

---

# TESTBED Win2003 Server

## SekChek for Windows Security Report

---

System: PROMETHEUS (OLYMPUS)

20 December 2011

---

## Contents

SekChek Options	3
System Details	4
System Configuration	5
1. Report Summaries	8
1.1 Comparisons Against Industry Average and Leading Practice	9
1.2 Answers to Common Questions	16
1.3 Summary of Changes since the Previous Analysis	19
2. System Accounts Policy	20
3. Audit Policy Settings	23
4. Registry Key Values	25
5. User Accounts Defined On Your System	31
6. Local Groups and their Members	33
7. Global Groups and their Members (DCs only)	36
8. Last Logons, 30 Days and Older	37
9. Passwords, 30 Days and Older	39
10. Passwords that Never Expire	41
11. Invalid Logon Attempts Greater than 3	42
12. Users not Allowed to Change Passwords	43
13. Accounts with Expiry Date	44
14. Disabled Accounts	45
15. Rights and Privileges	46
15.1 Descriptions & General Recommendations for Rights	47
15.2 Rights Assigned to Local Groups	51
15.3 Rights Assigned to Global Groups (DCs only)	52
15.4 Rights Assigned to Users	53
16. Trusted and Trusting Domains (DCs only)	56
17. Local Accounts (DCs only)	57
18. Servers and Workstations	58
19. RAS Privileges	59
20. Services and Drivers on the Machine	61
21. Security Updates, Patches and Hot-Fixes	75
22. Products Installed	76
23. Current Network Connections	77
24. Domain Controllers in the Domain (DCs only)	79
25. Logical Drives	80
26. Network Shares	81
27. Home Directories, Logon Scripts and Logon Profiles	82
28. File Permissions and Auditing	84

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

SekChek Options	
Reference Number	1009090005
Requester	Richard Burns
Telephone Number	+44 (881) 846 8971
City	London
Client Country	UK
Charge Code	SEK100906
Client Code	SEK001
Client Industry Type	Communications
Host Country	UK
Security Standards Template	0 - SekChek Default
Evaluate Against Industry Type	<All>
Compare Against Previous Analysis	Not Selected
Report Format	Word 2007
Paper Size	A4 (21 x 29.7 cms)
Spelling	English UK
Large Report Format	MS-Access database
Large Report (Max Lines in Word Tables)	10000
Summary Document Requested	Yes
Scan Software Version Used	Version 5.0.4
Scan Software Release Date	14-May-2010

Your *SekChek* report was produced using the above options and parameters.

You can change these settings for all files you send to us for processing via the *Options* menu in the *SekChek* Client software on your PC. You can also tailor them (i.e. temporarily override your default options) for a specific file via the *Enter Client Details* screen. This screen is displayed:

- For *SekChek* for Windows and NetWare - during the Scan process on the target Host system;
- For *SekChek* for AS/400 and UNIX - during the file encryption process in the *SekChek* Client software.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

System Details	
Computer Name	PROMETHEUS
Windows Version	5.2 (Windows 2003)
Scan Time	06-Sep-2010 08:20
Scanned By	administrator
Computer Role**	SERVER
Domain / Work Group	OLYMPUS
Build / Service Pack	3790/

*Report Date: 20 December, 2011*

\*\* **Computer Role:** PDC = Primary Domain Controller; BDC = Backup Domain Controller; SERVER = A Server that does not control a Domain; WORKSTATION = A Workstation; UNDEFINED = Not Known.

### If SekChek is run on:

- A domain controller, it will report on security information at the domain level for users, accounts and groups and on domain-wide security settings.
- A server or workstation that is not a domain controller, it will report on security information at the local (server or workstation) level for users, accounts, groups and on security settings for that machine only. It will not analyse accounts and security settings defined at the domain level, although it will list domain or workgroup memberships.

### Declaration.

*The provided observations and recommendations are in response to a benchmarking analysis that compares the user's information security features against industry. The recommendations are organized to identify possible implications to the company based on the gathered information, to identify a leading practices risk rating of the implications and provide possible recommended actions. The benchmarking analysis and the related observations and recommendations should supplement management's analysis but should not be and cannot be solely relied upon in any instance to identify and/or remediate information security deficiencies. Further, the observations and recommendations herein do not identify the cause of a possible deficiency or the cause of any previously unidentified deficiencies. The causes of the deficiencies must be determined by management for the recommendations selected to be relevant.*

© 1996-2011 SekChek IPS. All rights reserved.

SekChek is a registered trademark of SekChek IPS. All other trademarks are the property of their respective owners.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## System Configuration

### Operating System

OS Name	Microsoft(R) Windows(R) Server 2003, Enterprise Edition
Serial Number	69713-640-3988347-45227
OS Installed	2004-04-02
Last BootUp	2010-09-06
Country Code	1
Time Zone	GMT +02:00
Boot Device	\Device\HarddiskVolume1
System Drive	C:
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
PAE Enabled	No
Visible Memory	0.250 GB
Free Memory	0.142 GB
Encryption Level	168 bits
OS Language	English - United States
OS Stock Keeping Unit Name	Unknown
Maximum Number of Processes	Unknown
Number of Licensed Users	10
Number of Current Users	2
Registered User	Dev
Data Execution Prevention (DEP)...	
DEP Available	Yes
DEP Enabled for 32-bit Appls	Yes
DEP Enabled for Drivers	Yes
DEP Policy	Opt Out

### System Recovery Options

Write an event to the system log	Yes
Send an administrative alert	Yes
Automatically restart	Yes
Write debugging information	Complete memory dump
Dump file	%SystemRoot%\MEMORY.DMP
Overwrite any existing file	Yes

### BIOS

Manufacturer	American Megatrends Inc.
BIOS	080002
Version	2.3
Release Date	2006-02-22

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)

Analysis Date: 06-Sep-2010

CONFIDENTIAL

### Base Board (Motherboard)

Manufacturer	Microsoft Corporation
Product	Virtual Machine
Serial Number	0249-3361-1329-9435-8173-0166-10
Version	5.0

### Page Files

Number of Page Files	1
Name of Page File #1	C:\pagefile.sys
Temporary Page File	No
Create Date	2004-04-02
Allocated Size	0.750 GB
Current Usage	0.004 GB
Peak Usage	0.004 GB

### Computer

Manufacturer	Microsoft Corporation
Model	Virtual Machine
System Type	X86-based PC
Remote Desktop Enabled	Unknown
Nbr of Processors	1
Total Memory	0.250 GB
BootUp State	Normal boot
Wake-up Type	Power Switch
Boot ROM Supported	Yes
Infrared (IR) Supported	No
Power Management Supported	No
Computer Role	Member Server
Domain	olympus.com

### Processors

Number of Processors	1
Processor #1...	
Manufacturer	GenuineIntel
Name	Intel(R) Pentium(R) III processor
Family	Pentium® III
Description	x86 Family 6 Model 7 Stepping 10
Processor Id	07C0A97B0001067A
Clock Speed	2929 MHz
External Clock Speed	100 MHz
Address Width	32 bits
Data Width	32 bits
Level 2 Cache Size	256 KB
Level 2 Cache Speed	2929 MHz
Number of Cores	Unknown
Nbr of Logical Processors	Unknown
Chip Socket	X1

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Availability Running/Full Power

### Network Adapters (IP enabled)

Connection Id	Local Area Connection
Connection Status	Connected
Name	Intel 21140-Based PCI Fast Ethernet Adapter (Generic)
Service Name	DC21x4
Manufacturer	Intel
Adapter Type	Ethernet 802.3
Speed (Mbs)	Unknown Mbs
Last Reset	2010-09-06 03:34:11
IP Enabled	Yes
IP Address	200.200.100.184
IP Subnet	255.255.255.0
Default Gateway	
MAC Address	00:03:FF:69:9D:5E
DHCP Enabled	No
DHCP Lease Expires	
DHCP Lease Obtained	
DHCP Server	
DNS Search Order	200.200.100.181

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

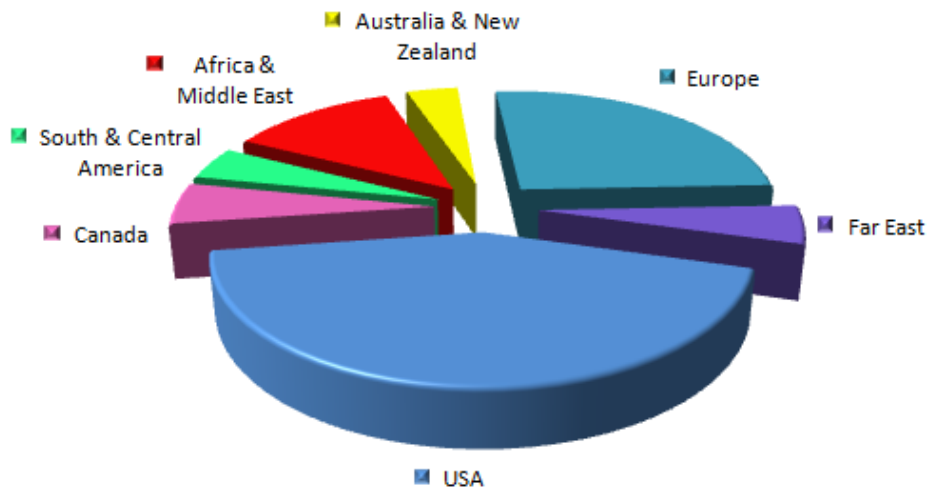
CONFIDENTIAL

## 1. Report Summaries

The following two charts illustrate the diversity of regions and industries that make up the population of *Windows systems (excluding Domain Controllers running Active Directory)* in our statistics database. The remaining graphs in the *Report Summary* section evaluate security on your system against this broad base of real-life security averages.

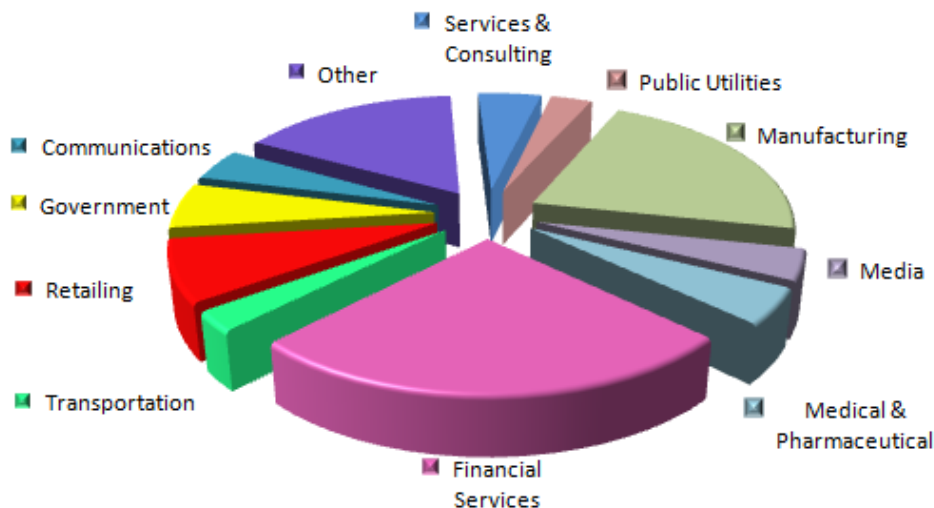
SekChek is used by the Big Four audit firms, IS professionals, internal auditors, security consultants & general management in more than 120 countries.

### Statistics Population by Region



As new reviews are processed, summaries of the results (excluding client identification) are automatically added to a unique statistics database containing more than 60,000 assessments.

### Statistics Population by Industry Type



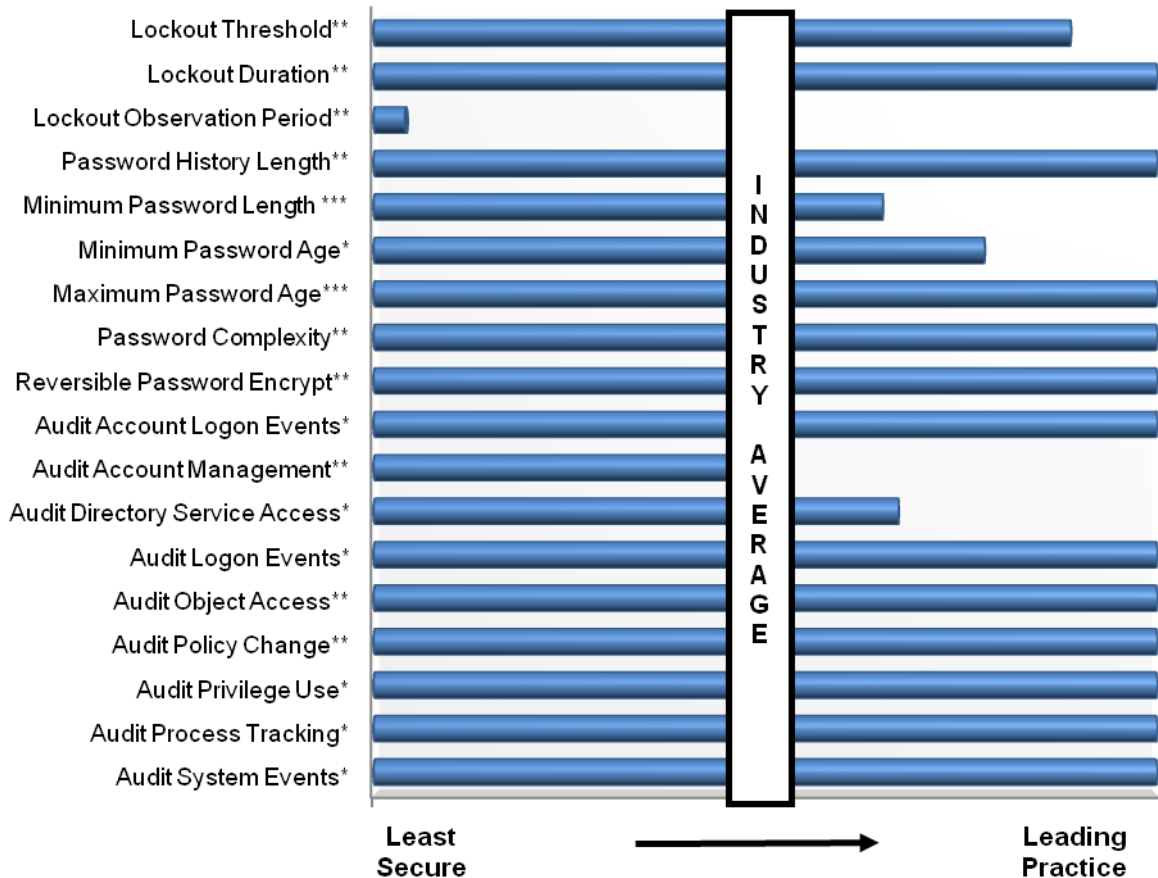
# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 1.1 Comparisons Against Industry Average and Leading Practice

### Summary of Policy Values



This graph compares your Policy values against the industry average using the following criteria:  
Country = <All>; Industry Type = <All>; Machine Size (Nbr of Accounts) = <All>

This and the following summary reports are of most value when they are used to compare 'snapshots' of your security measures at different points in time. Used in this way, they provide a fairly clear picture of whether your security measures are improving or becoming weaker.

**Industry Average** is a dynamic, calculated average for *all* Microsoft Windows systems processed by *SekChek* using the above criteria. It indicates how your security measures compare with those of other organisations using Microsoft Windows systems..

**Leading Practice** is the standard adopted by the top 10 to 20 percent of organisations.

**Asterisks** (\*) after Policy Values indicate their relative importance and individual contribution towards security of your system. I.e. Policy Values followed by 3 asterisks (\*\*\*) are considered more important, and to have a greater impact on security than those followed by 1 asterisk (\*). This is an approximation and should be used as a guide only.

For more information and details, see the report sections [System Accounts Policy](#) and [Audit Policy Settings](#).

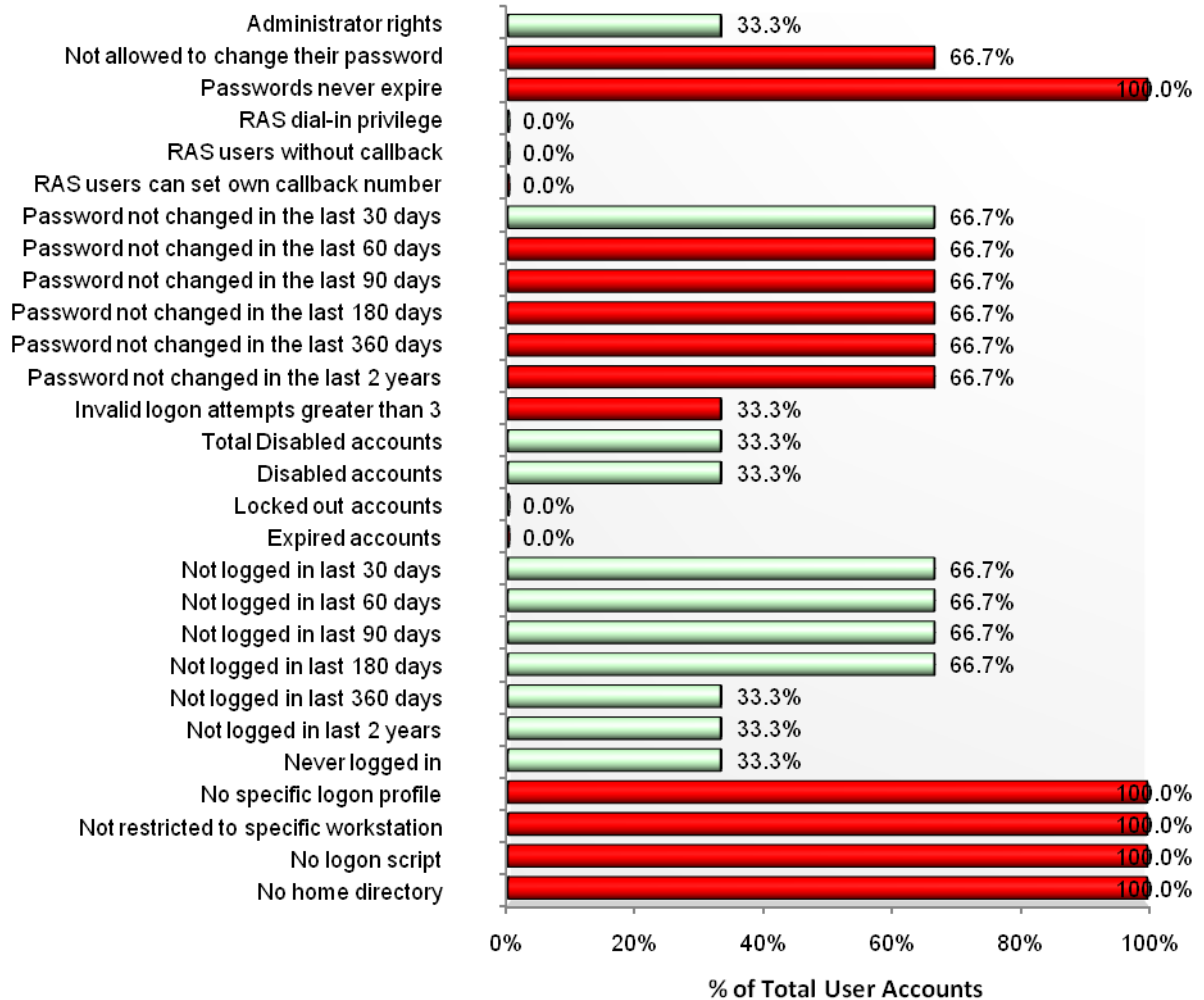
# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## Comparisons Against Industry Average and Leading Practice (Cont.)

### Summary of User Accounts



This graph compares against the industry average using the following criteria:  
Country = <All>; Industry Type = <All>; Machine Size (Nbr of Accounts) = Very Small  
■ Better than the industry average; ■ Worse than the industry average

Total number of user accounts defined to your system: 3

This summary report presents the number of user accounts, with the listed characteristics, as a percentage of the total number of accounts defined to your system. In general, longer bars highlight potential weaknesses in your security measures and should be investigated. For more details, refer to the relevant sections in the main body of the report.

The graph is sorted in order of importance. This is an approximation and should be used as a guide only.

