

C13 - Establishing a Windows Baseline

Mike Villegas



September 21, 2009 – September 23, 2009

Windows Security Baselines

Presented by
Miguel (Mike) O. Villegas, CISA, CISSP
Session # C13



September 21, 2009 – September 23, 2009



Agenda

- ❖ INTRODUCTION TO WINDOWS
- ❖ MICROSOFT BASELINE SECURITY ANALYZER – MBSA
- ❖ WINDOWS SERVER SECURITY OVERVIEW
- ❖ WINDOWS SERVER INDUSTRY STANDARDS
- ❖ TRIPWIRE TO TEST CIS BASELINE
- ❖ SAMPLE BASELINE TYPES
- ❖ WINDOWS SERVER 2003 BASELINE EXAMPLE
 - ❖ GO THROUGH BASELINES
 - ❖ IDENTIFY SERVER TYPE DIFFERENCES
 - ❖ DISCUSS ISSUES
- ❖ SUMMARY



Introduction to Windows

Desktop Products

- ❖ Windows 1.0 and later
- ❖ Windows 95, Windows 98, Windows Me, Windows 2000
- ❖ Windows XP Tablet PC Edition
- ❖ Windows XP Media Center Edition
- ❖ Windows XP Home
- ❖ Windows XP Professional
- ❖ Windows Vista

Server Products

- ❖ Windows NT Server
- ❖ Windows 2000 Server Family
- ❖ Windows Server 2003 Family
- ❖ Windows Home Server
- ❖ Windows Server 2008

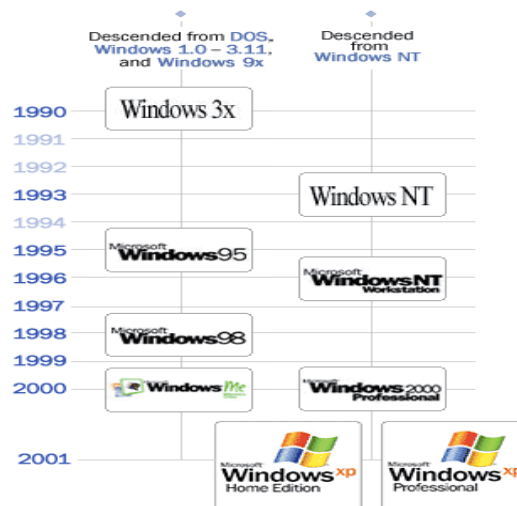
This session will focus on the server products only

CONVERGENCE

3

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Windows Desktop Timeline

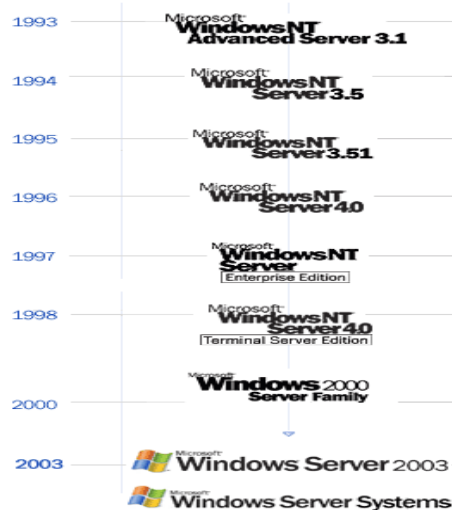


CONVERGENCE

4

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Windows Server Timeline



CONVERGENCE

5

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Benefits of a Baseline

- ❖ Automates the set up a new machine.
- ❖ Includes:
 - ❖ installing software,
 - ❖ applying operating system security updates,
 - ❖ applying local security policy settings, and
 - ❖ configuring automatic update settings.
- ❖ As configurations change, baselines can keep machines in compliance.
- ❖ Make it easier to trouble shoot and maintain systems on a timely and consistent manner.
- ❖ Security baselines allow companies to stay in compliance with:
 - ❖ industry standards and
 - ❖ maintain a reasonable level of assurance and security.

