

Summary Report: TESTBED Win2003 DC

System: ZEUS (olympus.com)
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Rating Against Industry Average

		
	X	

Overall Comments

Overall, security is about average compared with other Active Directory domains.
The machine does not have the latest Service Pack for Windows installed. The latest is SP2.

Report Highlights

Report Section	Comments
3	Some System policies are weak, for example: <ul style="list-style-type: none">Controls that reduce the risk of intruders gaining access to the system via repeated password guessing attempts could be strengthenedThe client should consider renaming the Administrator (uid 500) and Guest (uid 501) accounts via policy See comment 15 also.
4.1	The client is making some use of Windows' auditing features.
5	You should check the policies defined in the Group Policy Objects to ensure they are appropriate.
8	Many accounts are <i>not</i> clearly assigned to specific people. This could raise accountability concerns if they have access to sensitive functions or information. 12% (9) of accounts have security administration privileges. The Administrator account (uid 500) has not been renamed.
10	Note that 3 accounts from another domain are members of 2 local groups, including the Administrators group. These accounts will acquire the privileges of the local groups they belong to. See comment 24.5 also.
13	SekChek shows that 97% (73) of accounts have not been used in the last 3 months. Some have not been used for several years. This should be OK for service accounts.
14	Passwords for 96% (72) of accounts have not been changed in the last 3 months. Some have not been changed for several years. This should be OK for service accounts.
15	20% (15) of users are not required to change their passwords due to settings at account level. Note that these settings override the system's Policy settings (see report section 3). This should be OK for service accounts.

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.

Summary Report: TESTBED Win2003 DC

System: ZEUS (olympus.com)
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Report Section	Comments
16	12% (9) of users are allowed to logon with a zero length password due to security settings in individual user accounts. See the report for implications and a detailed explanation. See also SekChek's white paper: MS-Windows Accounts not Requiring a Password .
17	You should review the invalid logon attempts.
18	Passwords for 9% (7) of accounts can only be changed by a security administrator. This should be OK for service accounts.
20	9% (7) of accounts, including the Guest account, are disabled.
24.5	Powerful rights are assigned to accounts other than those with security administration privileges. Note that accounts from another domain will also acquire powerful privileges. See 10 above.
25	The client should check that the listed permissions over objects are appropriate and in line with users' job functions.
26	The domain analysed has trust relationships with 1 other domain. <i>Note that security on the domain analysed is very dependent on the quality of security (particularly user authentication controls) on the trusted domain also. Similarly, security on the trusting domain is very dependent on the quality of security on the domain analysed.</i>
29	7 accounts can be used to dial-in to the domain via RAS. Dial-back controls are not implemented.
30	There does not seem to be any anti-virus software running on the machine. <i>Please note that service names for anti-virus software occasionally change. If the above observation seems incorrect, please let us know so we can update SekChek's look-up tables.</i>
34	The system is using the NTFS file system.

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.