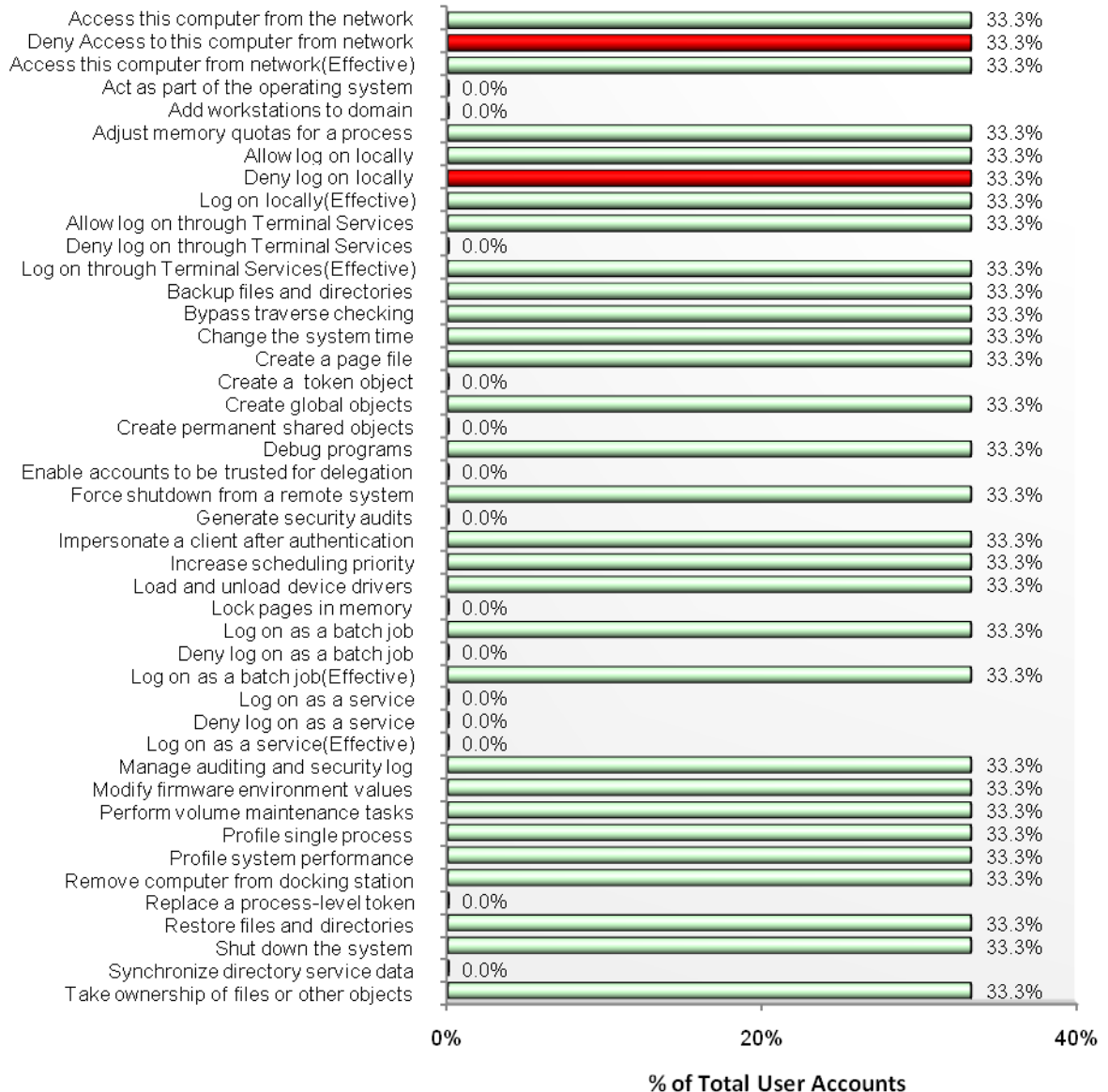
## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
 Analysis Date: 06-Sep-2010

CONFIDENTIAL

### Comparisons Against Industry Average and Leading Practice (Cont.)

#### Summary of Rights



This graph compares against the industry average using the following criteria:  
 Country = <All>; Industry Type = <All>; Machine Size (Nbr of Accounts) = Very Small  
■ Better than the industry average; ■ Worse than the industry average

This summary report presents the number of user accounts, with the listed rights, as a percentage of the total number of accounts defined to your system. For more details, refer to the [Rights Assigned to Users](#) sections in the main body of the report.

The graph is sorted in alphabetical sequence.

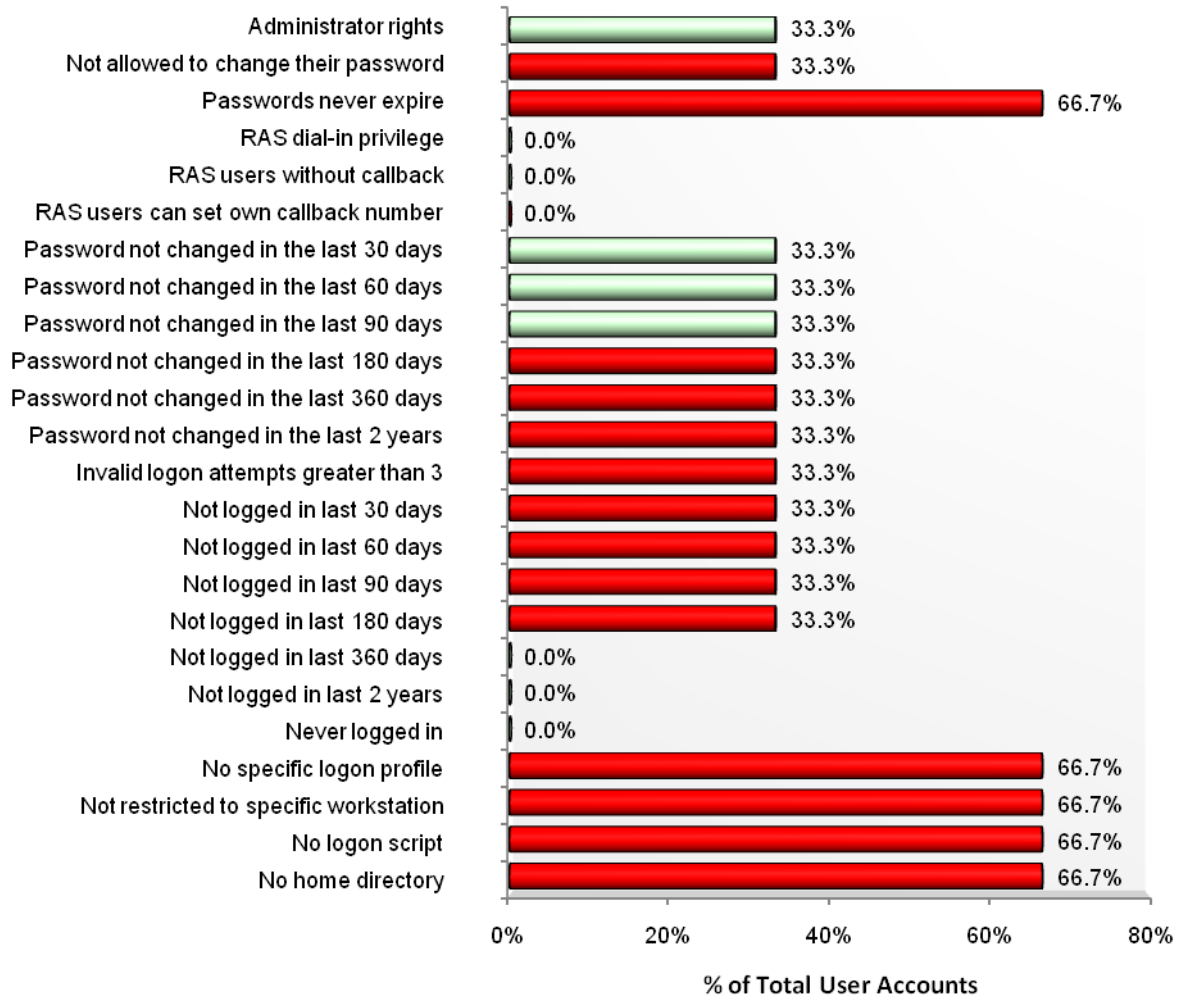
## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### Comparisons Against Industry Average and Leading Practice (Cont.)

#### Summary of User Accounts (excluding disabled accounts)



This graph compares against the industry average using the following criteria:  
Country = <All>; Industry Type = <All>; Machine Size (Nbr of Accounts) = Very Small

Green Better than the industry average; Red Worse than the industry average

Total number of user accounts defined to your system: 3

This summary report presents the number of *enabled* accounts (i.e. excluding accounts with a status of disabled or accounts that are locked) with the listed characteristics, as a percentage of the total number of accounts defined to your system. In general, longer bars highlight potential weaknesses in your security measures and should be investigated. For more details, refer to the relevant sections in the main body of the report.

The graph is sorted in order of importance. This is an approximation and should be used as a guide only.

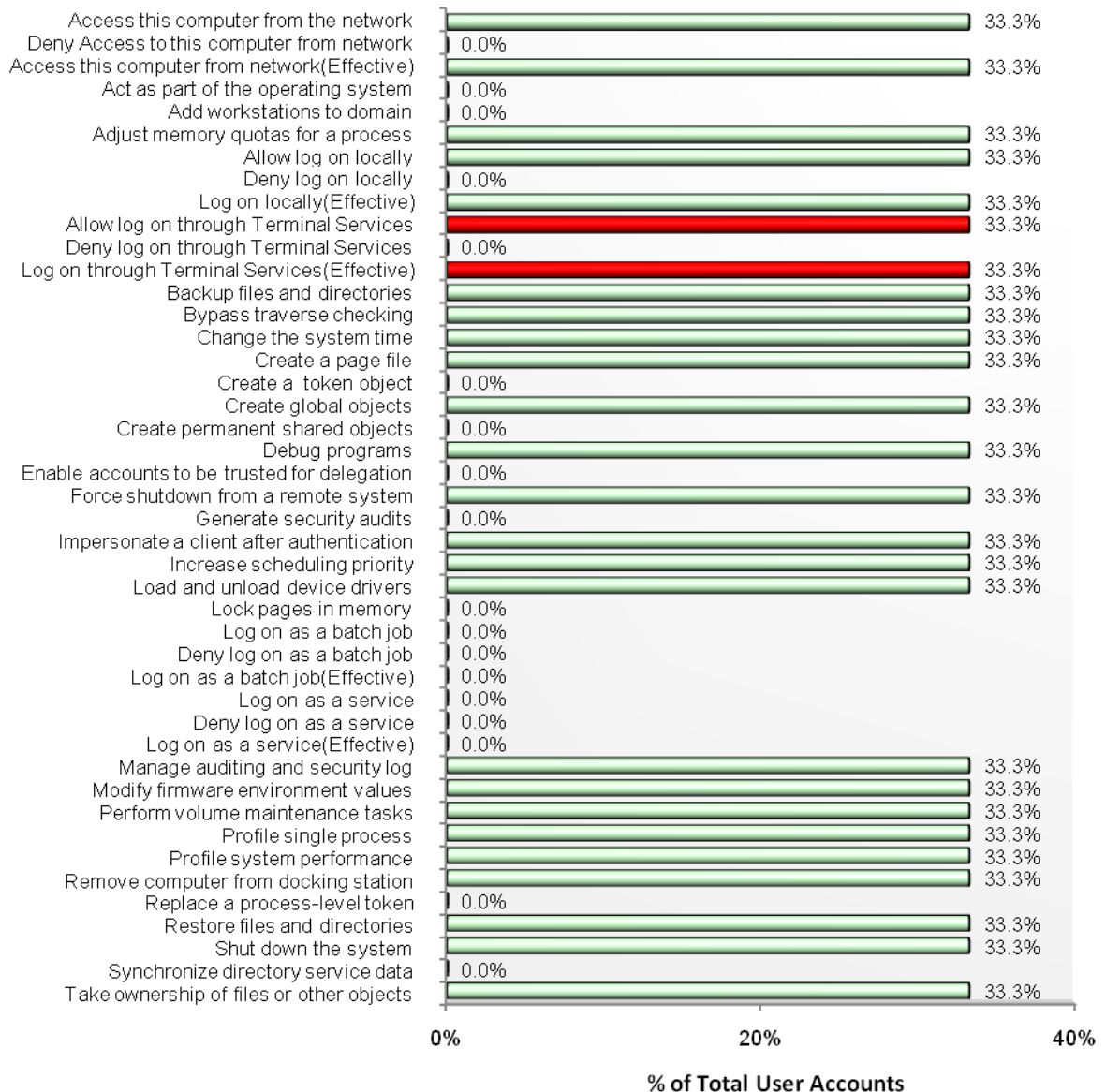
## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### Comparisons Against Industry Average and Leading Practice (Cont.)

#### Summary of Rights (excluding disabled accounts)



This graph compares against the industry average using the following criteria:  
Country = <All>; Industry Type = <All>; Machine Size (Nbr of Accounts) = Very Small  
Better than the industry average; Worse than the industry average

This summary report presents the number of *enabled* accounts (i.e. excluding accounts with a status of disabled or accounts that are locked) with the listed rights, as a percentage of the total number of accounts defined to your system. For more details, refer to the [Rights Assigned to Users](#) sections in the main body of the report.

The graph is sorted in alphabetical sequence.

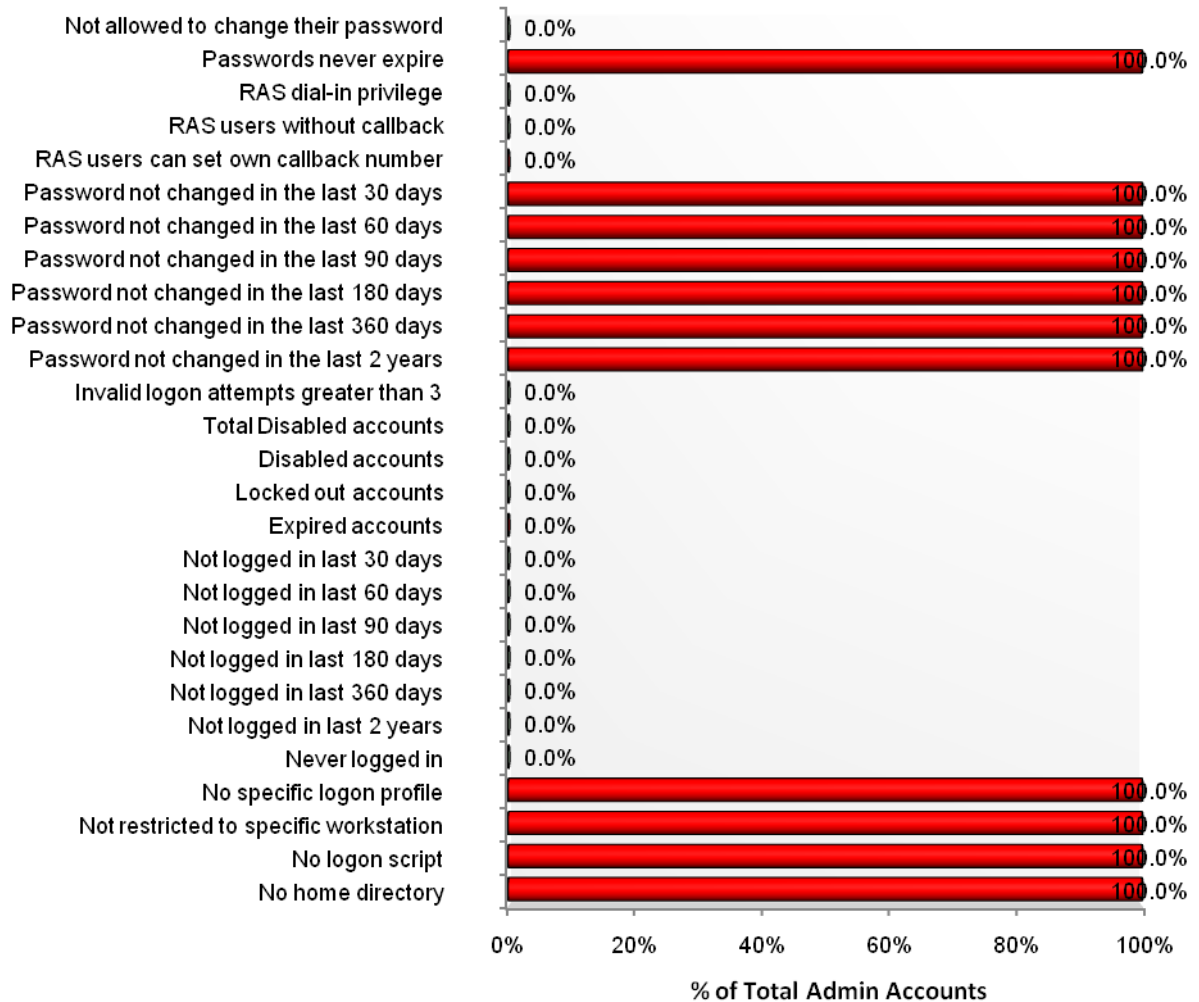
# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## Comparisons Against Industry Average and Leading Practice (Cont.)

### Summary of Administrator Accounts



This graph compares against the industry average using the following criteria:  
Country = <All>; Industry Type = <All>; Machine Size (Nbr of Accounts) = Very Small  
■ Better than the industry average; ■ Worse than the industry average

Total number of user accounts with administrative privileges defined to your system: 1

This summary report presents the number of *administrator* accounts (i.e. accounts that have administrative privileges) with the listed characteristics, as a percentage of the total number of Administrator accounts defined to your system. In general, longer bars highlight potential weaknesses in your security measures and should be investigated. For more details, refer to the relevant sections in the main body of the report.

The graph is sorted in order of importance. This is an approximation and should be used as a guide only.

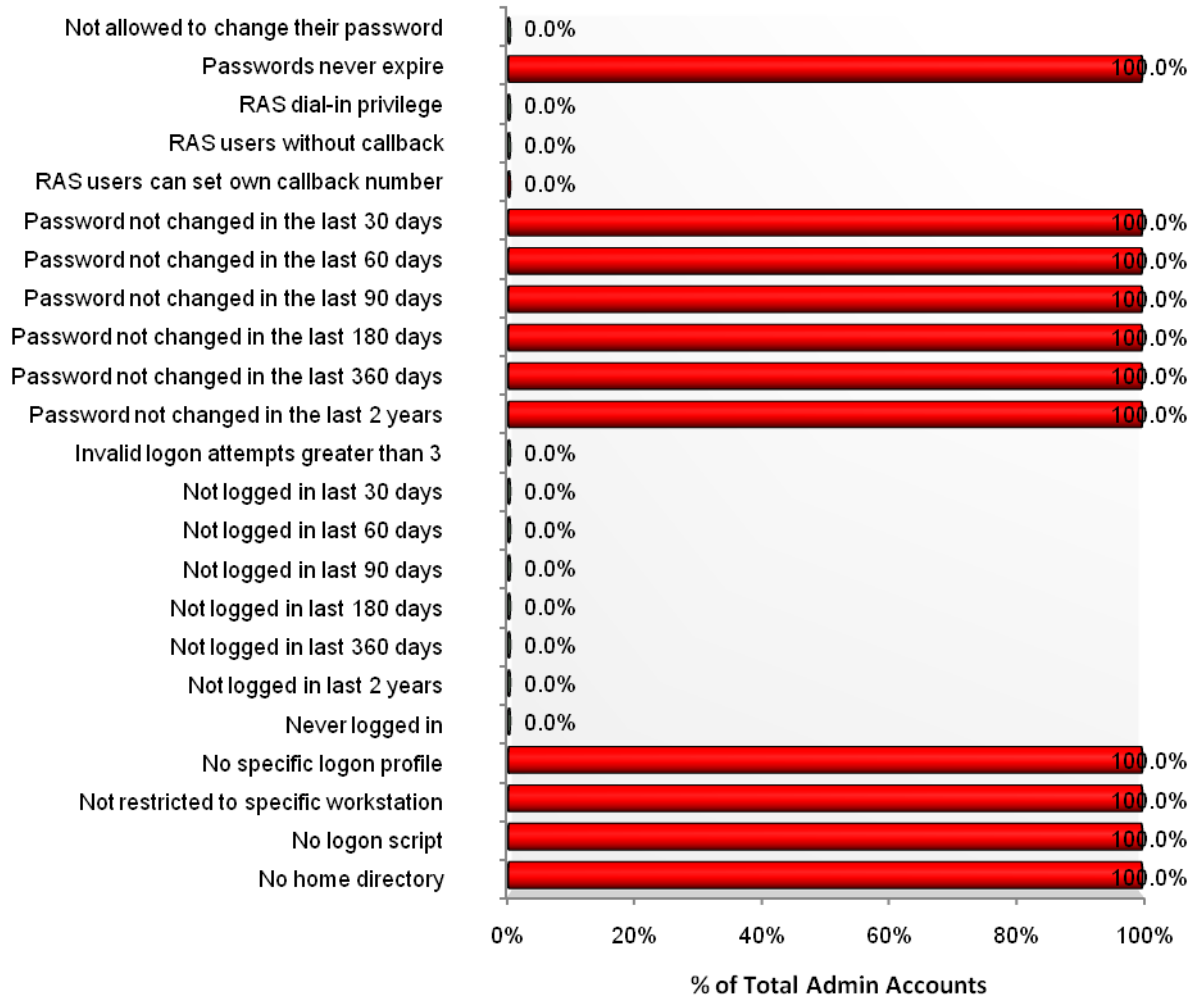
# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## Comparisons Against Industry Average and Leading Practice (Cont.)

### Summary of Administrator Accounts (excluding disabled accounts)



This graph compares against the industry average using the following criteria:  
Country = <All>; Industry Type = <All>; Machine Size (Nbr of Accounts) = Very Small  
■ Better than the industry average; ■ Worse than the industry average

Total number of user accounts with administrative privileges defined to your system: 1

This summary report presents the number of *enabled administrator* accounts (i.e. accounts that have administrative privileges, excluding those accounts with a status of disabled or accounts that are locked) with the listed characteristics, as a percentage of the total number of administrator accounts defined to your system. In general, longer bars highlight potential weaknesses in your security measures and should be investigated. For more details, refer to the relevant sections in the main body of the report.

The graph is sorted in order of importance. This is an approximation and should be used as a guide only.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 1.2 Answers to Common Questions

The following charts are intended to provide quick answers to the most common questions regarding security of a system.

The diagrams highlight the relative numbers of objects with the listed attributes. The total population used to plot each chart is included in brackets ( ) after each chart title. Each section includes a link to more detailed information contained in other sections of this report.

### What is the status of user accounts?

The charts analyse user accounts by their status: active or disabled. An account may be disabled because: its status has been set to disabled; the account has expired; or the account was locked by the system due to excessive password guessing attempts. Note that an account may be both locked and expired, or disabled and expired.

1 out of 3 accounts are disabled on this system.

More information: [Disabled Accounts](#)



### How active are user accounts?

The charts indicate when accounts were last used to logon to the system. Grouped by all accounts and accounts with Administrative privileges. Excludes disabled accounts.

SekChek queried the system's local SAM database to obtain the information.

More information: [Last Logons, 30 Days and Older](#)



## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### How frequently do users change their passwords?