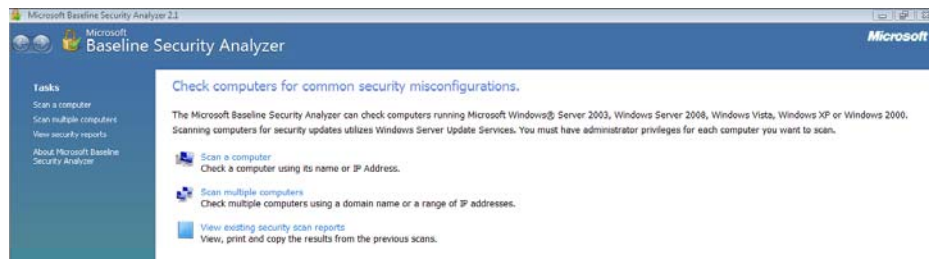
CONVERGENCE

6

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Microsoft Baseline Security Analyzer

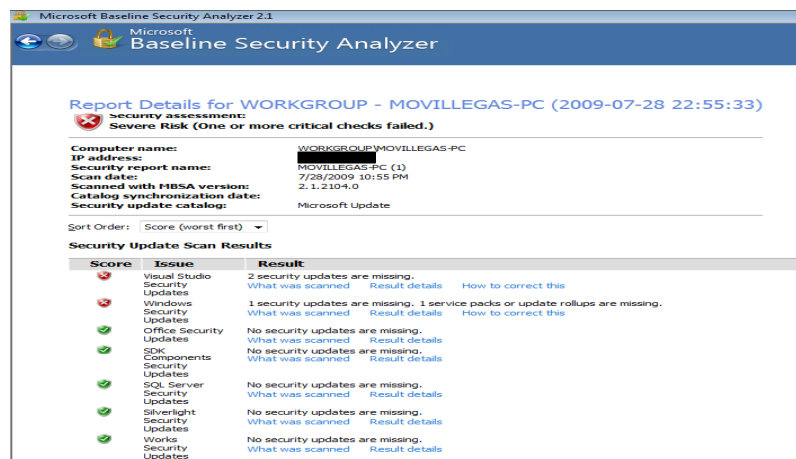
<http://technet.microsoft.com/en-us/security/cc184924.aspx>



7



MSBA – Scan a Computer



8



MSBA – Scan a Computer

Microsoft Baseline Security Analyzer 2.1

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
❌	File System	Not all hard drives are using the NTFS file system. What was scanned Result details How to correct this
⚠️	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details How to correct this
⚠️	Password Expiration	Some user accounts (5 of 6) have non-expiring passwords. What was scanned Result details How to correct this
⚠️	Incomplete Updates	No incomplete software update installations were found. What was scanned
⚠️	Windows Firewall	Windows Firewall is managed through Group Policy on this computer. Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
✅	Local Account Password Test	Some user accounts (2 of 6) have blank or simple passwords, or could not be analyzed. What was scanned Result details
✅	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned
✅	Autologon	Autologon is not configured on this computer. What was scanned
✅	Guest Account	The Guest account is disabled on this computer. What was scanned
✅	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned

Additional System Information

Score	Issue	Result
⚠️	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access. What was scanned How to correct this
⚠️	Services	No potentially unnecessary services were found. What was scanned
⚠️	Shares	12 share(s) are present on your computer. What was scanned Result details How to correct this
⚠️	Windows Version	Computer is running Microsoft Windows Vista. What was scanned



9



MSBA – Scan a Computer

Internet Information Services (IIS) Scan Results

Score	Issue	Result
❌	IIS Status	IIS is not running on this computer.

SQL Server Scan Results

Score	Issue	Result
❌	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✅	IE Zones	Internet Explorer zones have secure settings for all users. What was scanned
❌	Macro Security	No supported Microsoft Office products are installed.



