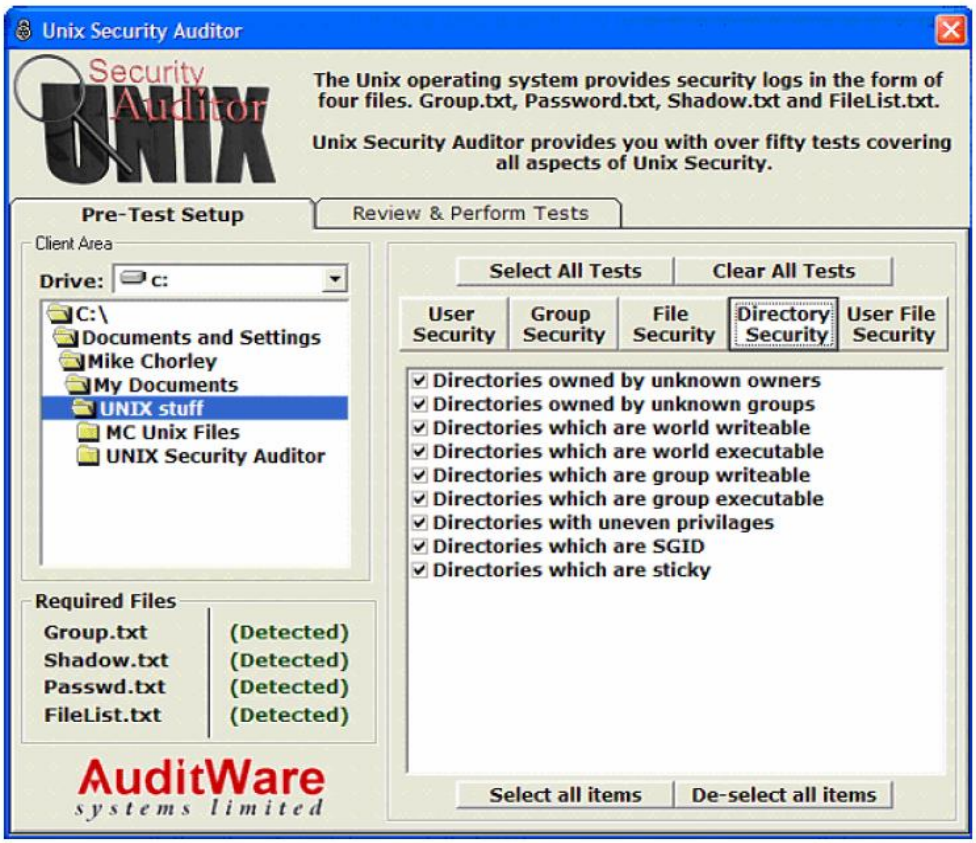
HOW CAN YOU RESOLVE THESE PROBLEMS?

? You could **do nothing**. Easy to do, but this will present you with major challenges at a later date, especially if something goes desperately wrong.

? Carry out a **manual review**, which only allows you to look at a small sample of records and therefore dramatically lacks accuracy.

? **Use the existing security software that the IT department might have.** This could appear the most appropriate choice, however, they might not let you have the necessary permission and if anything goes wrong on the system, you will likely face the blame.

✓ Purchase **UNIX Security Auditor** and let your PC carry out the audit and review for you. All the significant tests and programmed for you and you can carry out further work on the file it creates.



THE UNIX SECURITY AUDITOR BENEFITS

- 100% testing of all records audited;
- Let your PC do the work for you while you look at other critical areas or projects;
- The ability to carry out further analysis and manipulation of the results file;
- A consistent and professional approach for UNIX audits;
- A non-invasive review of your target systems;
- Access to the experience and expertise of UNIX specialists, so you don't have to employ people with these skills;
- Reassurance that some of the most risky systems in your organisation are operating as expected and in a controlled manner;

Four main files are interrogated. These include the Password, Shadow, Group and File/Directory Listing files.

UNIX Security Auditor carries out 50 tests against these files and creates a text report file and an IDEA IMD file of all the test results.

Some of the tests include:

- Primary GID;
- Secondary GID;
- Users With an Invalid Home Directory;
- Users With No Home Directory;
- Users With No/Invalid GID;
- Users With No/Invalid UID;
- Users Without a Shell;
- Directories Owned by Unknown Groups;
- Directories Which are World Executable;
- Directories With Uneven Privileges;
- Files Which Are World Writeable;
- Files With Uneven Privileges;
- Home Directory Not Sticky;
- Home Directory Writeable by Others;
- Groups With No Users;
- Users With an Invalid Shell;
- Sticky Files;
- Duplicate Names in Password File;
- Groups With the Same Name;

AuditWare

www.auditware.co.uk | sales@auditware.co.uk

twitter.com/auditware | linkedin.com/company/auditware

+44 (0) 1892 514334