The charts show when user login passwords were last changed. 'Next Logon' means that the password must be changed the next time the account is used to logon to the system. Grouped by all accounts and accounts with Administrative privileges. Excludes disabled accounts.

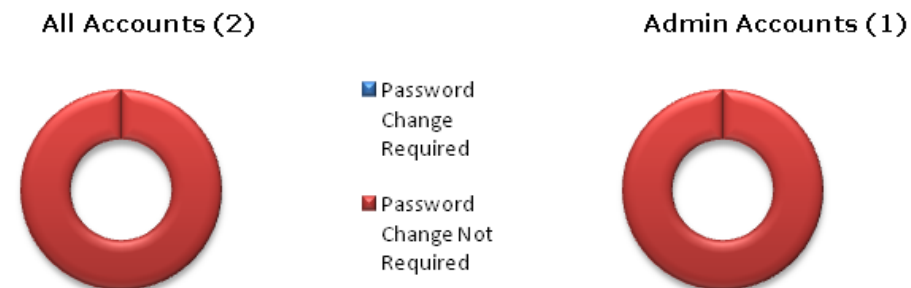
More information: [Passwords, 30 Days and Older](#)



### Are users forced to change their passwords?

The charts show the percentage of accounts with a password that is not required to be changed. Grouped by all accounts and accounts with Administrative privileges. Excludes disabled accounts.

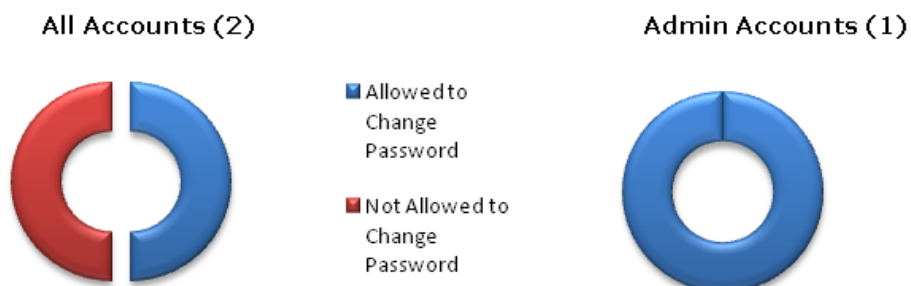
More information: [Passwords that Never Expire](#)



### Are users allowed to change their passwords?

The charts show the percentage of accounts that are not allowed to change their passwords. Grouped by all accounts and accounts with Administrative privileges. Excludes disabled accounts.

More information: [User Accounts not Allowed to Change Password](#)



## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### What privileges are assigned to user accounts?

The charts show the percentage of user accounts with Administrative, User and Guest privileges. These privileges are determined by group memberships. Excludes disabled accounts.

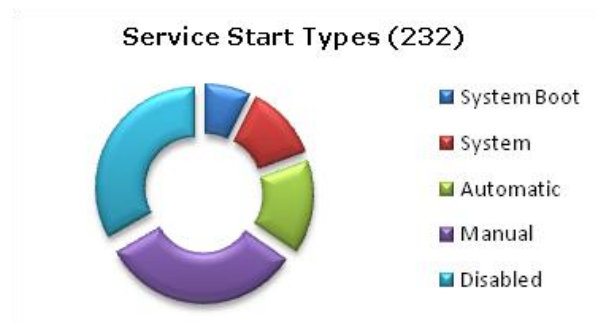
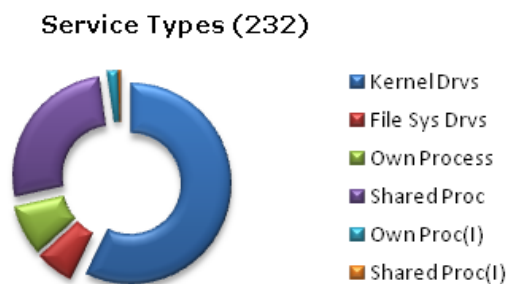
More information: [User Accounts Defined on Your System](#)



### What are the service types and their start types?

These charts summarise the types of services and drivers installed on the system and their start types. The charts include running and stopped services.

More information: [Services and Drivers](#)



## Security Analysis: TESTBED Win2003 Server

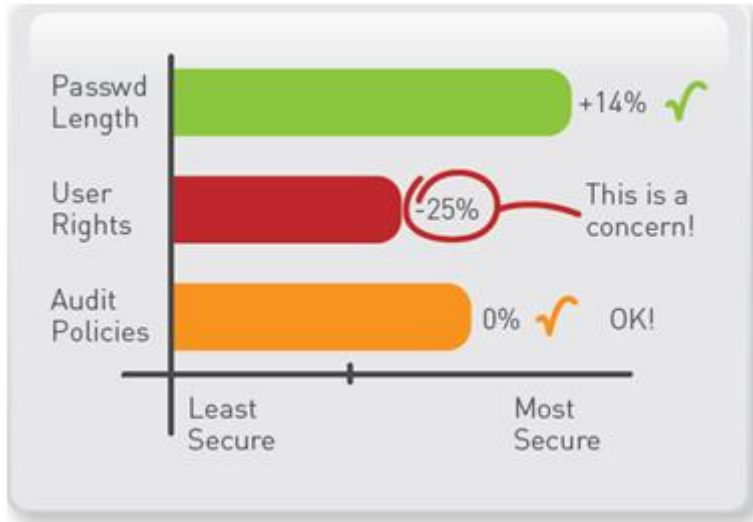
System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### 1.3 Summary of Changes since the Previous Analysis

Need to quickly highlight changes in security controls since your previous review?

SekChek's latest time-comparison graphs are just the solution!



*Note: The above graph is provided for illustrative purposes only.*

A collection of easy-to-read reports in a very familiar format provides you with visual indicators of:

- Whether security has improved, weakened, or remained about the same since your previous analysis
- The effectiveness of your measures to strengthen controls
- Whether risk is increasing or decreasing
- The degree of change, both positive and negative

The applications are endless. Some of the practical benefits are:

- Time savings. Reduced time spent poring over volumes of unconnected information
- Objectivity. The results are guaranteed to be the same regardless of who performs the review
- Compliance with legislation. Easier monitoring for compliance with statutory requirements imposed by SOX, HIPAA and other legislative changes relating to corporate governance
- More powerful justifications. The ability to present more convincing arguments to senior, non-technical management who do not have the time, or the inclination, to understand masses of technical detail

Interested?

Contact us at [inbox@sekchek.com](mailto:inbox@sekchek.com) to find out how to get started!

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 2. System Accounts Policy

This report lists the System Account Policy defaults defined for your system and compares them with Leading Practice.

Domain /Work Group	OLYMPUS
Machine Controlling Domain (PDC)	\\ZEUS
Name of Computer Being Analysed	PROMETHEUS

Policy Items	Current Value	Leading Practice
Minimum Password Length	7	8 or greater
Minimum Password Change Interval in Days	1	0
Maximum Password Change Interval in Days	30	30 to 60
Password History Length	24	15 or greater
Forced Logoff	-1	0
Lockout Duration	0	0
Lockout Threshold	5	3
Lockout Observation Period in Minutes	30	1440
Password Complexity Requirements	Enabled	Enabled
Store Passwords with Reversible Encryption	Disabled	Disabled

### Notes

**Leading Practice** is the standard adopted by the top 10 to 20 percent of organisations.

#### **Domain Name/Work Group**

The Domain Name/Work Group is the name of the Domain or Work Group to which the computer being analysed belongs.

A domain is a collection of computers defined by the administrator of a Microsoft Windows Server network that share a common account database and security policy. A domain provides access to the centralised user accounts and group accounts maintained by the domain administrator. Each domain has a unique name.

A workgroup is a collection of computers that are grouped for browsing purposes and sharing of resources. Each workgroup is identified by a unique name. A workgroup is not a domain and does not have centralised user accounts or a common security policy. Each computer in the workgroup maintains its own set of accounts, groups and security policy.

*If networking is not installed the Domain Name/Work Group will be "N/A".*

#### **Machine Controlling Domain**

This is the name of the server controlling the domain. This is the Primary Domain Controller or PDC.

*When analysing servers or workstations, which are not members of a Domain, the Machine Controlling Domain will be "NONE".*

The Primary Domain Controller (PDC) is the computer running Microsoft Windows Server that authenticates domain logons and maintains the security database for a domain. The PDC tracks changes made to accounts, groups, policy and trust relationships in a domain. It is the only computer to receive these changes directly. A domain has only one PDC.

A member server is a computer that runs Microsoft Windows Server but is not a Primary Domain Controller (PDC) or Backup Domain Controller (BDC) of a Windows domain. Member servers do not receive copies of the domain security database. Also called a stand-alone server.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

### ***Functions of Accounts Policy Values and Potential Exposures***

Policy values set the defaults for all accounts in a domain or for the server / workstation.

Note that some of these values can be overridden at individual account level. For example: Maximum Password Change Interval.

Appropriate policy values do not necessarily mean that security at account level is similarly appropriate. You should consult other sections of this report to confirm that security settings in individual user accounts do not override and negate your intended policy settings.

#### **Minimum Password Length**

Defines the minimum number of characters a password can contain. If it is zero then blank passwords are allowed. Allowing blank passwords is a *very high security risk*, as it could allow any person in possession of a valid User ID (Account Name) to gain access to your system.

*The Leading Practice value is 8 or greater.*

#### **Minimum Password Change Interval in Days**

The *minimum* number of days that must elapse between password changes. The value can be between 0 and 999 days. A value of '0' allows a user to change her password *immediately* if she suspects it is known by someone else.

However, this setting can increase the risk of passwords remaining the same despite system-enforced changes. This is because a user could change her password several times in quick succession until it is set back to the original value. Setting the [Password History Length](#) to a sufficiently large value can reduce this risk.

*The Leading Practice value is 0 (no restrictions). If this control is used, the value cannot exceed the Maximum Password Change Interval.*

#### **Maximum Password Change Interval in Days**

The period of time a password can be used before the system forces the user to change it. The value can be between 1 and 999 days.

*A value of -1 means that passwords never expire. Passwords that never expire are a security risk as they can be compromised over time.*

Note that it is possible to override this value in individual user accounts via the **Password Never Expires** or **User Cannot Change Password** parameters. Consult the [Passwords that Never Expire](#) and the [Users not Allowed to Change Passwords](#) sections in this report.

It is good practice to set the **User Must Change Password At Next Logon** indicator for new user accounts or when administrators change passwords. This will force the user to change the initial or new password allocated at the first or next logon.

*The Leading Practice value is 30 to 60 days.*

#### **Password History Length**

Determines whether old passwords can be reused. It is the number of new passwords that must be used by a user account before an old password can be reused. For this to be effective, immediate changes should not be allowed under [Minimum Password Change Interval](#).

*The Leading Practice value is 15 or greater.*

#### **Forced Logoff**

Specifies the number of seconds after which the system forcibly disconnects users when their valid logon hours expire.

A value of 0 indicates that users will be forcibly disconnected from servers on the domain immediately their valid logon hours are exceeded. A value of -1 prevents users from making *new* connections after their valid logon hours are exceeded, but does not forcibly disconnect those that are already logged on. Valid logon hours are defined per user account.

This option enhances security by ensuring that users are disconnected if they exceed their valid logon hours or do not log off when leaving work. However, it could be disruptive to users who have to work after hours and could compromise data integrity etc.

*This option should be used at the discretion of Management.*

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

### Lockout Threshold, Lockout Duration and Observation Period

**Lockout Threshold** indicates the number of failed logon attempts for user accounts before accounts are locked out. The value can be 1 to 999 failed attempts. A value of 0 will allow an unlimited number of failed logon attempts.

**Lockout Duration** indicates the amount of time an account will remain locked out when the **Lockout Threshold** is exceeded. The value can be 1 to 99999 minutes; a value of 0 (forever) indicates that the account cannot log on until an administrator unlocks it.

**Observation Period.** Specifies the period within which invalid logon attempts are monitored. I.e. if the number of failed logon attempts defined in **Lockout Threshold** is reached within the number of minutes defined for **Observation Period** the account is locked out for the period specified under **Lockout Duration**. The value for **Observation Period** can be 1 to 99999 minutes

Allowing an excessive or unlimited number of invalid logon attempts can compromise security and allow intruders to log on to your system.

Setting the **Lockout Duration** to 0 (forever) will help ensure that administrators are alerted of potential intruder attacks as only they can unlock accounts.

Setting **Lockout Duration** to a small amount (e.g. 5 minutes) will undermine the effectiveness of the **Lockout Threshold** and administrators might not be alerted to potential intruder attacks.

If the value for **Observation Period** is too small (e.g. 1 minute) it will increase the risk of intruders gaining access to your system via repeated password guessing attempts. If the value is too high it may inconvenience *genuine* users by locking out their accounts when they enter incorrect passwords accidentally.

*The Leading Practice values are:*

- *Lockout Threshold = 3*
- *Lockout Duration = 0 (Forever)*
- *Observation Period = 1440 minutes (24 hours)*

### Password Complexity Requirements

In order to meet the password complexity requirement, passwords must contain characters from at least 3 of the following 4 classes:

- *English Upper Case Letters (A through Z)*
- *English Lower Case Letters (a through z)*
- *Westernised Arabic Numerals (0 through 9)*
- *Non-alphanumeric characters (e.g.: !, #, \$, %)*

Note that complexity requirements are enforced when passwords are changed or created.

This analysis was introduced in SekChek V5.0.3 / Windows 2003.

*The Leading Practice value is 'Enabled'.*

### Store Passwords with Reversible Encryption

Determines whether Windows will store passwords using reversible encryption. This analysis was introduced in SekChek V5.0.3 / Windows 2003.

This policy setting provides support for applications, which use protocols that require knowledge of the user password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing clear-text versions of the passwords. For this reason, this policy should not be enabled unless application requirements outweigh the need to protect password information.

*The Leading Practice value is 'Disabled'.*

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### 3. Audit Policy Settings

Security auditing features are **ENABLED** on the computer or domain being analysed.

Audit Policy	Audited Events
Audit Account Logon Events	Success & Failure
Audit Account Management	Success
Audit Directory Service Access	Success
Audit Logon Events	Success & Failure
Audit Object Access	Success & Failure
Audit Policy Change	Success & Failure
Audit Privilege Use	Success & Failure
Audit Process Tracking	Success & Failure
Audit System Events	Success & Failure

#### **Audit Features**

The auditing features can be used to record details of user and other activities in audit logs. This information enhances security by providing you with a powerful detective control and a historical analysis tool. The audit logs can be viewed via *Event Viewer*.

#### **Explanation of Audit Policy Settings**

##### **Account Logon Events**

These events provide tracking information for activities such as logons of service accounts and the authentication of service accounts.

##### **Account Management Events**

Logs an event when, for example:

- A user account or group is created, changed, or deleted;
- A user account is renamed, disabled, or enabled; or
- A password is set or changed.

##### **Directory Service Access Events**

These events provide tracking information for activities in the Active Directory (e.g. changing an object's properties and settings).

##### **Logon Events**

Logs an event when, for example, a user logs on, logs off, or connects to the network.

##### **Object Access Events**

Logs an event when, for example, a user:

- Accesses a directory or a file that is flagged for auditing; or
- A user sends a print job to a printer that is flagged for auditing.

##### **Policy Change Events**

Logs an event when, for example, a change is made to the User Rights, Audit, or Trust Relationship policies.

##### **Privilege Use Events**

Logs an event when, for example, a user exercises a user right (except for those rights related to logon and logoff).

##### **Process Tracking Events**

These events provide detailed tracking information for events such as program activation, some forms of handle duplication, indirect object accesses, and process exit.

##### **System Events**

Logs an event when, for example:

- A user restarts or shuts down the computer; or
- An event that affects the system security or security log occurs.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

### ***Audited Events***

Determines whether audit records are logged for successful events, failed events, or both.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 4. Registry Key Values

Category	Description/Key	Value
Customer-Selected	HKEY_CLASSES_ROOT\MIME\Database\Codepage\1200 - BodyCharset	unicode
Customer-Selected	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor - AutoRun	HKEY_USERS\DEFAULT\Environment - TEMP=#ERROR#
Event Log	Filename for application log	%SystemRoot%\system32\config\AppEvent.Evt
Event Log	Filename for security log	%SystemRoot%\System32\config\SecEvent.Evt
Event Log	Filename for system log	%SystemRoot%\system32\config\SysEvent.Evt
Event Log	Maximum size for application log (in bytes)	16777216
Event Log	Maximum size for security log (in bytes)	16777216
Event Log	Maximum size for system log (in bytes)	16777216
Event Log	Restrict guest access to application log	1
Event Log	Restrict guest access to security log	1
Event Log	Restrict guest access to system log	1
Event Log	Retention method for application log in seconds (-1 = Do not overwrite events, clear manually; 0 = Overwrite as needed)	0
Event Log	Retention method for security log in seconds (-1 = Do not overwrite events, clear manually; 0 = Overwrite as needed)	0
Event Log	Retention method for system log in seconds (-1 = Do not overwrite events, clear manually; 0 = Overwrite as needed)	0
Event Log	Sources for application log	Registry key not found
Event Log	Sources for security log	SpoolerSecurity Account ManagerSC ManagerNetDDE ObjectLSADSSecurity
Event Log	Sources for system log	Registry key not found
Hardware	Component information	
Hardware	CPU feature set	80831
Hardware	CPU identifier	x86 Family 6 Model 7 Stepping 10
Hardware	CPU speed	2929
Hardware	CPU update status	1
Hardware	CPU vendor identifier	GenuineIntel
Hardware	System Bios date	02/22/06
Hardware	System Bios version	A M I - 2000622BIOS Date: 02/22/06 20:54:49 Ver: 08.00.02BIOS Date: 02/22/06 20:54:49 Ver: 08.00.02
Hardware	System identifier	AT/AT COMPATIBLE
Hardware	Video Bios date	Registry key not found
NTFS File System	Allow extended characters in 8.3 file names	Registry key not found
NTFS File System	Do not create 8.3 file names for long file names	0
NTFS File System	Do not update last file access time	Registry key not found
Remote Access	Allow remote TCP/IP clients to request a predetermined IP address	0

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Category	Description/Key	Value
Remote Access	Allow TCP/IP clients to access the entire network	1
Remote Access	Auditing enabled	Registry key not found
Remote Access	Autodisconnect (Minutes)	Registry key not found
Remote Access	Callback time (Seconds)	Registry key not found
Remote Access	End IP address for remote TCP/IP clients	Registry key not found
Remote Access	Force encrypted data	Registry key not found
Remote Access	Force encrypted password (0 = any/clear text, 1 = encrypted, 2 = MS-CHAP authentication)	Registry key not found
Remote Access	Maximum authentication retries	Registry key not found
Remote Access	NetBios gateway enabled	Registry key not found
Remote Access	Observation period (Minutes)	Registry key not found
Remote Access	Start IP address for remote TCP/IP clients	Registry key not found
Remote Access	Use DHCP to assign remote TCP/IP client addresses	1
Security	Allow server operators to schedule tasks (Domain Controllers only)	Registry key not found
Security	Allow system to be shutdown without having to log on	0
Security	Audit access to internal system objects	0
Security	Audit use of all user rights including Backup and Restore	
Security	AutoDisconnect: Allow sessions to be disconnected when they are idle	1
Security	AutoDisconnect: Amount of idle time (in minutes) required before disconnecting session	15
Security	Automated logon - default domain	OLYMPUS
Security	Automated logon - default password	Registry key not found
Security	Automated logon - default user account	administrator
Security	Automated logon (1 = enabled)	0
Security	Automatically detect slow network connections	Registry key not found
Security	Choose profile default operation. 1 = Download Profile, 0 = Use Local Profile	Registry key not found
Security	Clear virtual memory pagefile when system shuts down	0
Security	Create hidden drive shares (server)	Registry key not found
Security	Create hidden drive shares (workstation)	Registry key not found
Security	Delete cached copies of roaming profiles	Registry key not found
Security	Digitally sign client-side communication always	Registry key not found
Security	Digitally sign client-side communication when possible	Registry key not found
Security	Digitally sign server-side communication always	0
Security	Digitally sign server-side communication when possible	0

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Category	Description/Key	Value
Security	Disable browse thread on this computer for printers	Registry key not found
Security	Disable password change	0
Security	Disallow enumeration of account names and shares by anonymous users	0
Security	Display policy remote update Verbose	Registry key not found
Security	Do not display last username in logon screen	Registry key not found
Security	Load balancing for policy remote update	Registry key not found
Security	Logon legal notice caption	
Security	Logon legal notice text	
Security	Logon prompt text	Registry key not found
Security	Number of previous logons to cache in case Domain Controller not available	10
Security	Path for manual update for policy remote update	Registry key not found
Security	Power down after shutdown	0
Security	Prevent users from installing print drivers	Registry key not found
Security	Restrict CD ROM access to locally logged on user only	0
Security	Restrict Floppy access to locally logged on user only	0
Security	Restrict management of shared resources such as com1	1
Security	Scheduler priority	0
Security	Secure Channel: Digitally encrypt or sign secure channel data always	1
Security	Secure Channel: Digitally encrypt secure channel data when possible	1
Security	Secure Channel: Digitally sign secure channel data when possible	1
Security	Secure Channel: Scripts	Registry key not found
Security	Secure Channel: Update	no
Security	Send downlevel LanMan compatible password	2
Security	Send unencrypted password in order to connect to 3rd Party SMB servers	Registry key not found
Security	Shutdown system immediately if unable to log security audits	0
Security	Slow network connection timeout (Milliseconds)	Registry key not found
Security	Slow network default profile operation. 1 = Download Profile, 0 = Use Local Profile	Registry key not found
Security	Timeout for dialog boxes when logging on (Seconds)	Registry key not found
Security	Update mode for policy remote update. 1 = Automatic, 2 = Manual	1
Security	Wait for the logon scripts to complete before starting the users's shell.	Registry key not found
Security, Current User	Cannot display Entire Network in Network Neighborhood	Registry key not found