10



Windows Server 2003 Overview

- ❖ Authentication
 - ❖ *Interactive logon*
 - ❖ *Network authentication*
- ❖ Object-based access control
- ❖ Security policy
- ❖ Auditing
- ❖ Active Directory and security
- ❖ Data protection
- ❖ Encrypting File System (EFS)
- ❖ Network data protection
- ❖ Routing and Remote Access
- ❖ Internet Authentication Service (IAS)
- ❖ Public key infrastructure



11



Windows Server 2008 Overview

- ❖ AppLocker
- ❖ Authorization Manager
- ❖ BitLocker Drive Encryption
- ❖ Encrypting File System
- ❖ Encrypting File System (EFS)
- ❖ Kerberos
- ❖ Security Auditing
- ❖ Security Configuration Wizard
- ❖ Server Security Policy Management
- ❖ User Account Control
- ❖ Windows Authentication



12



Windows Server Industry Standards

- ❖ Center for Internet Security (CIS)
www.cisecurity.org
- ❖ National Institute of Standards and Technology (NIST)
<http://csrc.nist.gov/cc/> - Common Criteria Project (**obsolete**)
- ❖ National Security Agency (NSA) – NIAP CCEVS
<http://www.niap-ccevs.org/cc-scheme/>
- ❖ SysAdmin Audit Network Security (SANS)
www.sans.org – provided in courses
- ❖ Your Own



13

The screenshot shows the homepage of the Center for Internet Security (CIS). The header includes the CIS logo, the text "the CENTER for INTERNET SECURITY", the website URL "www.cisecurity.org", and navigation links for "SITE MAP", "CONTACT US", and "PRIVACY POLICY". Below the header is a main navigation bar with links: "HOME", "WHAT'S NEW", "WHAT IS CIS?", "BENCHMARKS/TOOLS", "OTHER RESOURCES", "JOIN US", "TESTIMONIALS", and "FAQ". The main content area is divided into three columns. The left column contains a "Members Site" section with links to "Become a CIS member!", "CIS Members Worldwide", "Find Out How To Get Involved!", "US Federal government agency license.", "CIS certifies commercial software.", "CIS licenses resources for commercial use.", and "CIS Trademarks & Logos". The middle column contains sections for "Measurably reducing risk through collaboration, consensus & practical security management", "DOWNLOAD FREE OF CHARGE" (40 consensus Security Configuration Benchmarks), "CIS Configuration Benchmark Scoring Tools", and "Consensus Based Metrics for Information Security". The right column contains an "ANNOUNCEMENTS" section with links to "GETTING TO A USEFUL SET OF SECURITY METRICS", "CIS MEMBER AND DEVELOPER UPDATE", "CIS WEB EVENT: CIS web event on Configuration Management - What Is It and How Do You Document It?", and "CIS WEB EVENT ON PROTECTING INFORMATION".



14



CIS Trademarks & Logos
Click here for more info >>

Upcoming CIS-Related Presentations
Click here for more info >>

CIS Benchmarks/Scoring Tools Now Available, Free of Charge!

Operating Systems		
Benchmark	Version	Updated
AIX	1.01	10/21/2005
Debian Linux	1.0	08/17/2007
FreeBSD	1.0.5	10/21/2005
HP-UX	1.4.2	06/03/2008
Mac OS X 10.4 (Tiger)	2.0	10/16/2006
Mac OS X 10.5 (Leopard)	1.0	05/21/2008
Novell OES/NetWare	1.0	08/14/2006
Red Hat Linux 4 (for RHEL 2.1, 3.0, 4.0 and Fedora Core 1,2,3,4, & 5)	1.0.5	10/01/2006
Red Hat Linux 5 (for RHEL 5)	1.1.2	06/17/2009
Slackware Linux	1.1	06/16/2006
Solaris 2.5.1 - 9.0	1.3	08/11/2004
Solaris 10 11/06 and 8/07	4.0	11/01/2007
SUSE Linux	2.0	05/21/2008
Windows 2000	1.2.2	02/04/2005
Windows 2000 Professional	2.2.1	12/17/2004
Windows 2000 Server	2.2.1	12/17/2004
Windows NT	1.05	03/04/2005
Windows Server 2003	2.0	11/21/2007
Windows XP Professional SP1/SP2	2.01	09/09/2005
Network Devices		
Check Point Firewall	1.0	12/11/2007
Cisco ASA, FWSM, and PIX	2.0	11/20/2007
Cisco IOS Router	2.2	11/20/2007
Multi-Function Devices	1.0.0	04/24/2009
Wireless Networks	1.0	04/14/2005
Applications		
Apache Web Server	2.2.0	11/10/2008
Exchange Server 2003	1.0	08/15/2005
Exchange Server 2007	1.0	12/31/2007
FreeRADIUS	1.0	08/16/2007
ISC	1.0	08/16/2007

