

Summary Report: TESTBED Linux

System: Linuxwhite
Analysis Date: 09-Sep-2010

CONFIDENTIAL

Rating Against Industry Average

		
		X

Overall Comments

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

Report Highlights

Report Section	Comments
2	The system is using passwd shadowing features.
3	Many accounts are not clearly assigned to specific people. This could raise accountability concerns if they have access to powerful functions or sensitive information. 3 accounts have a UID equal to 0. None of these accounts are disabled.
6	May indicate a housekeeping issue.
7	May indicate a (minor) housekeeping issue.
8	34 accounts are disabled. Most of these are system/pseudo-ids.
9	<i>SekChek</i> found 3 accounts with trivial passwords assigned to them.
10	Passwords for 100% (47) of accounts have not been changed in the last 90 days.
11	Most accounts seem to be active.
14	The client should check this list for signs of sensitive files with world-writeable permissions on them.
17	Permissions on programs that SUID (switch User Id) seem reasonable.
18	Permissions on programs that SGID (switch Group Id) seem reasonable.
21	There is 1 trusted host defined to the system. <i>Note that security on the system analysed is very dependent on the quality of security (particularly user authentication controls) on the trusted hosts also.</i>
22	<i>SekChek</i> did not find any <i>rhosts</i> files in users' home directories.
23	We generally recommend that powerful accounts (e.g. those with a UID = 0) are prevented from accessing the system via <i>ftp</i> .

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.