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
 Analysis Date: 06-Sep-2010

CONFIDENTIAL

Category	Description/Key	Value
Security, Current User	Cannot display workgroup contents in Network Neighborhood	Registry key not found
Security, Current User	Custom Message for Profile quota	Registry key not found
Security, Current User	Custom shell. This is the Shell name (eg: explorer.exe)	Registry key not found
Security, Current User	Deny access to display icon	Registry key not found
Security, Current User	Disable Change Password	Registry key not found
Security, Current User	Disable Lock Workstation	Registry key not found
Security, Current User	Disable Registry editing tools	Registry key not found
Security, Current User	Disable Task Manager	Registry key not found
Security, Current User	Don't save settings at exit	Registry key not found
Security, Current User	Exclude directories in roaming profile	Registry key not found
Security, Current User	Hide all items on desktop	Registry key not found
Security, Current User	Hide Appearance tab from Display	Registry key not found
Security, Current User	Hide Background tab from Display	Registry key not found
Security, Current User	Hide Screen Saver tab	Registry key not found
Security, Current User	Hide Settings tab	Registry key not found
Security, Current User	Include registry in file list of profile quota	Registry key not found
Security, Current User	Limit profile size	Registry key not found
Security, Current User	Maximum Profile size (KB)	Registry key not found
Security, Current User	Minutes between warning user of profile timeout	Registry key not found
Security, Current User	Notify user when profile storage space is exceeded	Registry key not found
Security, Current User	Parse Autoexec.bat. When enabled, 1 environment variables declared in autoexec.bat are included in the users environment	
Security, Current User	Remove Shut Down command from Start menu	Registry key not found
Security, Current User	Wait for the logon scripts to complete before starting the users's shell.	Registry key not found
Synchronisation	BDC back off period in seconds	Registry key not found
Synchronisation	Maximum number of simultaneous pulses from PDC to BDCs	Registry key not found
Synchronisation	Maximum pulse frequency in seconds	Registry key not found
Synchronisation	Number of seconds the PDC waits for a BDC to complete partial replication	Registry key not found
Synchronisation	Number of seconds the PDC waits for a response from a BDC	Registry key not found
Synchronisation	Pulse frequency in seconds	Registry key not found
Synchronisation	Size and frequency of data transferred on each call from a BDC to the PDC	Registry key not found
System	Install date	02-Apr-2004
System	Product Id	69713-640-3988347-45227
Time Zone	Active time bias	-120
Time Zone	Name	South Africa Standard Time
Time Zone	Time bias	-120

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Category	Description/Key	Value
Windows Explorer	Machine Common Programs	%ALLUSERSPROFILE%\Start Menu\Programs
Windows Explorer	Machine Custom shared desktop icons	%ALLUSERSPROFILE%\Desktop
Windows Explorer	Machine Custom shared Start menu	%ALLUSERSPROFILE%\Start Menu
Windows Explorer	Machine Custom shared Startup folder	%ALLUSERSPROFILE%\Start Menu\Programs\Startup
Windows Explorer, Current User	Custom desktop icons.	%USERPROFILE%\Desktop
Windows Explorer, Current User	Custom Network Neighborhood	%USERPROFILE%\NetHood
Windows Explorer, Current User	Custom Programs folder	%USERPROFILE%\Start Menu\Programs
Windows Explorer, Current User	CustomFolders displayed in Start menu	%USERPROFILE%\Start Menu
Windows Explorer, Current User	CustomFolders displayed in Startup folder	%USERPROFILE%\Start Menu\Programs\Startup
Windows Explorer, Current User	Disable context menus for the taskbar	Registry key not found
Windows Explorer, Current User	Disable Explorer's default context menu	Registry key not found
Windows Explorer, Current User	Disable link file tracking	Registry key not found
Windows Explorer, Current User	Disable Logoff	Registry key not found
Windows Explorer, Current User	Hide drives in My Computer	Registry key not found
Windows Explorer, Current User	Hide Network Neighborhood	Registry key not found
Windows Explorer, Current User	Hide Start menu subfolders	Registry key not found
Windows Explorer, Current User	Only use approved shell extensions	Registry key not found
Windows Explorer, Current User	Remove common program groups from Start menu	Registry key not found
Windows Explorer, Current User	Remove File menu from Explorer	Registry key not found
Windows Explorer, Current User	Remove Find command from Start menu	Registry key not found
Windows Explorer, Current User	Remove folders from Settings on Start menu	Registry key not found
Windows Explorer, Current User	Remove Run command from Start menu	Registry key not found
Windows Explorer, Current User	Remove Taskbar from Settings on Start menu	Registry key not found
Windows Explorer, Current User	Remove the "Map Network Drive" and "Disconnect Network Drive" options	Registry key not found
Windows Explorer, Current User	Remove Tools, GoTo menu from Explorer	Registry key not found
Windows Explorer, Current User	Remove View Options menu from Explorer	Registry key not found
Windows Explorer, Current User	Run only allowed Windows applications	Registry key not found

**NOTE:** The above list of registry values is provided for information purposes and as an aid in the evaluation of security and other settings for the system being analysed.

**Registry key not found** = the registry key was not defined on the system. In many cases, a default setting is adopted for the feature.

For many registry keys a value of '0' means that the feature is not enabled and a value of '1' or greater means enabled.

### Implications

The correct settings of certain registry keys will enhance security, auditing and management on the system.

For example, having appropriate values for "remote access" will decrease the risk of intruders gaining illegal access to the system.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

### Risk Rating

---

Low to high. (Dependant on the registry setting being considered).

### Recommended Action

---

Ensure that registry values are set to appropriate values where applicable.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 5. User Accounts Defined On Your System

### Section Summary

There are a total of 3 user accounts defined on your system:

- 33.3% (1) of user accounts have Administrator privileges
- 66.7% (2) of user accounts have Guest privileges
- 0.0% (0) of user accounts have User privileges
- Status of the Administrator account (uid 500): Not renamed, not disabled.
- Status of the Guest account (uid 501): Renamed, not disabled.

### Section Detail

Account Name	Owner	Privilege	Member of Group	Type
Administrator		Administrator	Administrators	Local
			None	Global
SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	Guest	HelpServicesGroup	Local
			None	Global
Visitor		Guest	Guests	Local
			None	Global

**NOTE:** The above is a list of user accounts that have been registered on the system/domain. It does not include user or group accounts, from other domains or servers that are members of this server's local groups.

For those "external" accounts, consult the report section titled: [Local Groups and their Members](#).

### Implications

If users belong to groups with permissions and rights greater than they need, they will have access to resources and system functions not in line with their job functions.

The Guest privilege is equivalent to normal users privilege. Use Guest privileges to exclude temporary or occasional users from the Users group.

*The Administrator privilege is the most powerful privilege on the system and can perform all actions on the server or domain. Users with Administrator privilege have full control over the server and/or domain resources.*

Members of groups such as *Print Operators, Account Operators, Server Operators and Backup Operators* also acquire special privileges. Consult the report section titled: [Local Groups and their Members](#), for a more detailed analysis.

### Risk Rating

Medium to high (dependent on users' job functions and the number of accounts with special privileges).

### Recommended Action

Users' privileges and group membership should be checked to ensure they are not granted unnecessary privileges or rights.

Most users should be assigned to the built in global group *Domain Users* and the built in local group *Users*.

The number of accounts with Administrator privilege should be kept to a minimum. These accounts should only be used for administrative functions. Users with administrative privileges should use a separate account for normal day-to-day use.

You should consider renaming the "built in" "*Administrator*" account to a less obvious name to lessen the possibility of hackers guessing the password, as they would have to guess the account name also. This account can never be locked out due to failed logon attempts. The account cannot be disabled or deleted.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)

Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

You should consider renaming the “built in” “*Guest*” account to a less obvious name. Hackers trying to obtain illegal access often target this account. This account cannot be deleted.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 6. Local Groups and their Members

### Section Summary

There are a total of 13 local groups, containing the following 9 members, defined on your system:

- 33.3% (3) of these members are external accounts or groups
- 8 local groups do not have any members

### Section Detail

Group Name	Group Description	Member (Domain\Account)	Member Type
Administrators	Administrators have complete and unrestricted access to the computer/domain	OLYMPUS\Domain Admins	Group
		PROMETHEUS\Administrator	User
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files		
Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted	OLYMPUS\Visitorzz	User
		PROMETHEUS\Visitor	User
HelpServicesGroup	Group for the Help and Support Center	PROMETHEUS\SUPPORT_388945a0	User
Network Configuration Operators	Members in this group can have some administrative privileges to manage configuration of networking features		
Performance Log Users	Members of this group have remote access to schedule logging of performance counters on this computer	NT AUTHORITY\NETWORK SERVICE	WellKnownGroup
Performance Monitor Users	Members of this group have remote access to monitor this computer		
Power Users	Power Users possess most administrative powers with some restrictions. Thus, Power Users can run legacy applications in addition to certified applications		
Print Operators	Members can administer domain printers		
Remote Desktop Users	Members in this group are granted the right to logon remotely		
Replicator	Supports file replication in a domain		
TelnetClients	Members of this group have access to Telnet Server on this system.		
Users	Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications	NT AUTHORITY\Authenticated Users	WellKnownGroup
		NT AUTHORITY\INTERACTIVE	WellKnownGroup

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Group Name	Group Description	Member (Domain\Account)	Member Type
		OLYMPUS\Domain Users	Group

**NOTE:** When **Account Type = Unknown**, it means that the account or group is a member of the local group but that the server/domain where the account or group is registered could not be reached to obtain the account information. The local groups showing these accounts as members should be checked to establish the origin and details of these accounts.

When a server/domain cannot be reached for account information, the server/domain is either not available through the network or the server/domain no longer exists in the domain.

### Local Group

For Windows Servers which are Primary or Backup Domain Controllers, a group that can be granted permissions and rights only for the domain controllers (primary and backup) of its own domain.

**However, a local group can contain user accounts and global groups (not local groups) both from its own domain and from trusted domains.**

Local groups provide a way to group together users with similar access requirements from both inside and outside a domain.

For Windows Workstations and Servers that are not Primary or Backup Domain Controllers, a local group can be granted permissions and rights for the workstation or server only. However, a local group can contain its own user accounts and, if the workstation or server belongs to a domain, user accounts and global groups (not local groups) **both from the domain and trusted domains.**

### Implications

If users or groups belong to local groups with permissions and rights greater than they need, they will have access to unnecessary resources and system functions via the permissions and rights associated with the local groups.

The "built in" local groups with special rights and permissions are:

- "Administrators":
  - √ Members can fully administer the computer/domain and its resources.
- "Account Operators":
  - √ Can create, remove, and modify user accounts that have User or Guest privileges.
  - √ Can create, remove and modify groups.
  - √ Can modify logon restrictions and add workstations to the domain.
  - √ Cannot modify an account that has Administrator privilege, except to change group memberships.
  - √ Cannot change an account's privileges to the Administrator level.
- "Print Operators":
  - √ Can share and stop sharing printer queues.
  - √ Can create, remove, and modify printer queues.
  - √ Can control print jobs and view a list of all resources shared on the server (Including resources available only to Administrators).
- "Server Operators":
  - √ Can start and stop services.
  - √ Can share and stop sharing resources.
  - √ Can read and clear the error log.
  - √ Can close user sessions and the files users have opened.
  - √ Can view a list of all the resources shared on the server (Including resources available only to Administrators).
- "Backup Operators":
  - √ Can bypass file and directory security to backup files and directory.

The "built in" local group, which has normal default user rights and permissions, is the "Users" local group. Another "built in" local group with limited default privileges is "Guests".

"Built in" local groups cannot be deleted. These groups can be copied. The duplicated group(s) *do not* retain the rights and privileges of the copied group(s).

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

New local groups can be created and powerful rights (e.g. "Take Ownership of Files and other Objects") can be assigned to them via the User Rights policy.

You may find other "Account Types" (Account Type in the list above) as members of local groups. These account types can be one of the following: ALIAS or WELLKNOWNGROUP.

ALIAS refers to another group, which is an alias of the group. An example is the "BUILTIN\Administrators" (Administrators local group) being an alias of a local group, which "Can create and manage Webs".

WELLKNOWNGROUP refers to "generic groups" which can be made members of local groups. These "generic groups" are standard groups created by the system. When these "generic groups" are members of local groups, they will acquire the privileges/rights of the local group(s) they are members of. The "generic group" can be one of the following:

<b>Everyone</b>	A group that includes all users, even anonymous users and guests. Membership is controlled by the operating system.
<b>Dialup</b>	A group that implicitly includes all users who are logged on to the system through a dial-up connection. Membership is controlled by the operating system.
<b>Network</b>	A group that implicitly includes all users who are logged on through a network connection. Membership is controlled by the operating system.
<b>Batch</b>	A group that implicitly includes all users who have logged on through a batch queue facility such as task scheduler jobs. Membership is controlled by the operating system.
<b>Interactive</b>	A group that includes all users who have logged on interactively. Membership is controlled by the operating system.
<b>Service</b>	A group that includes all security principals that have logged on as a service. Membership is controlled by the operating system.
<b>Authenticated Users</b>	A group that includes all users whose identities were authenticated when they logged on. Membership is controlled by the operating system.

### Risk Rating

---

Medium to high (dependent on users' job functions).

### Recommended Action

---

Privileges and rights acquired by users via their membership of local groups should be checked to ensure they are consistent with the users' job functions.

Most users or global groups should be assigned to the built in local group "USERS".

Users or groups assigned to privileged local groups should be kept to a minimum and their membership fully justified. As a rule, only individual users and not global groups, should be added to privileged local groups as this affords better control.

Those accounts or groups from other domains, which are members of "privileged" local groups, should be carefully checked and fully justified.

If it can be avoided, users and groups from other domains should not be members of privileged local groups.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 7. Global Groups and their Members (DCs only)

### Section Summary

---

\*\*\*This report section only applies to Domain Controllers. There will be no data for Servers or Workstations.\*\*\*

### Section Detail

---

\*\* No data found \*\*

#### Global Group

For Windows Servers which are Primary or Backup Domain Controllers, a group that can be used in its own domain, member servers, workstations of the domain and trusting domains.

A global group can be granted rights and permissions in the above areas and can be a member of local groups, thus acquiring their rights. However, it can only contain individual user accounts from its own domain. Groups (local or global) cannot be members of global groups. User accounts must belong to at least one global group (their primary group).

Global groups provide a way to group together users with similar access requirements inside the domain. They are available for use both in and out of the domain.

Global groups cannot be created or maintained on Windows Workstations or Servers that are not Primary or Backup Domain Controllers. However, for Windows Workstation or Server computers that participate in a domain, domain global groups can be granted rights and permissions at those workstations or servers, and can be members of local groups at those workstations or servers.

#### Implications

---

If users are assigned to global groups with permissions and rights greater than they need, they will have access to unnecessary system resources and functions via the permissions and rights associated with the global groups.

Global groups can be members of local groups, thus acquiring their rights and granting those rights to users belonging to the global groups.

The "built in" global group with default special rights and permissions is "Domain Admins" (Designated administrators of the domain).

Other, built in, global groups are:

- Domain Guests (All domain guests)
- Domain Users (All domain users)

"Built in" global groups cannot be deleted. They can be copied. The duplicated group(s) *will not* retain the rights and privileges contained in the group(s) copied from.

New global groups can be created and powerful rights (e.g. Take Ownership of Files and other Objects) assigned to them via the User Rights policy.

#### Risk Rating

---

Medium to high (dependent on users' job functions).

#### Recommended Action

---

Privileges and rights assigned to global groups and their membership of privileged local groups should be checked to ensure that they are justified.

Most users should only be assigned to the "built in" global group "Domain Users".

Users assigned to privileged global groups (such as "Domain Admins") should be kept to a minimum and their membership fully justified.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 8. Last Logons, 30 Days and Older

### Section Summary

#### All Accounts

66.7% (2) of user accounts have not logged-on in the last 30 days:

- 66.7% (2) have not logged-on in the last 60 days
- 66.7% (2) have not logged-on in the last 90 days
- 66.7% (2) have not logged-on in the last 180 days
- 33.3% (1) have not logged-on in the last 360 days
- 33.3% (1) have not logged-on in the last 2 years
- 33.3% (1) have never been used, or their last logon date is unknown

#### Excluding Disabled Accounts

33.3% (1) of user accounts have not logged-on in the last 30 days:

- 33.3% (1) have not logged-on in the last 60 days
- 33.3% (1) have not logged-on in the last 90 days
- 33.3% (1) have not logged-on in the last 180 days
- 0.0% (0) have not logged-on in the last 360 days
- 0.0% (0) have not logged-on in the last 2 years
- 0.0% (0) have never been used, or their last logon date is unknown

#### All Administrator Accounts

0.0% (0) of administrator accounts have not logged-on in the last 30 days:

- 0.0% (0) have not logged-on in the last 60 days
- 0.0% (0) have not logged-on in the last 90 days
- 0.0% (0) have not logged-on in the last 180 days
- 0.0% (0) have not logged-on in the last 360 days
- 0.0% (0) have not logged-on in the last 2 years
- 0.0% (0) have never been used, or their last logon date is unknown

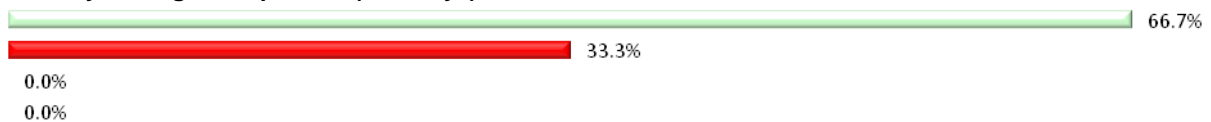
#### Administrator Accounts (Excluding Disabled Accounts)

0.0% (0) of administrator accounts have not logged-on in the last 30 days:

- 0.0% (0) have not logged-on in the last 60 days
- 0.0% (0) have not logged-on in the last 90 days
- 0.0% (0) have not logged-on in the last 180 days
- 0.0% (0) have not logged-on in the last 360 days
- 0.0% (0) have not logged-on in the last 2 years
- 0.0% (0) have never been used, or their last logon date is unknown

The last logon for the builtin Administrator account was 2 days ago.

#### Industry Average Comparison (> 30 days)



*Note. This is an exception report, so only lists accounts that have not logged on in the last 30 days. I.e. if an account logged in 29 days ago (or more recently) it will not be listed in the report section.*

### Section Detail

Last Logon	Account Name	Owner	Privilege	Disabled
	SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	Guest	Yes
15-Jan-2010	Visitor		Guest	

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

### Implications

---

Some of these user accounts may no longer be required. Inactive user accounts are a prime target for intruders. If their passwords are compromised, they can be used with little fear of detection.

A value of *Yes* in the *Account Disabled* column indicates that the account has been disabled by a security administrator, is locked due to excessive failed login attempts, or has expired. See [Disabled Accounts](#) for details.

### Risk Rating

---

Low to Medium.

### Recommended Action

---

The list of accounts should be reviewed and redundant ones should be deleted.

Accounts that will be required later (longer term), should be disabled until required.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 9. Passwords, 30 Days and Older

### Section Summary

#### All Accounts

66.7% (2) of user accounts have not had their passwords changed in the last 30 days:

- 66.7% (2) have not had their passwords changed in the last 60 days
- 66.7% (2) have not had their passwords changed in the last 90 days
- 66.7% (2) have not had their passwords changed in the last 180 days
- 66.7% (2) have not had their passwords changed in the last 360 days
- 66.7% (2) have not had their passwords changed in the last 2 years

33.3% (1) of users must change their password at next logon (see note below).

#### Excluding Disabled Accounts

33.3% (1) of user accounts have not had their passwords changed in the last 30 days:

- 33.3% (1) have not had their passwords changed in the last 60 days
- 33.3% (1) have not had their passwords changed in the last 90 days
- 33.3% (1) have not had their passwords changed in the last 180 days
- 33.3% (1) have not had their passwords changed in the last 360 days
- 33.3% (1) have not had their passwords changed in the last 2 years

33.3% (1) of users must change their password at next logon (see note below).

#### All Administrator Accounts

100.0% (1) of administrator accounts have not had their passwords changed in the last 30 days:

- 100.0% (1) have not had their passwords changed in the last 60 days
- 100.0% (1) have not had their passwords changed in the last 90 days
- 100.0% (1) have not had their passwords changed in the last 180 days
- 100.0% (1) have not had their passwords changed in the last 360 days
- 100.0% (1) have not had their passwords changed in the last 2 years

0.0% (0) of administrator accounts must change their password at next logon (see note below).

#### Administrator Accounts (Excluding Disabled Accounts)

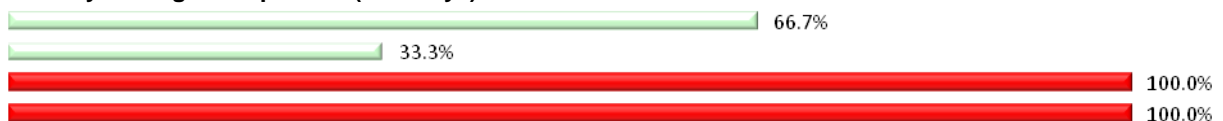
100.0% (1) of administrator accounts have not had their passwords changed in the last 30 days:

- 100.0% (1) have not had their passwords changed in the last 60 days
- 100.0% (1) have not had their passwords changed in the last 90 days
- 100.0% (1) have not had their passwords changed in the last 180 days
- 100.0% (1) have not had their passwords changed in the last 360 days
- 100.0% (1) have not had their passwords changed in the last 2 years

0.0% (0) of administrator accounts must change their password at next logon (see note below).