15

CIS Benchmark Documents

Name

- CIS_Benchmark_Exchange2007_1.0
- CIS_Cisco_Firewall_Benchmark_v2.0
- CIS_Cisco_IOS_Benchmark_v2.2
- CIS_Exchange2003_Benchmark_v1.0
- CIS_IIS_Benchmark_v1.0
- CIS_Security_Metrics_v1.0.0
- CIS_SQL2000_Benchmark_v1.0
- CIS_SQL2005_Benchmark_v1.1
- CIS_Win2K_Level-1_Benchmark_v1.2.2
- CIS_Win2K_Pro_Benchmark_v2.2.1
- CIS_Win2K_Srv_Benchmark_v2.2.1
- CIS_Win2003_DC_Benchmark_v2.0
- CIS_Win2003_MS_Benchmark_v2.0
- CIS_WindowsXP_Benchmark_v2.01
- CIS_Wireless_Addendum_Apple
- CIS_Wireless_Addendum_Cisco
- CIS_Wireless_Addendum_DLink
- CIS_Wireless_Addendum_Linksys
- CIS_Wireless_Assessment4_Example_v2.0
- CIS_Wireless_Assessment_v2.0
- CIS_Wireless_Benchmark_v1.0
- cisco-ios-router-benchmark
- cisco-ios-router-questionnaire
- CIS-WinNT-v1.0.5

Section 1 – Summary Checklist

Setting:	Legacy	Enterprise	Specialized Security – Limited Functionality
1 Service Packs and Hotfixes			
1.1 Major Service Pack and Hotfix Requirements			
1.1.1 Current Service Pack Installed		SP2	
1.2 Minor Service Pack and Hotfix Requirements			
1.2.1 Hotfixes recognized by HFSetChk		All Critical and Important Hotfixes	
2 Auditing and Account Policies			
2.1 Major Auditing and Account Policies Requirements			
2.1.1 Minimum Password Length	8 Characters	42 Days	12 Characters
2.1.2 Maximum Password Age			
2.2 Minor Auditing and Account Policies Requirements			
2.2.1 Audit Policy (minimum)			
2.2.1.1 Audit Account Logon Events		Success and Failure	
2.2.1.2 Audit Account Management		Success and Failure	
2.2.1.3 Audit Directory Service Access		<Not Defined>	
2.2.1.4 Audit Logon Events		Success and Failure	
2.2.1.5 Audit Object Access		Success and Failure	
2.2.1.6 Audit Policy Change		Success (minimum)	
2.2.1.7 Audit Privilege Use		<Not Defined>	
2.2.1.8 Audit Process Tracking		<Not Defined>	
2.2.1.9 Audit System Events		Success (minimum)	
2.2.2 Account Policy			
2.2.2.1 Minimum Password Age		1 day	
2.2.2.2 Maximum Password Age		42 days	
2.2.2.3 Minimum Password Length	8 characters		12 characters
2.2.2.4 Password Complexity		Enabled	
2.2.2.5 Password History		24 passwords remembered	
2.2.2.6 Store Passwords using Reversible Encryption		Disabled	

Page 10 of 122

www.cisecurity.org

16

Tripwire

Detailed Test Inventory - Windows Servers PCI Mappings

Date: 12/10/08 9:53 AM
Descend test groups: Yes
Display criteria at end: No
Show full details: Yes
Weight: All
Test Severity range: All
Tests: MS Windows Server 2003 DM Data Security Standard Mapping - PCI v1.1

MS Windows Server 2003 DM Data Security Standard Mapping - PCI v1.1

(Generated 21:15 13 Oct 2008)

Requirement 2 Security Parameters

Do not use vendor-supplied defaults for system passwords and other security parameters

2.2 Develop Configuration Standards for All System Components. Assure That These Standards Address All Known Security Vulnerabilities and Are Consistent with Industry-accepted System Hardening Standards as Defined

