Summary Report: TESTBED Linux

System: Linuxwhite
Analysis Date: 04-Nov-2013 CONFIDENTIAL

Rating Against Industry Average

☺	😐	☹
	X	

Overall Comments

Overall, security on this machine is about average compared with other UNIX systems used in the Communications sector.

Note that 78% of user accounts are disabled.

Report Highlights

Report Section / Comments	
1	**Summary Graphs** Graphical comparisons against the industry average and leading practice.
2	**System Policy** System-wide Policy settings seem reasonable.
3	**Password Shadowing** The system is using passwd shadowing features.
4	**Usernames, UIDs, Home Directories** There are 47 accounts defined on this system. 36 are disabled. In general, accounts are clearly assigned to specific people. 2 accounts have a UID equal to 0. However, one is disabled.
6	**Discrepancies in Passwd and Shadow Password Files** Probably indicates a housekeeping issue.
7	**Duplicate Usernames, UIDs, GIDs** May indicate a housekeeping issue.
8	**Password Change Intervals** Regular password changes are not enforced for many accounts. However, most accounts are disabled.
9	**Redundant Groups** May indicate a housekeeping issue.
10	**Disabled Usernames** 36 accounts are disabled.
11	**Trivial Passwords** SekChek found 2 accounts with trivial passwords.

This report summary is provided to highlight some of the main issues detailed in the SekChek reports. The overall rating is against the industry average and not against leading practice. All comments are generic. For best results they should be considered together with an understanding of the client's own unique business and computer environments.

Report Section / Comments
12 Password Changes Passwords for 74% (35) of accounts have not been changed in the last 90 days. However, most accounts are disabled. Regular password changes are not enforced for most accounts.
13 Last Logons You should check the list for accounts that are inactive and redundant.
16 Files with World Writeable Permissions You should check this list for signs of sensitive files with world-writeable permissions on them.
17 Permissions on Selected Files The client should check this list for signs of sensitive files with group- or world-writeable permissions on them.
19 SUID Permissions Permissions on programs that switch User Id (SUID) seem reasonable.
20 SGID Permissions Permissions on programs that switch Group Id (SGID) seem reasonable.
21 Network Services You should check what information is given out by finger. This information is often helpful to intruders.
23 Trusted Hosts There is 1 trusted host defined to the system. Note that security on the system analysed is very dependent on the strength of user authentication controls on the trusted host.
24 Trusted Users SekChek did not find any rhosts files in users' home directories.
25 FTP Access In general, you should ensure powerful accounts (e.g. those with a UID = 0) are prevented from accessing the system via ftp.

Tip: Make navigation easier by adding the back button  *to your Quick Access Toolbar in MS-Word.*