The password for the builtin Administrator account was last changed 2348 days ago.

#### Industry Average Comparison (> 30 days)



*Note. This is an exception report, so only lists accounts whose passwords have not changed in the last 30 days. I.e. if an account's password was changed 29 days ago (or more recently) it will not be listed in the report section.*

A Password Age of '0' indicates that the user is required to change his password at the next logon. SekChek cannot determine the last password change date because it is not stored by the system.

### Section Detail

Password Age (days)	Account	Owner	Password Expired	Privilege	Disabled
2348	Administrator			Administrator	
2348	SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US		Guest	Yes

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Password Age (days)	Account	Owner	Password Expired	Privilege	Disabled
0	Visitor			Guest	

### Implications

This could indicate that these users are not required to change their passwords on a regular basis or that the accounts are inactive and redundant. A password that is not changed on a frequent basis increases the risk of it being compromised over time.

A value of *Yes* in the *Account Disabled* column indicates that the account has been disabled by a security administrator, is locked due to excessive failed login attempts, or has expired. See [Disabled Accounts](#) for details.

### Risk Rating

Medium. If password controls are weak (e.g. [Password Never Expires](#) set in user accounts) the risk is high.

### Recommended Action

The accounts should be reviewed and deleted if they are no longer required. Otherwise, their password change interval should be brought in line with installation standards.

The [Leading Practice](#) is to force users to change their passwords every 30 to 60 days.

Some service accounts, such as for SMS, normally do not have their passwords changed frequently. For those accounts, the account name and password should be such that they are very difficult to guess.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 10. Passwords that Never Expire

### Section Summary

#### All Accounts

100.0% (3) of users are never required to change their passwords due to security settings in individual user accounts.

#### Excluding Disabled Accounts

66.7% (2) of users are never required to change their passwords due to security settings in individual user accounts.

#### All Administrator Accounts

100.0% (1) of administrator accounts are never required to change their passwords due to security settings in individual user accounts.

#### Administrator Accounts (Excluding Disabled Accounts)

100.0% (1) of administrator accounts are never required to change their passwords due to security settings in individual user accounts.

#### Industry Average Comparison



### Section Detail

Account Name	Owner	Privilege	Disabled
Administrator		Administrator	
SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	Guest	Yes
Visitor		Guest	

### Implications

If users are not required to change their passwords on a frequent basis, their passwords are likely to become known to other employees and potential intruders. The user profile could then be used to gain unauthorised access to systems and data until the real user changes the password to a new one.

The password change interval is set in the [Accounts Policy](#). However, the system default can be overridden via the **Password Never Expires** parameter at user account level.

A value of Yes in the *Account Disabled* column indicates that the account has been disabled by a security administrator, is locked due to excessive failed login attempts, or has expired. See [Disabled Accounts](#) for details.

### Risk Rating

Medium to High.

### Recommended Action

Password change intervals for these user accounts should be brought in-line with the installation standard.

The [Leading Practice](#) for a password change interval is between 30 and 60 days.

You should also check the Accounts Policy to confirm that the **Maximum Password Change Interval** is set to an acceptable value.

Some service accounts, such as for SMS, normally do not have their passwords changed frequently. For those accounts, the account name and password should be such that they are very difficult to guess.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 11. Invalid Logon Attempts Greater than 3

### Section Summary

#### All Accounts

33.3% (1) of user accounts have invalid logon attempts greater than 3.

#### Excluding Disabled Accounts

33.3% (1) of user accounts have invalid logon attempts greater than 3.

#### All Administrator Accounts

0.0% (0) of administrator accounts have invalid logon attempts greater than 3.

#### Administrator Accounts (Excluding Disabled Accounts)

0.0% (0) of administrator accounts have invalid logon attempts greater than 3.

#### Industry Average Comparison



### Section Detail

Invalid Logon Attempts	Account	Owner	Last Logon	Privilege	Disabled
4	Visitor		15-Jan-2010	Guest	

### Implications

Invalid logon attempts indicate the number of unsuccessful attempts at signing on to your system with the listed accounts. The value is reset to '0' after a successful sign-on to the system.

Consistently high values could indicate that an intruder is attempting to guess user passwords to gain access to your system.

The **Lockout Threshold** parameter in the **accounts policy** determines the number of failed logon attempts for user accounts before accounts are locked out.

A value of Yes in the **Account Disabled** column indicates that the account has been disabled by a security administrator, is locked due to excessive failed login attempts, or has expired. See **Disabled Accounts** for details.

### Risk Rating

Low to Medium. (Dependent on the value assigned to the **Lockout Threshold** parameter in the **Accounts Policy**)

### Recommended Action

You should ensure that the **Lockout Threshold** in the Accounts Policy is set to a reasonable value. A value of 3 is the **Leading Practice**.

Ideally, the **Lockout Duration** should be set to 0 (forever) in the Accounts Policy. This ensures that accounts are locked when the lockout threshold is exceeded and can only be unlocked by Administrators.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 12. Users not Allowed to Change Passwords

### Section Summary

#### All Accounts

66.7% (2) of the users are not allowed to change their passwords.

#### Excluding Disabled Accounts

33.3% (1) of the users are not allowed to change their passwords.

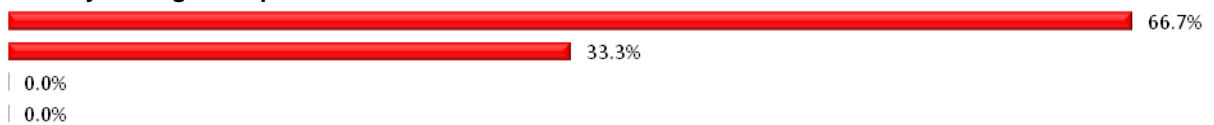
#### All Administrator Accounts

0.0% (0) of administrators are not allowed to change their passwords.

#### Administrator Accounts (Excluding Disabled Accounts)

0.0% (0) of administrators are not allowed to change their passwords.

#### Industry Average Comparison



### Section Detail

Account Name	Owner	Privilege	Disabled
SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	Guest	Yes
Visitor		Guest	

### Implications

If users are not permitted to change their passwords on a frequent basis, their passwords are likely to become known to other employees and potential intruders. The user profile could then be used to gain unauthorised access to systems and data until the password is changed to a new one.

The password change interval is set in the [Accounts Policy](#). However, individual accounts can have the **User Cannot Change Password parameter** set which overrides the policy standard.

A value of *Yes* in the *Account Disabled* column indicates that the account has been disabled by a security administrator, is locked due to excessive failed login attempts, or has expired. See [Disabled Accounts](#) for details.

### Risk Rating

Medium to High.

### Recommended Action

The **User Cannot Change Password** parameter in user accounts should only be set for those accounts where a common sign on is required (The “built in” Guest account is an example of a “common” account). The privileges and group membership of these accounts should be carefully monitored.

Some service accounts, such as for SMS, normally do not have their passwords changed frequently. For those accounts, the account name and password should be such that they are very difficult to guess.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

### 13. Accounts with Expiry Date

#### Section Summary

---

##### All Accounts

0.0% (0) of user accounts are set to expire on a certain date.

##### All Administrator Accounts

0.0% (0) of administrator accounts are set to expire on a certain date.

#### Section Detail

---

\*\* No data found \*\*

#### Implications

---

The **Account Expires** parameter allows you to ensure the account is automatically disabled on the assigned date. When an account expires, a user who is logged on remains logged on but cannot establish new network connections. After logging off, that user cannot log on again unless the expiration date is reset or cleared.

#### Risk Rating

---

Low to Medium.

#### Recommended Action

---

It is good practice to set an expiration date for temporary accounts or accounts assigned to contractors and part-time workers.

For added security and to help ensure that accounts are disabled when no longer used, you could consider setting expiration dates for *all* user accounts. Note however, that this will add to the administrative workload and may inconvenience genuine users when their accounts expire and need to be reset by an administrator.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 14. Disabled Accounts

### Section Summary

#### All Accounts

33.3% (1) of user accounts have been 'disabled' and cannot be used to login to your system:

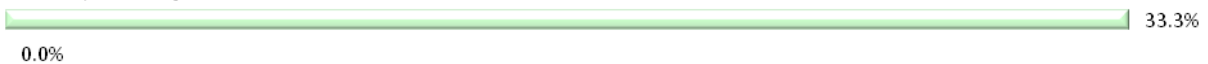
- 0.0% (0) of user accounts are locked
- 33.3% (1) of user accounts are disabled
- 0.0% (0) of user accounts are expired

#### All Administrator Accounts

0.0% (0) of administrator accounts have been 'disabled' and cannot be used to login to your system:

- 0.0% (0) of administrator accounts are locked
- 0.0% (0) of administrator accounts are disabled
- 0.0% (0) of administrator accounts are expired

#### Industry Average Comparison



### Section Detail

Account Name	Owner	Last Logon	Locked	Disabled	Expired	Privilege
SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US			Yes		Guest

### Implications

No security risks. A housekeeping issue only.

Accounts are disabled because they have reached the account expiration date, have been disabled by an administrator, or have been automatically locked by the system due to excessive failed login attempts.

*Note. Accounts can be disabled and also locked or expired. For this reason, the total number of 'disabled' accounts that appears at the top of the Section Summary may be less than the number of accounts listed in the Section Detail.*

### Risk Rating

None.

### Recommended Action

You should determine the reason that these accounts are disabled. If they are inactive and no longer required they should be deleted from the system.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

### 15. Rights and Privileges

The following four subsections provide general recommendations regarding rights, and analyses of rights assigned to Local groups, Global groups, and user accounts:

- [Descriptions & General Recommendations for Rights](#)
- [Rights Assigned to Local Groups](#)
- [Rights Assigned to Global Groups \(PDC/BDC only\)](#)
- [Rights Assigned to Users](#)

#### Implications

---

Rights allow users to perform certain actions on the system, such as the ability to Backup Files & Directories. Rights apply to the system as a whole and are different to permissions, which apply to specific objects.

Rights are assigned to specific User accounts *directly* via the User Rights policy, or *indirectly* via Group memberships.

Note that members of a Local or Global group automatically inherit *all* rights granted to that group. ***This includes Global groups or users from other domains that are members of a Local group.***

If users are given inappropriate rights it can lead to a high security risk.

A value of Yes in the *Account Disabled* column indicates that the account has been disabled by a security administrator, is locked due to excessive failed login attempts, or has expired. See [Disabled Accounts](#) for details.

#### Risk Rating

---

Medium to high depending on the rights granted to groups and users.

#### Recommended Action

---

Rights should be justified according to the person's job function.

In general, rights should be assigned by adding user accounts to one of the built-in groups that already has the needed rights, rather than by administering the User Rights policy.

The recommendations on the following page serve as a guideline only. ***Powerful*** rights should only be granted to users or special accounts (e.g. SMS account) when absolutely necessary. They should also be reviewed on a regular basis.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### 15.1 Descriptions & General Recommendations for Rights

Right	Description	Recommendation
Access Credential Mgr as a trusted caller	Windows Vista or later. This setting is used by Credential Manager during Backup/Restore. Users' saved credentials might be compromised if this privilege is given to other entities.	No accounts should have this privilege, as it is only assigned to Winlogon.
Access this computer from the network	Allows a user to connect to the computer over the network. At domain level this applies to all domain controllers in the domain. On a server or workstation, this applies to that machine only.	Initially granted to Administrators, Everyone and Power Users. Restrict as required.
Act as part of the operating system	Allows a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this right.	Grant to no one.
Add workstations to domain	Allows a user to add workstations to the domain. Adding a workstation to a domain enables the workstation to recognize the domain's user and global groups accounts. By default, members of a domain's Administrators and Account Operators groups have the right to add a workstation to a domain. This right cannot be taken away. They can also grant this right to other users.	Grant to Administrators and Account Operators.
Adjust memory quotas for a process	Allows the quota assigned to a process to be increased.	Grant to no one.
Allow log on locally	Allows a user to log on at the computer from the computer's keyboard. At domain level this applies to all domain controllers in the domain. On a server or workstation, this applies to that machine only.	For servers and domain controllers (i.e. not work stations), grant to Administrators and Operators only.
Allow log on through Terminal Services	Windows XP (or later) only. Allows a user to log on to the computer by using a Remote Desktop connection.	By default, this right is assigned to Administrators and Remote Desktop Users.
Backup files and directories	Allows a user to back up files and directories of the computer. This right supersedes files and directory permissions. At domain level this applies to all domain controllers in the domain. On a server or workstation, this applies to that machine only.	Grant only to Administrator and Backup Operator.
Bypass traverse checking	Allows a user to change directories and travel through directory trees of the computer, even if the user has no permissions for the traversed directories. This is an advanced user right. At domain level this applies to all domain controllers in the domain. On a server or workstation, this applies to that machine only.	Restrict as required. It is enabled by default for all users.
Change the system time	Allows modification of the system time (internal clock). At domain level this applies to all domain controllers in the domain. On a server or workstation, this applies to that machine only.	Grant to Administrators only.
Change the time zone	Windows Vista or later. This setting determines which users can change the time zone of the computer. This ability holds no great danger for the computer and may be useful for mobile workers.	Restrict as required.
Create a page file	Allows creation of a paging file.	Grant to Administrators only.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Right	Description	Recommendation
Create a token object	Allows creation of an access token that is typically created only by the Windows NT executive layer. The primary token can be assigned to a process to represent the default security information for that process.	Grant to no one.
Create global objects	Windows 2000 (SP4 or later) only. Allows a user account to create global objects in a Terminal Services session. Note that users can still create session-specific objects without being assigned this user right.	By default, members of the Administrators group, the System account, and Services that are started by the Service Control Manager are assigned the "Create global objects" user right.
Create permanent shared objects	Allows a user to create special permanent objects such as \\Device used within NT.	Grant to no one or to Administrators only.
Create symbolic links	Windows Vista or later. Determines which users can create symbolic links. In Windows Vista, existing NTFS file system objects, such as files and folders, can be accessed by referring to a new kind of file system object called a symbolic link. A symbolic link is a pointer (much like a shortcut or .lnk file) to another file system object. Consult Microsoft documentation for details on Symbolic Links.	Symbolic links can potentially expose security vulnerabilities in applications that are not designed to use them. The privilege for creating symbolic links should only be assigned to trusted users. By default, only Administrators can create symbolic links
Debug programs	Allows a user to debug a process.	Grant to no one unless required for development purposes.
Deny access to this computer from the network	Windows 2000 only. Prevents a user from connecting to the computer over the network.	Grant as required.
Deny log on as a batch job	Windows 2000 only. Prevents user from logging on as a batch job	Grant as required.
Deny log on as a service	Windows 2000 only. Prevent a process from registering with the system as a service.	Grant as required.
Deny log on through Terminal Services	Windows XP (or later) only. Prohibits a user from logging on to the computer using a Remote Desktop connection.	Grant as required.
Deny user from logging on locally	Windows 2000 only. Prevent a user from logging on at the computer from the computer's keyboard.	Grant as required.
Enable accounts to be trusted for delegation	Windows 2000 only. Allows a user to set the "Trusted for Delegation" setting on a user or computer object.	Grant to Administrators only. Misuse of this privilege could make the network vulnerable to sophisticated attacks using Trojan horse programs that impersonate incoming clients and use their credentials to gain access to network resources.
Force shutdown from a remote system	Allows a user to shut down a system using a network request.	Grant to Administrators only.
Generate security audits	Allows generation of audit-log entries.	Give this right to secure servers.
Impersonate a Client after authentication	Windows 2000 (SP4 or later) only. Permits programs that run on behalf of the user to impersonate a client. This security setting helps to prevent unauthorized servers from impersonating clients that connect to it through methods such as remote procedure calls (RPC) or named pipes.	By default, members of the Administrators group and the System account are assigned the right.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Right	Description	Recommendation
Increase a process working set	Windows Vista or later. Determines which user accounts can increase or decrease the size of a process' working set. Increasing the working set size for a process decreases the amount of physical memory available to the rest of the system. It would be possible for malicious code to increase the process working set to a level that could severely degrade system performance and potentially cause a denial of service.	This right is granted to all users by default. This should be assigned to specific users to limit the risks.
Increase scheduling priority	Allows a user to increase the execution priority of a process.	Grant to Administrators only.
Load and unload device drivers	Allows a user to install and remove device drivers.	Grant to Administrators only.
Lock pages in memory	Allows a user to lock pages in memory so they cannot be paged out to a backing store such as Pagefile.sys.	Grant to no one.
Log on as a batch job	Allows a user to log on as a batch job.	Grant to no one.
Log on as a service	Allows a process to register with the system as a service. This is an advanced user right. At domain level this applies to all domain controllers in the domain. On a server or workstation, this applies to that machine only.	Grant to no one.
Manage auditing and security log	Allows a user to manage the auditing of files, directories, and other objects. A user with this right can use the Security tab in the Properties dialog box to specify auditing options for the selected objects, users and groups, and types of access. This right does not enable a user to use Audit on the Policies menu to configure security events to be audited. This ability is always held only by Administrators. At domain level this applies to all domain controllers in the domain. On a server or workstation, this applies to that machine only.	Grant to Administrators only.
Modify an object label	Windows Vista or later. This privilege determines which user accounts can modify the integrity label of objects, such as files, registry keys, or processes owned by other users. Processes running under a user account can modify the label of an object owned by that user to a lower level without this privilege.	Grant to no one.
Modify firmware environment values	Allows a user to modify the non-volatile RAM of systems that use this type of memory to store configuration information.	Grant to Administrators only.
Perform volume maintenance tasks	Windows XP (or later) only. Allows a non-administrative or remote user to manage volumes or disks. The operating system checks for the privilege in a user's access token when a process running in the user's security context calls SetFileValidData().	By default, this right is assigned to members of the Administrators group.
Profile single process	Allows a user to gather profiling information for a single process.	Grant to Administrators only.
Profile system performance	Allows a user to gather profiling information (performance sampling) for the entire system.	Grant to Administrators or Operators.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)

Analysis Date: 06-Sep-2010

CONFIDENTIAL

Right	Description	Recommendation
Remove computer from docking station	Windows 2000 only. Allows a user to undock a laptop with the Windows 2000 user interface.	Grant as required.
Replace a process-level token	Allows a user to modify a process security access token.	Grant to no one. This is a powerful right used only by the system.
Restore files and directories	Allows a user to restore backed up files and directories. At domain level this applies to all domain controllers in the domain. On a server or workstation, this applies to that machine only.	Grant to Administrators and Backup Operators only. This right overrides file and directory permissions.
Shut down the system	Allows a user to shut down Windows NT. At domain level this applies to all domain controllers in the domain. On a server or workstation, this applies to that machine only.	Grant to Administrators and Operators only. Especially for domain controllers or servers. On workstations, this can be granted to all users.
Synchronize directory service data	Windows 2000 only. Allows a user to synchronize directory service data.	Grant to Administrators only.
Take ownership of files or other objects	Allows a user to take ownership of files, directories, printers and other objects on the computer. At domain level this applies to all domain controllers in the domain. On a server or workstation, this applies to that machine only.	Grant to Administrators only. This right overrides permissions protecting the object(s).

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### 15.2 Rights Assigned to Local Groups

Local Group	Right
Administrators	Access this computer from the network
	Adjust memory quotas for a process
	Allow log on locally
	Allow log on through Terminal Services
	Backup files and directories
	Bypass traverse checking
	Change the system time
	Create a page file
	Create global objects
	Debug programs
	Force shutdown from a remote system
	Impersonate a Client after authentication
	Increase scheduling priority
	Load and unload device drivers
	Manage auditing and security log
	Modify firmware environment values
	Perform volume maintenance tasks
	Profile single process
	Profile system performance
	Remove computer from docking station
Restore files and directories	
Shut down the system	
Take ownership of files or other objects	
Backup Operators	Access this computer from the network
	Allow log on locally
	Backup files and directories
	Bypass traverse checking
	Restore files and directories
Shut down the system	
Power Users	Access this computer from the network
	Allow log on locally
	Bypass traverse checking
	Change the system time
	Profile single process
	Remove computer from docking station
Shut down the system	
Remote Desktop Users	Allow log on through Terminal Services
Users	Access this computer from the network
	Allow log on locally
	Bypass traverse checking

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### 15.3 Rights Assigned to Global Groups (DCs only)

A Group name followed by a (Local) Group name in brackets indicates that the Global group acquires these rights *indirectly* via its membership of the Local group. E.g.



\*\*\*This report section only applies to Domain Controllers. There will be no data for Servers or Workstations.\*\*\*

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### 15.4 Rights Assigned to Users

The following two reports list *all* rights assigned to users, including rights assigned *directly* via the User Rights Policy, and rights acquired *indirectly* via memberships of Local and Global groups. The first report is **Grouped by Right** and the second is **Grouped by User Account**.

A Group name of 'None', with a Group Type of 'N/A', indicates that the right is assigned *directly* to the User account. A Local Group name followed by a (Global) Group name in brackets indicates that the right is acquired *indirectly* via the Global Group's membership of the Local Group. E.g.

<b>User Account</b>	is a member of...	<b>(Member)</b>	is a member of...	<b>Group Name</b>	which has...	<b>Right 1</b>
User1		(GlobalGroup2)		LocalGroup3		Right 2

Consult reports **Rights Assigned to Local Groups** and **Rights Assigned to Global Groups (PDC/BDC only)** for a complete list of rights assigned to all Group accounts.