2.2.0 Tests

2.2.0.1 Maximum Password Age



17



Tripwire

Maximum Password Age Is Greater than 0 and Less than or Equal to 42

Description	This test verifies that the password policy on this system is configured to require passwords that are greater than 0 and less than or equal to 42 days old. Changing passwords regularly helps to prevent unauthorized users from gaining access to the system.
Type	Attribute Test
Severity	0
Rules	Local Machine RSOP
Element	Equals (case insensitive) "Computer"
Version conditions	Action if missing: Fail MaximumPasswordAge Exists AND MaximumPasswordAge Greater than 0 AND MaximumPasswordAge Less than or equal 42
Weight	1
Remediation	To remediate failure of this policy test, configure the password policy to use a maximum password age that is greater than 0 and less than or equal to 42. Modifying the password policy on Windows 2003: <ol style="list-style-type: none"> 1. Select a group policy object to edit in the Microsoft Management Console. 2. Select Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy. 3. Right-click Maximum password age and select Properties. 4. Select Define this policy setting and in the Password can be changed after: box, enter an integer value that is greater than 0 and less than or equal to 42, then click OK. 5. Run the gpupdate command to apply the change. Note: <ul style="list-style-type: none"> • To perform this procedure you must be a domain administrator. • Tests may continue to fail until the domain refreshes the setting configured above. • When you change a security setting and click OK, that setting will take effect in the next refresh of settings, or after reboot. • The security settings are refreshed every 90 minutes on a workstation or server and every 5 minutes on a domain controller. The settings are also refreshed every 16 hours, whether or not there are any changes. For further details, please refer to: http://technet2.microsoft.com/windowsserver/en/library/039e0d42-fe50-4738-abf3-c798e74a03f61033.mspx?mfr=true



18



Tripwire

MS Windows Server 2000 Data Security Standard Mapping - PCI v1.1

(Generated 21:15 13 Oct 2008)

Requirement 2 Security Parameters

Do not use vendor-supplied defaults for system passwords and other security parameters

2.2 Develop Configuration Standards for All System Components. Assure That These Standards Address All Known Security Vulnerabilities and Are Consistent with Industry-accepted System Hardening Standards as Defined

2.2.0 Tests

2.2.0.1 Minimum Password Length

Minimum Password Length Is Greater than or Equal to 8

This test verifies that the password policy on this system is configured to require passwords of 8 or more characters. Using passwords of this length helps to protect the system from password guessing attacks.

Node	Element	Result	Time	Actual
(Windows Server)	Computer	Failed	1/23/09 12:47 PM	MinimumPasswordLength=0
(Windows Server)	Computer	Failed	1/23/09 12:47 PM	MinimumPasswordLength=0
(Windows Server)	Computer	Failed	1/23/09 12:47 PM	MinimumPasswordLength=0



19



Sample Baseline Types

Security Baseline for Ecommerce Servers

FOR Windows Server 2003 Operating System

Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
----------	-------------	------	-------------	---------------

Security Baseline for Servers in Card Holder Environment

FOR Windows Server 2003 Operating System

Setting:	Data Center Servers	AntiVirus Servers	Bridge Servers	DB Management Servers
Setting:	ABS Application Servers	Oversea Servers	Payment Servers	SO Application Servers
Setting:	Role Management Servers	Mercury Domain Controller	Backup Exec Servers	

You may need to do the same for Windows 2000 and Windows 2008.