### Section Summary

33.3% (1) of user accounts have right 'Access this computer from the network'  
33.3% (1) of user accounts have right 'Deny access to this computer from the network'  
33.3% (1) of user accounts have right 'Access this computer from the network(Effective)'  
0.0% (0) of user accounts have right 'Act as part of the operating system'  
0.0% (0) of user accounts have right 'Add workstations to domain'  
33.3% (1) of user accounts have right 'Adjust memory quotas for a process'  
33.3% (1) of user accounts have right 'Allow log on locally'  
33.3% (1) of user accounts have right 'Deny log on locally'  
33.3% (1) of user accounts have right 'Log on locally(Effective)'  
33.3% (1) of user accounts have right 'Allow logon through Terminal Services'  
0.0% (0) of user accounts have right 'Deny logon through Terminal Services'  
33.3% (1) of user accounts have right 'Logon through Terminal Services(Effective)'  
33.3% (1) of user accounts have right 'Backup files and directories'  
33.3% (1) of user accounts have right 'Bypass traverse checking'  
33.3% (1) of user accounts have right 'Change the system time'  
33.3% (1) of user accounts have right 'Create a page file'  
0.0% (0) of user accounts have right 'Create a token object'  
33.3% (1) of user accounts have right 'Create global objects'  
0.0% (0) of user accounts have right 'Create permanent shared objects'  
33.3% (1) of user accounts have right 'Debug programs'  
0.0% (0) of user accounts have right 'Enable accounts to be trusted for delegation'  
33.3% (1) of user accounts have right 'Force shutdown from a remote system'  
0.0% (0) of user accounts have right 'Generate security audits'  
33.3% (1) of user accounts have right 'Impersonate a Client after authentication'  
33.3% (1) of user accounts have right 'Increase scheduling priority'  
33.3% (1) of user accounts have right 'Load and unload device drivers'  
0.0% (0) of user accounts have right 'Lock pages in memory'  
33.3% (1) of user accounts have right 'Log on as a batch job'  
0.0% (0) of user accounts have right 'Deny logon as a batch job'  
33.3% (1) of user accounts have right 'Logon as a batch job(Effective)'  
0.0% (0) of user accounts have right 'Log on as a service'  
0.0% (0) of user accounts have right 'Deny logon as a service'  
0.0% (0) of user accounts have right 'Logon as a service(Effective)'  
33.3% (1) of user accounts have right 'Manage auditing and security log'  
33.3% (1) of user accounts have right 'Modify firmware environment values'  
33.3% (1) of user accounts have right 'Perform volume maintenance tasks'  
33.3% (1) of user accounts have right 'Profile single process'  
33.3% (1) of user accounts have right 'Profile system performance'  
33.3% (1) of user accounts have right 'Remove computer from docking station'  
0.0% (0) of user accounts have right 'Replace a process-level token'  
33.3% (1) of user accounts have right 'Restore files and directories'  
33.3% (1) of user accounts have right 'Shut down the system'  
0.0% (0) of user accounts have right 'Synchronize directory service data'  
33.3% (1) of user accounts have right 'Take ownership of files or other objects'

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### Grouped by Right

Right	User Account	Group Name (Member)	Group Type	Disabled
Access this computer from the network	Administrator	Administrators	Local	
Access this computer from the network (Effective)	Administrator	Administrators	Local	
Adjust memory quotas for a process	Administrator	Administrators	Local	
Allow log on locally	Administrator	Administrators	Local	
Allow log on through Terminal Services	Administrator	Administrators	Local	
Allow log on through Terminal Services (Effective)	Administrator	Administrators	Local	
Backup files and directories	Administrator	Administrators	Local	
Bypass traverse checking	Administrator	Administrators	Local	
Change the system time	Administrator	Administrators	Local	
Create a page file	Administrator	Administrators	Local	
Create global objects	Administrator	Administrators	Local	
Debug programs	Administrator	Administrators	Local	
Deny access to this computer from the network	SUPPORT_388945a0	None	N/A	Yes
Deny user from logging on locally	SUPPORT_388945a0	None	N/A	Yes
Force shutdown from a remote system	Administrator	Administrators	Local	
Impersonate a Client after authentication	Administrator	Administrators	Local	
Increase scheduling priority	Administrator	Administrators	Local	
Load and unload device drivers	Administrator	Administrators	Local	
Log on as a batch job	SUPPORT_388945a0	None	N/A	Yes
Log on as a batch job (Effective)	SUPPORT_388945a0	None	N/A	Yes
Log on locally (Effective)	Administrator	Administrators	Local	
Manage auditing and security log	Administrator	Administrators	Local	
Modify firmware environment values	Administrator	Administrators	Local	
Perform volume maintenance tasks	Administrator	Administrators	Local	
Profile single process	Administrator	Administrators	Local	
Profile system performance	Administrator	Administrators	Local	
Remove computer from docking station	Administrator	Administrators	Local	
Restore files and directories	Administrator	Administrators	Local	
Shut down the system	Administrator	Administrators	Local	
Take ownership of files or other objects	Administrator	Administrators	Local	

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

### Grouped by User Account

User Account	Right	Group Name (Member)	Group Type	Disabled
Administrator	Access this computer from the network	Administrators	Local	
	Access this computer from the network (Effective)	Administrators	Local	
	Adjust memory quotas for a process	Administrators	Local	
	Allow log on locally	Administrators	Local	
	Allow log on through Terminal Services	Administrators	Local	
	Allow log on through Terminal Services (Effective)	Administrators	Local	
	Backup files and directories	Administrators	Local	
	Bypass traverse checking	Administrators	Local	
	Change the system time	Administrators	Local	
	Create a page file	Administrators	Local	
	Create global objects	Administrators	Local	
	Debug programs	Administrators	Local	
	Force shutdown from a remote system	Administrators	Local	
	Impersonate a Client after authentication	Administrators	Local	
	Increase scheduling priority	Administrators	Local	
	Load and unload device drivers	Administrators	Local	
	Log on locally (Effective)	Administrators	Local	
	Manage auditing and security log	Administrators	Local	
	Modify firmware environment values	Administrators	Local	
	Perform volume maintenance tasks	Administrators	Local	
	Profile single process	Administrators	Local	
	Profile system performance	Administrators	Local	
	Remove computer from docking station	Administrators	Local	
	Restore files and directories	Administrators	Local	
	Shut down the system	Administrators	Local	
	Take ownership of files or other objects	Administrators	Local	
	SUPPORT_388945a0	Deny access to this computer from the network	None	N/A
Deny user from logging on locally		None	N/A	Yes
Log on as a batch job		None	N/A	Yes
Log on as a batch job (Effective)		None	N/A	Yes

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

### 16. Trusted and Trusting Domains (DCs only)

#### Section Summary

---

\*\*\*This report section only applies to Domain Controllers. There will be no data for Servers or Workstations.\*\*\*

#### Section Detail

---

\*\* No data found \*\*

#### Implications

---

A trust relationship is a link between two Windows Server domains.

Trusted Domains are domains that the current domain trusts to use its resources. Only Windows Server domains can be trusted domains. Trust relationships can only be established between Windows Server domains.

Trusting domains allow their resources to be used by accounts in trusted domains.

Trusted domain users and global groups can hold user rights, resource permissions, and local group memberships on the trusting domain.

Trust relationships allow users to access resources on the trusting domain using a single user account and a single password. ***The trusting domain will rely on the trusted domain to verify the userid and password of users logging on the trusted domain.***

Trusted domains can potentially provide paths for illegal access to the trusting domain. Weak security standards applied in trusted domains can undermine security on the trusting domain.

#### Risk Rating

---

Medium to High (dependant on the quality of security standards applied in trusted domains).

#### Recommended Action

---

You should satisfy yourself that security in domains trusted by your system is implemented and administered to appropriate standards. You should consider running *SekChek* on domain controllers (i.e. a PDC or BDC) for all trusted domains.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

### 17. Local Accounts (DCs only)

#### Section Summary

---

\*\*\*This report section only applies to Domain Controllers. There will be no data for Servers or Workstations.\*\*\*

#### Section Detail

---

\*\* No data found \*\*

#### Implications

---

A local account is an account provided in the domain for a user whose regular account is not in a trusted domain. This might be a Windows Server domain that is not trusted by the domain, a LAN Manager domain, or another type of domain or network.

Local accounts can be used to access computers running Windows Workstation or Server over the network, and can be granted resource permissions and user rights. However, local accounts cannot be used to log on interactively to the domain.

Local accounts created in one domain cannot be used in trusting domains, and do not appear in the Add Users and Groups dialog boxes of trusting domains when adding accounts to groups.

It is best for a local account to use the same password both here and in its home domain.

#### Risk Rating

---

Low to Medium.

#### Recommended Action

---

Rights and privileges assigned to local accounts should be carefully monitored.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 18. Servers and Workstations

### Section Summary

There were a total of 3 Servers visible to your system at the time of the analysis:

- 33.3% (1) are Primary Domain Controllers
- 33.3% (1) are Backup Domain Controllers
- 33.3% (1) are Servers
- 0.0% (0) are Workstations

### Section Detail

Server	Description	Role	Software Version	Other Roles
HADES		BDC	5.2	Browser Backup; Time Source Server
PROMETHEUS	File Server on olympus.com	Server	5.2	Browser Backup
ZEUS	DC on olympus.com	PDC	5.2	Dial-in Service; Master Browser; Time Source Server

### Implications

Every server and workstation will provide different services to users within the domain/network.

Servers normally offer services such as SQL database, application, backup domain controller, primary domain controller, Internet services and remote access services.

Workstations are normally used by end users to logon to the network and make use of resources and services as required.

In a Windows environment, workstations can also act as servers providing services and resources to network users. Examples are workstations providing Internet services and **RAS services** within the network.

Resources and services can be shared (with varying access permission settings) on all servers and workstations.

For the above reasons, every server and workstation is a potential security risk providing an access path to domain/network resources.

### Risk Rating

Medium to High (Depending on the type of servers, their configuration and security setting standards applied).

### Recommended Action

You should ensure that:

- Configuration and security values are set to appropriate standards.
- Services and resources are appropriately restricted on servers and workstations.
- Accounts databases have the appropriate security settings to help prevent illegal access.
- The **rights and privileges** assigned to user accounts, global groups and local groups are effectively controlled.
- Effective virus detection and prevention services are installed, running and activated/started automatically at system start-up time.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 19. RAS Privileges

### Section Summary

There are 1 RAS (Remote Access Service) Servers defined on your Domain/Network.

#### All Accounts

0.0% (0) of users have permission to dial-in to your system through RAS:

#### Excluding Disabled Accounts

0.0% (0) of users have permission to dial-in to your system through RAS:

#### All Administrator Accounts

0.0% (0) of administrator accounts have permission to dial-in to your system through RAS:

#### Administrator Accounts (Excluding Disabled Accounts)

0.0% (0) of administrator accounts have permission to dial-in to your system through RAS:

### Section Detail

The following RAS Servers are defined on your Domain/Network:

Server	Description	Role	Ports
\\ZEUS	DC on olympus.com	PDC	11

The following profiles have permission to dial-in to your system through RAS:

\*\* No data found \*\*

#### LEGEND:

Call Back = Yes : The Server will call back the user before log on is allowed.  
Administrator sets Call Back Number = Yes : The call back number is pre set.  
Caller Sets Call Back Number = Yes : The user provides a call back number every time.  
Phone Number : Reflects the pre set phone number for call back.

If *SekChek* is analysing a Domain Controller (PDC or BDC) the above RAS privileges apply to the whole domain and domain accounts. If a Server (non-PDC or BDC) or Workstation is being analysed the above RAS privileges only apply to the local machine and local accounts.

If there are accounts listed with RAS privileges and no RAS servers found, it means that the accounts have been granted RAS privileges but that either:

- No RAS servers were visible when this analysis was done.  
Or
- There was a RAS service installed at some stage but it has been discontinued.

0 ports listed in RAS servers indicates that the server has the RAS service configured but not active (started).

### Implications

RAS (Remote Access Service) allows users to access your system remotely via modems, ISDN etc.

RAS increases the risk of unauthorised access to your system because your system is visible to a much larger number of potential intruders via the public telephone network. The risk is greater if privileged users, such as Administrators, are allowed access through RAS.

In general, multiple RAS servers also increase security risks simply because the number of external access points, which all require securing, is obviously greater. The strength of general security and RAS security on those servers is an important factor in controlling the risks.

You will obtain the most comprehensive view of RAS privileges by running *SekChek* on the domain controller, selected RAS servers, and domain controllers for each trusted domain and on their RAS servers.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

When servers and workstations are members of a domain, they will usually allow users to logon to the domain. For workstations and servers that are not domain members (i.e. Standalone machines), domain logon is normally not available to users.

Inappropriate security settings in RAS can create significant security exposures.

A value of *Yes* in the *Account Disabled* column indicates that the account has been disabled by a security administrator, is locked due to excessive failed login attempts, or has expired. See [Disabled Accounts](#) for details.

### Risk Rating

---

Medium to high (dependent on settings for RAS users, RAS parameters and the strength of password controls.).

### Recommended Action

---

You should only grant dial in (RAS) access to those users who require it for their job functions. Ensure that RAS access is not granted to all user accounts by default.

In general, you should ensure that the call back feature is enabled for all RAS users and that a pre-set phone number is used.

Do not grant RAS access to privileged accounts (e.g. Administrators) unless absolutely necessary.

If possible, restrict the log-on hours for RAS users. This feature can be set for individual user accounts.

Ensure that the option to prevent clear-text passwords being negotiated is utilised. This is a setting within RAS.

Review the RAS settings on all RAS servers on a regular basis and ensure that appropriate security standards are applied on all of these machines.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 20. Services and Drivers on the Machine

### Section Summary

There are a total of 232 Services installed.

These Services include the following types:

- 57.3% (133) are Kernel Drivers
- 6.0% (14) are File System Drivers
- 8.2% (19) are Own Process
- 26.3% (61) are Shared Process
- 1.7% (4) are Own Process (Interactive)
- 0.4% (1) are Shared Process (Interactive)

The Services start types are:

- 7.3% (17) System Boot
- 12.1% (28) System
- 15.1% (35) Automatic
- 32.3% (75) Manual
- 33.2% (77) Disabled

Their current states are:

- 54.3% (126) Stopped
- 0.0% (0) Starting
- 0.0% (0) Stopping
- 45.7% (106) Running
- 0.0% (0) Continuing
- 0.0% (0) Pausing
- 0.0% (0) Paused

Following are two reports. The first enumerates *services and drivers, their state and start type*. The second *enumerates services and drivers with their logon account and path name containing the executable*. The services listed are on the machine being analysed and do not reflect services installed on other machines.

### Section Detail

Service Name	Display Name	State	Service Type	Start Type
1-driver-vmsvc	Virtual Machine Additions Services Driver	Running	Kernel Driver	System
1-vmsvc	Virtual Machine Additions Services Application	Running	Own Process(l)	Automatic
Abiosdsk	Abiosdsk	Stopped	Kernel Driver	Disabled
ACPI	Microsoft ACPI Driver	Running	Kernel Driver	Boot
ACPIEC	ACPIEC	Stopped	Kernel Driver	Disabled
adpu160m	adpu160m	Stopped	Kernel Driver	Disabled
adpu320	adpu320	Stopped	Kernel Driver	Disabled
afcnt	afcnt	Stopped	Kernel Driver	Disabled
AFD	AFD Networking Support Environment	Running	Kernel Driver	Automatic
Aha154x	Aha154x	Stopped	Kernel Driver	Disabled
aic78u2	aic78u2	Stopped	Kernel Driver	Disabled
aic78xx	aic78xx	Stopped	Kernel Driver	Disabled
Alerter	Alerter	Stopped	Shared Process	Disabled
ALG	Application Layer Gateway Service	Stopped	Own Process	Manual

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Service Name	Display Name	State	Service Type	Start Type
Alilde	Alilde	Stopped	Kernel Driver	Disabled
AppMgmt	Application Management	Running	Shared Process	Manual
AsyncMac	RAS Asynchronous Media Driver	Stopped	Kernel Driver	Manual
atapi	Standard IDE/ESDI Hard Disk Controller	Running	Kernel Driver	Boot
Atdisk	Atdisk	Stopped	Kernel Driver	Disabled
Atmarpc	ATM ARP Client Protocol	Stopped	Kernel Driver	Manual
AudioSrv	Windows Audio	Stopped	Shared Process	Disabled
audstub	Audio Stub Driver	Running	Kernel Driver	Manual
Beep	Beep	Running	Kernel Driver	System
BITS	Background Intelligent Transfer Service	Stopped	Shared Process	Manual
Browser	Computer Browser	Running	Shared Process	Automatic
cbidf2k	cbidf2k	Stopped	Kernel Driver	Disabled
cd20xrnt	cd20xrnt	Stopped	Kernel Driver	Disabled
Cdfs	Cdfs	Running	File System Driver	Disabled
Cdrom	CD-ROM Driver	Running	Kernel Driver	System
Changer	Changer	Stopped	Kernel Driver	System
CiSvc	Indexing Service	Stopped	Shared Process	Disabled
ClipSrv	ClipBook	Stopped	Own Process	Disabled
ClusDisk	Cluster Disk Driver	Stopped	Kernel Driver	Disabled
Cmdlde	Cmdlde	Stopped	Kernel Driver	Disabled
COMSysApp	COM+ System Application	Stopped	Own Process	Manual
Cpqarray	Cpqarray	Stopped	Kernel Driver	Disabled
cpqarry2	cpqarry2	Stopped	Kernel Driver	Disabled
cpqcissm	cpqcissm	Stopped	Kernel Driver	Disabled
cpqfcalm	cpqfcalm	Stopped	Kernel Driver	Disabled
crcdisk	CRC Disk Filter Driver	Running	Kernel Driver	Boot
CryptSvc	Cryptographic Services	Running	Shared Process	Automatic
dac960nt	dac960nt	Stopped	Kernel Driver	Disabled
DC21x4	DC21x4 Based Network Adapter Driver	Running	Kernel Driver	Manual
dellcerc	dellcerc	Stopped	Kernel Driver	Disabled
Dfs	Distributed File System	Running	Own Process	Automatic
DfsDriver	DfsDriver	Running	File System Driver	Boot
Dhcp	DHCP Client	Running	Shared Process	Automatic
Disk	Disk Driver	Running	Kernel Driver	Boot
dmadmin	Logical Disk Manager Administrative Service	Stopped	Shared Process	Manual
dmboot	dmboot	Stopped	Kernel Driver	Disabled
dmio	Logical Disk Manager Driver	Running	Kernel Driver	Boot
dmload	dmload	Running	Kernel Driver	Boot
dmserver	Logical Disk Manager	Running	Shared Process	Automatic
Dnscache	DNS Client	Running	Shared Process	Automatic
dpti2o	dpti2o	Stopped	Kernel Driver	Disabled
ERSvc	Error Reporting Service	Running	Shared Process	Automatic
Eventlog	Event Log	Running	Shared Process	Automatic

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Service Name	Display Name	State	Service Type	Start Type
EventSystem	COM+ Event System	Running	Shared Process	Manual
Fastfat	Fastfat	Running	File System Driver	Disabled
Fdc	Floppy Disk Controller Driver	Running	Kernel Driver	Manual
Fips	Fips	Running	Kernel Driver	System
Flpydisk	Floppy Disk Driver	Running	Kernel Driver	Manual
Ftdisk	Volume Manager Driver	Running	Kernel Driver	Boot
gameenum	Game Port Enumerator	Running	Kernel Driver	Manual
Gpc	Generic Packet Classifier	Running	Kernel Driver	Manual
helpsvc	Help and Support	Running	Shared Process	Automatic
HidServ	Human Interface Device Access	Stopped	Shared Process	Disabled
hpn	hpn	Stopped	Kernel Driver	Disabled
hpt3xx	hpt3xx	Stopped	Kernel Driver	Disabled
HTTP	HTTP	Stopped	Kernel Driver	Manual
HTTPFilter	HTTP SSL	Stopped	Shared Process	Manual
i2omgmt	i2omgmt	Stopped	Kernel Driver	System
i2omp	i2omp	Stopped	Kernel Driver	Disabled
i8042prt	i8042 Keyboard and PS/2 Mouse Port Driver	Running	Kernel Driver	System
iirsp	iirsp	Stopped	Kernel Driver	Disabled
imapi	CD-Burning Filter Driver	Stopped	Kernel Driver	System
ImapiService	IMAPI CD-Burning COM Service	Stopped	Own Process	Disabled
Intellde	Intellde	Running	Kernel Driver	Boot
IpFilterDriver	IP Traffic Filter Driver	Stopped	Kernel Driver	Manual
IpInIp	IP in IP Tunnel Driver	Stopped	Kernel Driver	Manual
IpNat	IP Network Address Translator	Stopped	Kernel Driver	Manual
IPSec	IPSEC driver	Running	Kernel Driver	System
ipsraidn	ipsraidn	Stopped	Kernel Driver	Disabled
isapnp	PnP ISA/EISA Bus Driver	Running	Kernel Driver	Boot
IsmServ	Intersite Messaging	Stopped	Own Process	Disabled
Kbdclass	Keyboard Class Driver	Running	Kernel Driver	System
kdc	Kerberos Key Distribution Center	Stopped	Shared Process	Disabled
KSecDD	KSecDD	Running	Kernel Driver	Boot
lanmanserver	Server	Running	Shared Process	Automatic
lanmanworkstation	Workstation	Running	Shared Process	Automatic
LicenseService	License Logging	Stopped	Own Process	Disabled
LmHosts	TCP/IP NetBIOS Helper	Running	Shared Process	Automatic
Ip6nds35	Ip6nds35	Stopped	Kernel Driver	Disabled
Messenger	Messenger	Stopped	Shared Process	Disabled
mnmdd	mnmdd	Running	Kernel Driver	System
mnmsrvc	NetMeeting Remote Desktop Sharing	Stopped	Own Process(l)	Disabled
Modem	Modem	Stopped	Kernel Driver	Manual
Mouclass	Mouse Class Driver	Running	Kernel Driver	System
MountMgr	Mount Point Manager	Running	Kernel Driver	Boot
mraid35x	mraid35x	Stopped	Kernel Driver	Disabled

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
 Analysis Date: 06-Sep-2010

CONFIDENTIAL

Service Name	Display Name	State	Service Type	Start Type
MRxDAV	WebDav Client Redirector	Stopped	File System Driver	Manual
MRxSmb	MRxSmb	Running	File System Driver	System
MRxVPC	Virtual Machine Additions Folder Sharing Driver	Running	File System Driver	Automatic
MSDTC	Distributed Transaction Coordinator	Running	Own Process	Automatic
Msfs	Msfs	Running	File System Driver	System
MSIServer	Windows Installer	Stopped	Shared Process	Manual
msvmouf	Virtual Machine Additions Mouse Integration Filter Driver	Running	Kernel Driver	System
Mup	Mup	Running	File System Driver	Boot
NDIS	NDIS System Driver	Running	Kernel Driver	Boot
NdisTapi	Remote Access NDIS TAPI Driver	Running	Kernel Driver	Manual
Ndisuio	NDIS Usermode I/O Protocol	Running	Kernel Driver	Manual
NdisWan	Remote Access NDIS WAN Driver	Running	Kernel Driver	Manual
NDProxy	NDIS Proxy	Running	Kernel Driver	Manual
NetBIOS	NetBIOS Interface	Running	File System Driver	System
NetBT	NetBios over Tcpip	Running	Kernel Driver	System
NetDDE	Network DDE	Stopped	Shared Process	Disabled
NetDDEdsdm	Network DDE DSDM	Stopped	Shared Process	Disabled
Netlogon	Net Logon	Running	Shared Process	Automatic
Netman	Network Connections	Running	Shared Process	Manual
nfrd960	nfrd960	Stopped	Kernel Driver	Disabled
Nla	Network Location Awareness (NLA)	Running	Shared Process	Manual
Npfs	Npfs	Running	File System Driver	System
NtFrs	File Replication	Stopped	Own Process	Manual
Ntfs	Ntfs	Running	File System Driver	Disabled
NtLmSsp	NT LM Security Support Provider	Stopped	Shared Process	Manual
NtmsSvc	Removable Storage	Stopped	Shared Process	Manual
Null	Null	Running	Kernel Driver	System
Parport	Parallel port driver	Running	Kernel Driver	Manual
PartMgr	Partition Manager	Running	Kernel Driver	Boot
Parvdm	Parvdm	Running	Kernel Driver	Automatic
PCI	PCI Bus Driver	Running	Kernel Driver	Boot
PCIIde	PCIIde	Stopped	Kernel Driver	Disabled
Pcmcia	Pcmcia	Stopped	Kernel Driver	Disabled
PDCOMP	PDCOMP	Stopped	Kernel Driver	Manual
PDFRAME	PDFRAME	Stopped	Kernel Driver	Manual
PDRELI	PDRELI	Stopped	Kernel Driver	Manual
PDRFRAME	PDRFRAME	Stopped	Kernel Driver	Manual
perc2	perc2	Stopped	Kernel Driver	Disabled
perc2hib	perc2hib	Stopped	Kernel Driver	Disabled
PlugPlay	Plug and Play	Running	Shared Process	Automatic
PolicyAgent	IPSEC Services	Running	Shared Process	Automatic
PptpMiniport	WAN Miniport (PPTP)	Running	Kernel Driver	Manual

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
 Analysis Date: 06-Sep-2010

CONFIDENTIAL

Service Name	Display Name	State	Service Type	Start Type
Processor	Processor Driver	Stopped	Kernel Driver	Manual
ProtectedStorage	Protected Storage	Running	Shared Process(I)	Automatic
Ptilink	Direct Parallel Link Driver	Running	Kernel Driver	Manual
ql1080	ql1080	Stopped	Kernel Driver	Disabled
Ql10wnt	Ql10wnt	Stopped	Kernel Driver	Disabled
ql12160	ql12160	Stopped	Kernel Driver	Disabled
ql1240	ql1240	Stopped	Kernel Driver	Disabled
ql1280	ql1280	Stopped	Kernel Driver	Disabled
ql2100	ql2100	Stopped	Kernel Driver	Disabled
ql2200	ql2200	Stopped	Kernel Driver	Disabled
ql2300	ql2300	Stopped	Kernel Driver	Disabled
RasAcD	Remote Access Auto Connection Driver	Running	Kernel Driver	System
RasAuto	Remote Access Auto Connection Manager	Stopped	Shared Process	Manual
Rasl2tp	WAN Miniport (L2TP)	Running	Kernel Driver	Manual
RasMan	Remote Access Connection Manager	Stopped	Shared Process	Manual
RasPppoe	Remote Access PPPOE Driver	Running	Kernel Driver	Manual
Raspti	Direct Parallel	Running	Kernel Driver	Manual
Rdbss	Rdbss	Running	File System Driver	System
RDPCDD	RDPCDD	Running	Kernel Driver	System
rdpdr	Terminal Server Device Redirector Driver	Running	Kernel Driver	Manual
RDPWD	RDPWD	Stopped	Kernel Driver	Manual
RDSessMgr	Remote Desktop Help Session Manager	Stopped	Own Process	Manual
redbook	Digital CD Audio Playback Filter Driver	Stopped	Kernel Driver	System
RemoteAccess	Routing and Remote Access	Stopped	Shared Process	Disabled
RemoteRegistry	Remote Registry	Running	Shared Process	Automatic
RpcLocator	Remote Procedure Call (RPC) Locator	Stopped	Own Process	Manual
RpcSs	Remote Procedure Call (RPC)	Running	Shared Process	Automatic
RSOProv	Resultant Set of Policy Provider	Stopped	Shared Process	Manual
s3legacy	s3legacy	Stopped	Kernel Driver	Manual
sacsvr	Special Administration Console Helper	Stopped	Shared Process	Manual
SamSs	Security Accounts Manager	Running	Shared Process	Automatic
SCardSvr	Smart Card	Stopped	Shared Process	Manual
Schedule	Task Scheduler	Running	Shared Process	Automatic
Secdrv	Secdrv	Stopped	Kernel Driver	Manual
seclogon	Secondary Logon	Running	Shared Process	Automatic
SENS	System Event Notification	Running	Shared Process	Automatic
serenum	Serenum Filter Driver	Running	Kernel Driver	Manual
Serial	Serial port driver	Running	Kernel Driver	System
Sfloppy	Sfloppy	Stopped	Kernel Driver	System
SharedAccess	Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)	Stopped	Shared Process	Disabled
ShellHWDetection	Shell Hardware Detection	Running	Shared Process	Automatic
Simbad	Simbad	Stopped	Kernel Driver	Disabled
Sparrow	Sparrow	Stopped	Kernel Driver	Disabled

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)

Analysis Date: 06-Sep-2010

CONFIDENTIAL

Service Name	Display Name	State	Service Type	Start Type
Spooler	Print Spooler	Running	Own Process(l)	Automatic
Srv	Srv	Running	File System Driver	Manual
stisvc	Windows Image Acquisition (WIA)	Stopped	Shared Process	Disabled
swenum	Software Bus Driver	Running	Kernel Driver	Manual
swprv	Microsoft Software Shadow Copy Provider	Stopped	Own Process	Manual
sym_hi	sym_hi	Stopped	Kernel Driver	Disabled
sym_u3	sym_u3	Stopped	Kernel Driver	Disabled
symc810	symc810	Stopped	Kernel Driver	Disabled
symc8xx	symc8xx	Stopped	Kernel Driver	Disabled
symmpi	symmpi	Stopped	Kernel Driver	Disabled
SysmonLog	Performance Logs and Alerts	Stopped	Own Process	Manual
TapiSrv	Telephony	Stopped	Shared Process	Manual
Tcpip	TCP/IP Protocol Driver	Running	Kernel Driver	System
TDPIPE	TDPIPE	Stopped	Kernel Driver	Manual
TDTCP	TDTCP	Stopped	Kernel Driver	Manual
TermDD	Terminal Device Driver	Running	Kernel Driver	System
TermService	Terminal Services	Running	Shared Process	Manual
Themes	Themes	Stopped	Shared Process	Disabled
TIntSvr	Telnet	Stopped	Own Process	Disabled
TosIde	TosIde	Stopped	Kernel Driver	Disabled
TrkSvr	Distributed Link Tracking Server	Stopped	Shared Process	Disabled
TrkWks	Distributed Link Tracking Client	Running	Shared Process	Automatic
Tssdis	Terminal Services Session Directory	Stopped	Own Process	Disabled
Udfs	Udfs	Stopped	File System Driver	Disabled
ultra	ultra	Stopped	Kernel Driver	Disabled
Update	Microcode Update Driver	Running	Kernel Driver	Manual
uploadmgr	Upload Manager	Stopped	Shared Process	Manual
UPS	Uninterruptible Power Supply	Stopped	Own Process	Manual
vds	Virtual Disk Service	Stopped	Own Process	Manual
VgaSave	VGA Display Controller.	Running	Kernel Driver	System
Vialde	Vialde	Stopped	Kernel Driver	Disabled
VolSnap	Storage volumes	Running	Kernel Driver	Boot
VPCMap	Virtual Machine Additions Shared Folder Service	Running	Own Process(l)	Automatic
vpc-s3	vpc-s3	Running	Kernel Driver	Manual
VSS	Volume Shadow Copy	Stopped	Own Process	Manual
W32Time	Windows Time	Running	Shared Process	Automatic
Wanarp	Remote Access IP ARP Driver	Running	Kernel Driver	Manual
WDICA	WDICA	Stopped	Kernel Driver	Manual
WebClient	WebClient	Stopped	Shared Process	Disabled
WinHttpAutoProxySvc	WinHTTP Web Proxy Auto-Discovery Service	Stopped	Shared Process	Manual
winmgmt	Windows Management Instrumentation	Running	Shared Process	Automatic
WLBS	Network Load Balancing	Stopped	Kernel Driver	Manual

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Service Name	Display Name	State	Service Type	Start Type
WmdmPmSN	Portable Media Serial Number Service	Stopped	Shared Process	Manual
Wmi	Windows Management Instrumentation Driver Extensions	Stopped	Shared Process	Manual
WmiApSrv	WMI Performance Adapter	Stopped	Own Process	Manual
wuauerv	Automatic Updates	Running	Shared Process	Automatic
WZCSVC	Wireless Configuration	Running	Shared Process	Automatic

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## Section Detail

Service Name	Logon Name	Path Name
1-driver-vmsrv		System32\drivers\vmssvc.sys
1-vmsrv	LocalSystem	C:\Program Files\Virtual Machine Additions\vmssvc.exe
Abiosdsk		
ACPI		\SystemRoot\system32\DRIVERS\ACPI.sys
ACPIEC		
adpu160m		
adpu320		
afcnt		
AFD		\SystemRoot\System32\drivers\afd.sys
Aha154x		
aic78u2		
aic78xx		
Alerter	NT AUTHORITY\LocalService	C:\WINDOWS\system32\svchost.exe -k LocalService
ALG	NT AUTHORITY\LocalService	C:\WINDOWS\System32\alg.exe
Alilde		
AppMgmt	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
AsyncMac		system32\DRIVERS\asynccmac.sys
atapi		\SystemRoot\system32\DRIVERS\atapi.sys
Atdisk		
Atmarpc		system32\DRIVERS\atmarpc.sys
AudioSrv	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
audstub		system32\DRIVERS\audstub.sys
Beep		
BITS	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
Browser	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
cbidf2k		
cd20xrnt		
Cdfs		
Cdrom		system32\DRIVERS\cdrom.sys
Changer		
CiSvc	LocalSystem	C:\WINDOWS\system32\cisvc.exe
ClipSrv	LocalSystem	C:\WINDOWS\system32\clipsrv.exe
ClusDisk		system32\DRIVERS\ClusDisk.sys
Cmdlde		
COMSysApp	LocalSystem	C:\WINDOWS\system32\dlhhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
Cpqarray		
cpqarray2		
cpqcissm		
cpqfcalm		
crtdisk		\SystemRoot\system32\DRIVERS\crtdisk.sys
CryptSvc	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)

Analysis Date: 06-Sep-2010

CONFIDENTIAL

Service Name	Logon Name	Path Name
dac960nt		
DC21x4		system32\DRIVERS\dc21x4.sys
dellcerc		
Dfs	LocalSystem	C:\WINDOWS\system32\Dfssvc.exe
DfsDriver		\SystemRoot\system32\drivers\Dfs.sys
Dhcp	NT AUTHORITY\NetworkService	C:\WINDOWS\system32\svchost.exe -k NetworkService
Disk		\SystemRoot\system32\DRIVERS\disk.sys
dmadmin	LocalSystem	C:\WINDOWS\System32\dmadmin.exe /com
dmboot		System32\drivers\dmboot.sys
dmio		\SystemRoot\System32\drivers\dmio.sys
dmload		\SystemRoot\System32\drivers\dmload.sys
dmserver	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
Dnscache	NT AUTHORITY\NetworkService	C:\WINDOWS\system32\svchost.exe -k NetworkService
dpti2o		
ERSvc	LocalSystem	C:\WINDOWS\System32\svchost.exe -k WinErr
Eventlog	LocalSystem	C:\WINDOWS\system32\services.exe
EventSystem	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
Fastfat		
Fdc		system32\DRIVERS\fdc.sys
Fips		
Flpydisk		system32\DRIVERS\flpydisk.sys
Ftdisk		\SystemRoot\system32\DRIVERS\ftdisk.sys
gameenum		system32\DRIVERS\gameenum.sys
Gpc		system32\DRIVERS\msgpc.sys
helpsvc	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
HidServ	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
hpn		
hpt3xx		
HTTP		System32\Drivers\HTTP.sys
HTTPFilter	LocalSystem	C:\WINDOWS\System32\lsass.exe
i2omgmt		
i2omp		
i8042prt		system32\DRIVERS\i8042prt.sys
iirsp		
imapi		system32\DRIVERS\imapi.sys
ImapiService	LocalSystem	C:\WINDOWS\system32\imapi.exe
Intellde		\SystemRoot\system32\DRIVERS\intelide.sys
IpFilterDriver		system32\DRIVERS\ipfltdrv.sys
IpInIp		system32\DRIVERS\ipinip.sys
IpNat		system32\DRIVERS\ipnat.sys
IPSec		system32\DRIVERS\ipsec.sys
ipsraidn		
isapnp		\SystemRoot\system32\DRIVERS\isapnp.sys

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Service Name	Logon Name	Path Name
lsmServ	LocalSystem	C:\WINDOWS\System32\lsmServ.exe
Kbdclass		system32\DRIVERS\kbdclass.sys
kdc	LocalSystem	C:\WINDOWS\System32\lsass.exe
KSecDD		
lanmanserver	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
lanmanworkstation	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
LicenseService	NT AUTHORITY\NetworkService	C:\WINDOWS\System32\llssrv.exe
LmHosts	NT AUTHORITY\LocalService	C:\WINDOWS\system32\svchost.exe -k LocalService
Ip6nds35		
Messenger	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
mnmdd		
mnmsrvc	LocalSystem	C:\WINDOWS\system32\mnmsrvc.exe
Modem		
Mouclass		system32\DRIVERS\mouclass.sys
MountMgr		
mraid35x		
MRxDAV		system32\DRIVERS\mrxdav.sys
MRxSmb		system32\DRIVERS\mrxsmb.sys
MRxVPC		\\?\C:\WINDOWS\system32\drivers\MRxVPC.sys
MSDTC	NT AUTHORITY\NetworkService	C:\WINDOWS\system32\msdtc.exe
Msfs		
MSIServer	LocalSystem	C:\WINDOWS\system32\msiexec.exe /V
msvmmouf		system32\DRIVERS\msvmmouf.sys
Mup		
NDIS		
NdisTapi		system32\DRIVERS\ndistapi.sys
Ndisuio		system32\DRIVERS\ndisuio.sys
NdisWan		system32\DRIVERS\ndiswan.sys
NDProxy		
NetBIOS		system32\DRIVERS\netbios.sys
NetBT		system32\DRIVERS\netbt.sys
NetDDE	LocalSystem	C:\WINDOWS\system32\netdde.exe
NetDDEdsdm	LocalSystem	C:\WINDOWS\system32\netdde.exe
Netlogon	LocalSystem	C:\WINDOWS\system32\lsass.exe
Netman	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
nfrd960		
Nla	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
Npfs		
NtFrs	LocalSystem	C:\WINDOWS\system32\ntfrs.exe
Ntfs		
NtLmSsp	LocalSystem	C:\WINDOWS\system32\lsass.exe
NtmsSvc	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
Null		

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Service Name	Logon Name	Path Name
Parport		system32\DRIVERS\parport.sys
PartMgr		
Parvdm		system32\DRIVERS\parvdm.sys
PCI		\SystemRoot\system32\DRIVERS\pci.sys
PCIIde		
Pcmcia		
PDCOMP		
PDFFRAME		
PDRELI		
PDRFRAME		
perc2		
perc2hib		
PlugPlay	LocalSystem	C:\WINDOWS\system32\services.exe
PolicyAgent	LocalSystem	C:\WINDOWS\system32\lsass.exe
PptpMiniport		system32\DRIVERS\raspppt.sys
Processor		system32\DRIVERS\processr.sys
ProtectedStorage	LocalSystem	C:\WINDOWS\system32\lsass.exe
Ptilink		system32\DRIVERS\ptilink.sys
ql1080		
Ql10wnt		
ql12160		
ql1240		
ql1280		
ql2100		
ql2200		
ql2300		
RasAcd		system32\DRIVERS\rasacd.sys
RasAuto	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
Rasl2tp		system32\DRIVERS\rasl2tp.sys
RasMan	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
RasPppoe		system32\DRIVERS\rasppoe.sys
Raspti		system32\DRIVERS\raspti.sys
Rdbss		system32\DRIVERS\rdbss.sys
RDPCDD		System32\DRIVERS\RDPCDD.sys
rdpdr		system32\DRIVERS\rdpdr.sys
RDPWD		
RDSessMgr	LocalSystem	C:\WINDOWS\system32\sessmgr.exe
redbook		system32\DRIVERS\redbook.sys
RemoteAccess	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
RemoteRegistry	NT AUTHORITY\LocalService	C:\WINDOWS\system32\svchost.exe -k regsvc
RpcLocator	NT AUTHORITY\NetworkService	C:\WINDOWS\system32\locator.exe
RpcSs	LocalSystem	C:\WINDOWS\system32\svchost -k rpcss
RSOProv	LocalSystem	C:\WINDOWS\system32\RSOProv.exe

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Service Name	Logon Name	Path Name
s3legacy		system32\DRIVERS\s3legacy.sys
sacsvr	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
SamSs	LocalSystem	C:\WINDOWS\system32\lsass.exe
SCardSvr	NT AUTHORITY\LocalService	C:\WINDOWS\System32\SCardSvr.exe
Schedule	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
Secdrv		system32\DRIVERS\secdrv.sys
seclogon	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
SENS	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
serenum		system32\DRIVERS\serenum.sys
Serial		system32\DRIVERS\serial.sys
Sfloppy		
SharedAccess	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
ShellHWDetection	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
Simbad		
Sparrow		
Spooler	LocalSystem	C:\WINDOWS\system32\spoolsv.exe
Srv		system32\DRIVERS\srvc.sys
stisvc	NT AUTHORITY\LocalService	C:\WINDOWS\system32\svchost.exe -k imgsvc
swenum		system32\DRIVERS\swenum.sys
swprv	LocalSystem	C:\WINDOWS\System32\svchost.exe -k swprv
sym_hi		
sym_u3		
symc810		
symc8xx		
symmpi		
SysmonLog	NT Authority\NetworkService	C:\WINDOWS\system32\smlogsvc.exe
TapiSrv	LocalSystem	C:\WINDOWS\System32\svchost.exe -k tapisrv
Tcpip		system32\DRIVERS\tcpip.sys
TDPIPE		
TDTCP		
TermDD		system32\DRIVERS\termdd.sys
TermService	LocalSystem	C:\WINDOWS\System32\svchost.exe -k termsvc
Themes	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
TintSvr	NT AUTHORITY\LocalService	C:\WINDOWS\system32\tintsvr.exe
TosIde		
TrkSvr	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
TrkWks	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
Tssdis	LocalSystem	C:\WINDOWS\System32\tssdis.exe
Udfs		
ultra		
Update		system32\DRIVERS\update.sys
uploadmgr	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
UPS	NT AUTHORITY\LocalService	C:\WINDOWS\System32\ups.exe

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Service Name	Logon Name	Path Name
vds	LocalSystem	C:\WINDOWS\System32\vds.exe
VgaSave		\SystemRoot\System32\drivers\vga.sys
Vialde		
VolSnap		\SystemRoot\system32\DRIVERS\volsnap.sys
VPCMap	LocalSystem	C:\Program Files\Virtual Machine Additions\vpcmap.exe
vpc-s3		system32\DRIVERS\vpc-s3.sys
VSS	LocalSystem	C:\WINDOWS\System32\vssvc.exe
W32Time	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
Wanarp		system32\DRIVERS\wanarp.sys
WDICA		
WebClient	NT AUTHORITY\LocalService	C:\WINDOWS\system32\svchost.exe -k LocalService
WinHttpAutoProxySvc	NT AUTHORITY\LocalService	C:\WINDOWS\system32\svchost.exe -k LocalService
wimgmt	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
WLBS		system32\DRIVERS\wlbs.sys
WmdmPmSN	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
Wmi	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs
WmiApSrv	LocalSystem	C:\WINDOWS\system32\wbem\wmiapsrv.exe
wuauerv	LocalSystem	C:\WINDOWS\system32\svchost.exe -k netsvcs
WZCSVC	LocalSystem	C:\WINDOWS\System32\svchost.exe -k netsvcs

### Services and Drivers

A service is an executable object that is installed in a registry database maintained by the Service Control Manager. The executable file associated with a service can be started at boot time by a boot program or by the system, or the Service Control Manager can start it on demand. The two types of service are Win32 services and driver services.

A Win32 service is a service that conforms to the interface rules of the Service Control Manager. This enables the Service Control Manager to start the service at system start-up or on demand and enables communication between the service and service control programs. A Win32 service can execute in its own process, or it can share a process with other Win32 services.

A driver service is a service that follows the device driver protocols for Microsoft Windows rather than using the Service Control Manager interface.

### Implications

Having inappropriate or unnecessary services and drivers installed can create security risks and provide potential access paths or tools to intruders.

There are a great number of services and drivers that can be installed and it would require volumes to document the security implications attached to each one. Some of them will increase security risks if not appropriately configured, controlled and secured. Examples are; **Remote Access Services (RAS)**, Internet related services and network services.

Some of the more common services are:

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

<u>Service</u>	<u>Function</u>	<u>Comments</u>
<b>NetDDE, NetDDEdsdm</b>	Services for creating a communication channel or a trusted share for Windows applications to share data over a network.	Shares (directories, files and printers) should be managed to ensure that sensitive information is not made available unnecessarily via this channel.
<b>EventLog, SENS</b>	Event log Service and System Event Notification Service.	Ensure these services are started to enable the capturing of event messages to the logs.
<b>SNMP, SNMPTRAP</b>	Simple Network Management Protocol to manage devices on a network.	Manage access to information via this protocol, as it can supply valuable information about your network and network devices.
<b>W3SVC, IISADMIN</b>	Internet Information Server and World Wide Web Publishing Service.	Ensure correct configuration of these services as misconfiguration of these can compromise security.
<b>RemoteAccess, Rasman, RasAcD, RasAuto, RasArp</b>	Remote Access services.	Ensure correct configuration of these services as misconfiguration of these can compromise security.
<b>NdisTapi, NdisWan, NetBIOS, NwlnkSpx, Tcpiip</b>	Network Protocol and Transport layer services/drivers.	Ensure that these protocols/drivers are configured correctly as incorrect configuration can leave the network open to penetration.

Attaching unsecured logon accounts to services can create significant security exposures.

Installing driver and service executables in unsecured directories can also create significant security exposures.

### **Risk Rating**

Medium to High (Depending on the type of services installed, their configuration and security settings).

### **Recommended Action**

You should ensure that:

- Only required and appropriate services and drivers are installed and running.
- Their configuration and security settings are to appropriate standards.
- Service and driver executables are in secure directories.
- Logon accounts attached to services have the appropriate security settings to help prevent illegal access.
- The rights and privileges assigned to user accounts, global groups and local groups are effectively controlled (consult report section titled [Rights and Privileges](#)).
- Effective virus detection and prevention services are installed, running and activated/started automatically at system start-up time.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 21. Security Updates, Patches and Hot-Fixes

### Section Summary

There are a total of 1 Security Updates, Patches and Hot-Fixes installed on this system.

### Section Detail

Update Reference	Install Date	Installed By	Service Pack	Description
Q147222				

### Implications

This report section lists hot-fixes installed on the system by Microsoft's hotfix.exe or update.exe utilities.

Note that hot-fixes and patches applied to third-party (non-Microsoft) software products are not included because they are typically not installed by these utilities. Examples of other exclusions are entries written by Shavlik (records are in a proprietary format) and records relating to uninstall routines, such as ServicePackUninstall.

A software patch or hot-fix is a program file that installs one or more files on your system to correct a software problem. A Windows hot-fix program file is typically named KB (or Q) nnnnnn.exe, where nnnnnn is a six-digit number assigned by Microsoft. You can obtain details of a hot-fix by searching Microsoft's Knowledge Base (KB) on the unique hot-fix number.

Many hot-fixes address security vulnerabilities that are discovered in software components, such as Windows, Exchange, Internet Explorer, IIS and SQL.

If you lack a policy to ensure relevant hot-fixes are promptly identified and installed, your system will be exposed to an increased risk of being compromised, damaged or exploited.

Some examples of these security exposures are: unauthorised remote access to your system; illegal execution of code; elevation of privileges; and denial of service attacks.

### Risk Rating

Medium to High (Depending on the vulnerability).

### Recommended Action

You should implement policy to ensure you are aware of newly discovered security vulnerabilities. You should also ensure that appropriate hot-fixes are promptly evaluated and installed on your systems.

Microsoft offers several advisory services and tools that can assist you with the process. These include *Technet*, various notification services and security bulletins, and tools such as *Hfnetchk*, which checks computers for the absence of security patches / hot-fixes.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

## 22. Products Installed

### Section Summary

---

There are a total of 0 MSI-installed software products on this system.

### Section Detail

---

\*\* No data found. This is probably because an older version of the Scan software was used. The analysis of Products installed was introduced in SekChek V5.0.5.\*\*

### Implications

---

This report section lists software products that were installed by Windows Installer (MSI). Unauthorised software installations could cause the following risks:

- Compromised security, if the software does not originate from a reputable vendor or it has not been properly tested prior to implementation.
- Legal action and penalties due to the use of unlicensed software on your systems.
- Additional training and maintenance costs due to the need to support multiple versions of similar software.

### Risk Rating

---

Medium / High (if unauthorised software is installed on your system).

### Recommended Action

---

You should ensure that software policies define a list of approved software and prevent the installation of unauthorised software products. Policies should be consistently enforced and regularly monitored for compliance.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 23. Current Network Connections

### Section Summary

There were a total of 12 active network connections on your system.

### Section Detail

This report provides information regarding the state of processes attached to IP addresses and ports for Current Network Connections. The second report lists [source filenames associated with each process ID](#).

Process ID	Local Address	Local Port	Remote Address	Remote Port	State
0	200.200.100.184	1215	200.200.100.181	445	TIME_WAIT
0	200.200.100.184	1230	200.200.100.181	135	TIME_WAIT
0	200.200.100.184	1231	200.200.100.181	1025	TIME_WAIT
0	200.200.100.184	1232	200.200.100.181	135	TIME_WAIT
0	200.200.100.184	1233	200.200.100.181	1025	TIME_WAIT
0	200.200.100.184	1235	200.200.100.181	389	TIME_WAIT
4	200.200.100.184	1240	200.200.100.181	445	ESTABLISHED
432	200.200.100.184	1218	200.200.100.181	135	ESTABLISHED
432	200.200.100.184	1222	200.200.100.181	1025	ESTABLISHED
432	200.200.100.184	1223	200.200.100.181	1025	ESTABLISHED
432	200.200.100.184	1228	200.200.100.181	1025	ESTABLISHED
432	200.200.100.184	1239	200.200.100.181	1025	ESTABLISHED

### Source Filenames associated with each Process ID

Process ID	Filename
0	Path Unknown
4	Path Unknown
432	C:\WINDOWS\system32\lsass.exe

#### Process ID

The process identification number attached to the Current Network Connection.

#### Local Address

The address of the local end of the socket.

#### Local Port

The port number of the local end of the socket.

#### Remote Address

The address of the remote end of the socket.

#### Remote Port

The port number of the remote end of the socket.

#### State

Shows the connection state of the socket. This can be one of the following values:

CLOSE_WAIT	The remote end has shut down, waiting for the socket to close
CLOSED	The socket is not being used
CLOSING	Both sockets are shut down but we still don't have all our data sent
ESTABLISHED	The socket has an established connection
FIN_WAIT1	The socket is closed and the connection is shutting down
FIN_WAIT2	The connection is closed and the socket is waiting for a shutdown from the remote end
IDLE	Idle, opened but not bound

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

LAST_ACK	The remote end has shut down and the socket is closed. Waiting for acknowledgement
LISTENING	The socket is listening for incoming connections
SYN_RECV	A connection request has been received from the network
SYN_SENT	The socket is actively attempting to establish a connection
TIME_WAIT	The socket is waiting after close to handle packets still in the network
UNKNOWN	The state of the socket is unknown

### Filename

The filename of the process that is attached to the Current Network Connection.

### Implications

This report section lists all active network connections for TCP protocols, including the local and remote addresses, the ports in use and the state of each connection. It does not indicate which services are configured to use these ports.

The port numbers used by some of the most common network services are:

<u>Port number</u>	<u>Service</u>
7	echo
20	ftp data
21	ftp
22	ssh
23	telnet
25	smtp
43	whois
53	DNS
69	tftp
79	finger
80	http
110	POP3
119	nntp
143	IMAP
161	snmp
443	https
512	exec
194	Irc

Network services and their associated ports provide several opportunities for intruders to exploit your system. Some examples are:

- Services such as telnet (port 23) and ftp (port 21) transmit user passwords in clear text format, which makes them vulnerable to access via 'sniffer' software;
- Older versions of services often contain security weaknesses, which can be exploited to gain access to your system using the account under which the service is run;
- Services such as finger (port 79), provide intruders with useful information about your system, such as details of inactive user accounts, which can be used to gain access to your system.

### Risk Rating

Medium to High. (If inappropriate network services are running)

### Recommended Action

You should determine what services are configured to use these ports and:

- Disable any unused or redundant services;
- Limit the number of services that run under the 'administrator' account by running them under an account with less privileges;
- Frequently check with your software vendor for security vulnerabilities in the services you are running and apply any relevant software patches;
- Consider replacing services that transmit passwords in clear text format with more secure software;
- Ensure that hosts running open services are located behind properly configured firewall machines;
- Monitor open ports and connections for signs of unusual activity, particularly from addresses external to your organisation.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

## 24. Domain Controllers in the Domain (DCs only)

### Section Summary

---

\*\*\*This report section only applies to Domain Controllers. There will be no data for Servers or Workstations.\*\*\*

### Section Detail

---

\*\* No data found \*\*

PDC= Primary Domain Controller, BDC = Backup Domain Controller

### Implications

---

A Backup Domain Controller (BDC) is a computer running Windows Server that receives a copy of the domain's security database containing account and security policy information for the domain. The copy is synchronised periodically and automatically with the master copy on the primary domain controller (PDC).

BDCs also authenticate user logons and can be promoted to function as PDCs as needed. Multiple BDCs can exist in a domain.

BDCs provide resilience and add to the effectiveness of the logon process, especially in networks where servers and users are geographically dispersed.

### Risk Rating

---

Low to medium depending on the security standards applied to BDCs.

### Recommended Action

---

You should confirm that the security standards applied to BDCs conform to the security standards on the PDC as they also handle access control to the domain and authenticate users. This is especially true as a BDC can be promoted to a PDC.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 25. Logical Drives

### Section Summary

There were a total of 3 logical drives defined to your system when this analysis was run.

### Section Detail

Drive	Type	Volume Name	Serial Number	File System	Disk Size (MB)	Free Space (MB)
A:\	Removable					
C:\	Fixed		F4FA-0D53	NTFS	4086	2073
D:\	CDROM					

### Implications

The NTFS file system provides more security features than the FAT system. It should be used whenever security is a concern. With NTFS, you can assign a variety of protections to files and directories.

### Risk Rating

Medium to High (Depending on the sensitivity of files and directories).

### Recommended Action

In general, you should ensure that sensitive files and directories are on NTFS partitions.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 26. Network Shares

### Section Summary

There were a total of 4 Network Shares defined to your system when this analysis was run.

### Section Detail

Share Name	Path	Type	Max Uses	Remark
ADMIN\$	C:\WINDOWS	Special Share	*unlimited*	Remote Admin
C\$	C:\	Special Share	*unlimited*	Default share
Confidential	C:\Confidential	File Share	*unlimited*	
IPC\$		Interprocess communication (IPC)	*unlimited*	Remote IPC

### Implications

Windows Server enables you to designate resources you want to share with others. For example:

- When a directory is shared, authorised users can make connections to the directory (and access its files) from their own workstations.
- When a printer is shared, many users can print from it over the network.

Once a resource is shared, you can restrict its availability over the network to certain users. These restrictions, called *share permissions*, can vary from user to user. With Windows Server, you create the appropriate level of security with a combination of resource sharing and resource permissions.

### Risk Rating

Medium to High (Depending on the sensitivity of the data stored in the shared directories).

### Recommended Action

You should ensure that directories containing sensitive data files are not shared or are adequately secured via resource permissions.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 27. Home Directories, Logon Scripts and Logon Profiles

### Section Summary

#### All Accounts

100.0% (3) of user accounts do not have a home directory.  
100.0% (3) of user accounts do not have a logon script.  
100.0% (3) of user accounts are not restricted to logging on from specific workstations.  
100.0% (3) of user accounts do not have specific logon profiles.

#### Excluding Disabled Accounts

66.7% (2) of user accounts do not have a home directory.  
66.7% (2) of user accounts do not have a logon script.  
66.7% (2) of user accounts are not restricted to logging on from specific workstations.  
66.7% (2) of user accounts do not have specific logon profiles.

#### All Administrator Accounts

100.0% (1) of administrator accounts do not have a home directory.  
100.0% (1) of administrator accounts do not have a logon script.  
100.0% (1) of administrator accounts are not restricted to logging on from specific workstations.  
100.0% (1) of administrator accounts do not have specific logon profiles.

#### Administrator Accounts (Excluding Disabled Accounts)

100.0% (1) of administrator accounts do not have a home directory.  
100.0% (1) of administrator accounts do not have a logon script.  
100.0% (1) of administrator accounts are not restricted to logging on from specific workstations.  
100.0% (1) of administrator accounts do not have specific logon profiles.

#### Industry Average Comparison (All Accounts)



### Section Detail

Account Name	Home Directory	Logon Script Path	Workstation Restrictions	Logon Profile	Privilege	Disabled
Administrator	No	No	No	No	Administrator	
SUPPORT_388945a0	No	No	No	No	Guest	Yes
Visitor	No	No	No	No	Guest	

### Implications

A home directory is used as the user's default directory for the 'File Open' and 'Save As' dialog boxes, for the command prompt, and for all applications that do not have a defined working directory.

Home directories make it easier for an administrator to back up user files and delete user accounts because they are grouped in one location. The home directory can be a local directory on a user's computer or a shared network directory, and can be assigned to a single user or many users.

A user's logon script runs automatically every time the user logs on. It can be used to configure a user's working environment at every logon, and allows an administrator to affect a user's environment without managing all its aspects. A logon script can be assigned to one or more user accounts.

In Windows Server, Workstation Restrictions can be used to control the computers from which a user is allowed to log on. The alternative is to allow a user to logon from any computer.

Restricting the workstations a user can use to log on to your system can improve security and discourage potential hackers. This is especially true for sensitive accounts.

A user profile defines the Microsoft Windows configuration for a specific user or group of users.

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

By default, and with the exception of Guest accounts, each Windows computer maintains a profile for each user who has logged on to the computer. A profile contains information about a user's Windows configuration. Much of this information controls options the user can set, such as colour scheme, screen savers, and mouse and keyboard layout.

Other information control options that can be set only by a Windows administrator include access to common program groups or network printers.

A value of *Yes* in the *Account Disabled* column indicates that the account has been disabled by a security administrator, is locked due to excessive failed login attempts, or has expired. See [Disabled Accounts](#) for details.

### Risk Rating

---

Medium to Low.

### Recommended Action

---

To minimise potential loss of data and ease administration, users should have defined home directories, which can be regularly backed up.

To ease administration and afford better control over user environments, each user should have a logon script.

You should consider the additional benefits in security that workstation restrictions can provide. It is particularly suited to those environments with high security needs or very sensitive systems and information.

You should consider the benefits of defining logon profiles for users. This can ease administration and enhance security.

# Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

## 28. File Permissions and Auditing

### Section Summary

This report section details the permissions and audit settings for 3 predefined and 2 user selected directories/files on your system.

### Section Detail

For details please see table [Permissions](#) in the MS-Access database.

### Implications

This report section lists the owner and access permissions (DACL) for selected files and directories. It also lists the audit settings (SACL) for files and directories.

More specifically, the report section lists the contents of each Access Control Entry (ACE) in the file or directory's Discretionary Access Control List (DACL). A DACL contains one or more ACEs that control access to the associated resource.

An ACE in a DACL can *Allow* or *Deny* access to a resource. A *Deny* ACE always overrides an *Allow* ACE.

The report section also lists the contents of each Access Control Entry (ACE) in the file or directory's System Access Control List (SACL). A SACL contains one or more ACEs that define what actions on the object are audited (e.g. deletion of a file and changes to a folder's permissions). The event types are *Success* and *Failure*.

#### Legend:

Resource Name	The name of the resource being analysed.
Resource Type	The type of resource being analysed. At present the only resource types analysed by SekChek are files and directories.
ACL Type	The type of ACL being analysed: a DACL or a SACL.
Owner	The owner of the resource.
Owner Domain	The resource owner's domain.
Owner Account Type	The owner's account type. E.g. Alias, User.
Ace Nbr	The sequential number of the ACE. Window's reads ACEs in this order until it finds a <i>Deny</i> or <i>Allow</i> ACE that denies or permits access to the resource or an <i>Audit</i> ACE that defines what is audited and the event type.
Account	The name of the account to which this ACE applies.
Domain	The account's domain.
Account Type	The type of the account. E.g. Alias, User, Group.
Ace Type	<i>Allow</i> or <i>Deny</i> access to the resource in the case of an ACE in a DACL; <i>Success</i> or <i>Failure</i> events for a SACL.
Apply Onto	Specifies where permissions or auditing are applied. These values are shown as they appear in the Windows' property box. E.g.: <ul style="list-style-type: none"><li>• This folder / object only</li><li>• This folder, subfolders &amp; files</li><li>• This folder &amp; subfolders</li><li>• This folder &amp; files</li><li>• Subfolders &amp; files only</li><li>• Subfolders only</li><li>• Files only</li></ul>
Inherited	Indicates whether the permissions or audit settings are inherited from a higher level.

#### Special Permissions (ACE in a DACL):

Traverse Folder / Execute File **For folders:** Traverse Folder allows or denies moving through folders to reach other files or folders, even if the user has no permissions for the traversed

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

---

	<p>folders (applies to folders only). Traverse folder takes effect only when the group or user is not granted the <b>Bypass traverse checking</b> user right in the Group Policy snap-in. (By default, the Everyone group is given the <b>Bypass traverse checking</b> user right.).</p> <p><b>For files:</b> Execute File allows or denies running program files (applies to files only).</p> <p>Setting the Traverse Folder permission on a folder does not automatically set the Execute File permission on all files within that folder.</p>
List Folder / Read Data	<p>List Folder allows or denies viewing file names and subfolder names within the folder. List Folder only affects the contents of that folder and does not affect whether the folder you are setting the permission on will be listed. Applies to folders only.</p> <p>Read Data allows or denies viewing data in files (applies to files only).</p>
Read Attributes	<p>Allows or denies viewing the attributes of a file or folder, such as read-only and hidden. Attributes are defined by NTFS.</p>
Read Extended Attributes	<p>Allows or denies viewing the extended attributes of a file or folder. Extended attributes are defined by programs and may vary by program.</p>
Create Files / Write Data	<p>Create Files allows or denies creating files within the folder (applies to folders only).</p> <p>Write Data allows or denies making changes to the file and overwriting existing content (applies to files only).</p>
Create Folders / Append Data	<p>Create Folders allows or denies creating folders within the folder (applies to folders only).</p> <p>Append Data allows or denies making changes to the end of the file but not changing, deleting, or overwriting existing data (applies to files only).</p>
Write Attributes	<p>Allows or denies changing the attributes of a file or folder, such as read-only or hidden. Attributes are defined by NTFS.</p> <p>The Write Attributes permission does not imply creating or deleting files or folders, it only includes the permission to make changes to the attributes of a file or folder. In order to allow (or deny) create or delete operations, see <b>Create Files/Write Data</b>, <b>Create Folders/Append Data</b>, <b>Delete Subfolders and Files</b>, and <b>Delete</b>.</p>
Write Extended Attributes	<p>Allows or denies changing the extended attributes of a file or folder. Extended attributes are defined by programs and may vary by program.</p> <p>The Write Extended Attributes permission does not imply creating or deleting files or folders, it only includes the permission to make changes to the attributes of a file or folder. In order to allow (or deny) create or delete operations, see <b>Create Files/Write Data</b>, <b>Create Folders/Append Data</b>, <b>Delete Subfolders and Files</b>, and <b>Delete</b>.</p>
Delete Subfolders And Files	<p>Allows or denies deleting subfolders and files, even if the Delete permission has not been granted on the subfolder or file. (applies to folders)</p>
Delete	<p>Allows or denies deleting the file or folder. If you don't have Delete permission on a file or folder, you can still delete it if you have been granted Delete Subfolders and Files on the parent folder.</p>
Read Permissions	<p>Allows or denies reading permissions of the file or folder, such as Full Control, Read, and Write.</p>
Change Permissions	<p>Allows or denies changing permissions of the file or folder, such as Full Control, Read, and Write.</p>
Take Ownership	<p>Allows or denies taking ownership of the file or folder. The owner of a file or folder can always change permissions on it, regardless of any existing permissions that protect the file or folder.</p>
File Synchronise	<p>Allows or denies different threads to wait on the handle for the file or folder and synchronize with another thread that may signal it. This permission applies only to multithreaded, multiprocess programs.</p>

## Security Analysis: TESTBED Win2003 Server

System: PROMETHEUS (OLYMPUS)  
Analysis Date: 06-Sep-2010

CONFIDENTIAL

Windows' special permissions are logically grouped to form generic permissions: Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write.

The following table illustrates how special permissions are grouped together into these higher-level generic permissions.

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

### Risk Rating

High (if access permissions are inappropriate and allow unintended access to sensitive resources).

### Recommended Action

You should:

- Periodically check access permissions for sensitive files and directories to ensure they remain appropriate and reflect the requirements of a person's job function.
- Ensure that all changes to access permissions are properly authorised by management.
- Consider logging audit events for sensitive files and directories. Note that large numbers of audit log entries may be generated for frequently accessed files and directories.