20



Security Baseline for Ecommerce Servers

FOR Windows Server 2003 Operating System

Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
1 Service Packs and Hotfixes				
1.1 Major Service Pack and Hotfix Requirements				
1.1.1 Current Service Pack Installed	Service Pack 2	Service Pack 2	Service Pack 2	Service Pack 2
1.2 Minor Service Pack and Hotfix Requirements				
1.2.1 Hotfixes recognized by HFNetchk	All Critical and Important Hotfixes	All Critical and Important Hotfixes	All Critical and Important Hotfixes	All Critical and Important Hotfixes
2 Auditing and Account Policies				
2.2.1 Audit Policy (minimums)				
2.2.1.1 Audit Account Logon Events	Success and Failure	Success and Failure	Success and Failure	Success and Failure
2.2.1.2 Audit Account Management	Success and Failure	Success and Failure	Success and Failure	Success and Failure
2.2.1.3 Audit Directory Service Access	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
2.2.1.4 Audit Logon Events	Success and Failure	Success and Failure	Success and Failure	Success and Failure
2.2.1.5 Audit Object Access	Success and Failure	Success and Failure	Success and Failure	Success and Failure
2.2.1.6 Audit Policy Change	Success and Failure	Success and Failure	Success and Failure	Success and Failure
2.2.1.7 Audit Privilege Use	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
2.2.1.8 Audit Process Tracking	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
2.2.1.9 Audit System Events	Success and Failure	Success and Failure	Success and Failure	Success and Failure
2.2.2 Account Policy				
2.2.2.1 Minimum Password Age	1 day	1 day	1 day	1 day
2.2.2.2 Maximum Password Age	42 days	42 days	42 days	42 days
2.2.2.3 Minimum Password Length	8 characters	8 characters	8 characters	8 characters
2.2.2.4 Password Complexity	Enabled	Enabled	Enabled	Enabled
2.2.2.5 Password History	24 passwords	24 passwords	24 passwords	24 passwords
2.2.2.6 Store Passwords using Reversible Encryption	Disabled	Disabled	Disabled	Disabled



Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
2.2.3 Account Lockout Policy				
2.2.3.1 Account Lockout Duration	15 minutes	15 minutes	15 minutes	15 minutes
2.2.3.2 Account Lockout Threshold	15 attempts	15 attempts	15 attempts	15 attempts
2.2.3.3 Reset Account Lockout After	15 minutes	15 minutes	15 minutes	15 minutes
2.2.4 Event Log Settings – Application, Security, and System Logs				
2.2.4.1 Application Log				
2.2.4.1.1 Maximum Event Log Size	16 MB	16 MB	16 MB	16 MB
2.2.4.1.2 Restrict Guest Access	Enabled	Enabled	Enabled	Enabled
2.2.4.1.3 Log Retention Method	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
2.2.4.1.4 Log Retention	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
2.2.4.2 Security Log				
2.2.4.2.1 Maximum Event Log Size	80 MB	80 MB	80 MB	80 MB
2.2.4.2.2 Restrict Guest Access	Enabled	Enabled	Enabled	Enabled
2.2.4.2.3 Log Retention Method	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
2.2.4.2.4 Log Retention	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
2.2.4.3 System Log				
2.2.4.3.1 Maximum Event Log Size	16 MB	16 MB	16 MB	16 MB
2.2.4.3.2 Restrict Guest Access	Enabled	Enabled	Enabled	Enabled
2.2.4.3.3 Log Retention Method	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
2.2.4.3.4 Log Retention	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3 Security Settings				
3.1 Major Security Settings				
3.1.1 Network Access: Allow Anonymous SID/Name Translation	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.1.2 Network Access: Do not allow Anonymous Enumeration of SAM Accounts	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.1.3 Network Access: Do not allow Anonymous Enumeration of SAM Accounts and Shares	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2 Minor Security Settings				
3.2.1 Security Options				





Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
3.2.1.1 Accounts: Administrator Account Status	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.2 Accounts: Guest Account Status	Disabled	Disabled	Disabled	Disabled
3.2.1.3 Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled	Enabled	Enabled
3.2.1.4 Accounts: Rename Administrator Account	Non-standard Name with reference to Newegg User Matrix	Non-standard Name with reference to Newegg User Matrix	Non-standard Name with reference to Newegg User Matrix	Non-standard Name with reference to Newegg User Matrix
3.2.1.5 Accounts: Rename Guest Account	Non-standard Name with reference to Newegg User Matrix	Non-standard Name with reference to Newegg User Matrix	Non-standard Name with reference to Newegg User Matrix	Non-standard Name with reference to Newegg User Matrix
3.2.1.6 Audit: Audit the access of global system objects	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.7 Audit: Audit the use of backup and restore privilege	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.8 Audit: Shut Down system immediately if unable to log security alerts	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.9 DCOM: Machine Access Restrictions in Security Descriptor Definition Language	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.10 DCOM: Machine Launch Restrictions in Security Descriptor Definition Language	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.11 Devices: Allow undock without having to log on	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.12 Devices: Allowed to format and eject removable media	Administrators	Administrators	Administrators	Administrators
3.2.1.13 Devices: Prevent users from installing printer drivers	Enabled	Enabled	Enabled	Enabled
3.2.1.14 Devices: Restrict CD-ROM Access to Locally Logged-On User Only	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.15 Devices: Restrict Floppy Access to Locally Logged-On User Only	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.16 Devices: Unsigned Driver	"Warn, but allow..."	"Warn, but allow..."	"Warn, but allow..."	"Warn, but allow..."

Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
Installation Behavior				
3.2.1.17 Domain Controller: Allow Server Operators to Schedule Tasks	<Not Applicable>	<Not Applicable>	<Not Applicable>	<Not Applicable>
3.2.1.18 Domain Controller: LDAP Server Signing Requirements	<Not Applicable>	<Not Applicable>	<Not Applicable>	<Not Applicable>
3.2.1.19 Domain Controller: Refuse machine account password changes	<Not Applicable>	<Not Applicable>	<Not Applicable>	<Not Applicable>
3.2.1.20 Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always)	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.21 Domain Member: Digitally Encrypt Secure Channel Data (When Possible)	Enabled	Enabled	Enabled	Enabled
3.2.1.22 Domain Member: Digitally Sign Secure Channel Data (When Possible)	Enabled	Enabled	Enabled	Enabled
3.2.1.23 Domain Member: Disable Machine Account Password Changes	Disabled	Disabled	Disabled	Disabled
3.2.1.24 Domain Member: Maximum Machine Account Password Age	30 days	30 days	30 days	30 days
3.2.1.25 Domain Member: Require Strong (Windows 2000 or later) Session Key	Enabled	Enabled	Enabled	Enabled
3.2.1.26 Interactive Logon: Do Not Display Last User Name	Enabled	Enabled	Enabled	Enabled
3.2.1.27 Interactive Logon: Do not require CTRL+ALT+DEL	Disabled	Disabled	Disabled	Disabled
3.2.1.28 Interactive Logon: Message Text for Users Attempting to Log On	"This machine is protected by IT. Please do NOT touch it unless u have written notice from IT"	"This machine is protected by IT. Please do NOT touch it unless u have written notice from IT"	"This machine is protected by IT. Please do NOT touch it unless u have written notice from IT"	"This machine is protected by IT. Please do NOT touch it unless u have written notice from IT"
3.2.1.29 Interactive Logon: Message Title for Users Attempting to Log On	"This machine is protected by IT. Pls do NOT touch it unless u have written notice from IT"	"This machine is protected by IT. Pls do NOT touch it unless u have written notice from IT"	"This machine is protected by IT. Pls do NOT touch it unless u have written notice from IT"	"This machine is protected by IT. Pls do NOT touch it unless u have written notice from IT"



Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
3.2.1.30 Interactive Logon: Number of Previous Logons to Cache	<Not Defined>	from IT"	from IT"	IT"
3.2.1.31 Interactive Logon: Prompt User to Change Password Before Expiration	14 days	14 days	14 days	14 days
3.2.1.32 Interactive Logon: Require Domain Controller authentication to unlock workstation	Enabled.	Enabled.	Enabled.	Enabled.
3.2.1.33 Interactive logon: Require smart card	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.34 Interactive Logon: Smart Card Removal Behavior	Lock Workstation	Lock Workstation	Lock Workstation	Lock Workstation
3.2.1.35 Microsoft Network Client: Digitally sign communications (always)	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.36 Microsoft Network Client: Digitally sign communications (if server agrees)	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.37 Microsoft Network Client: Send Unencrypted Password to Connect to Third-Part SMB Server	Disabled	Disabled	Disabled	Disabled
3.2.1.38 Microsoft Network Server: Amount of Idle Time Required Before Disconnecting Session	15 Minutes	15 Minutes	15 Minutes	15 Minutes
3.2.1.39 Microsoft Network Server: Digitally sign communications (always)	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.40 Microsoft Network Server: Digitally sign communications (if client agrees)	Enabled	Enabled	Enabled	Enabled
3.2.1.41 Microsoft Network Server: Disconnect clients when logon hours expire	Enabled	Enabled	Enabled	Enabled
3.2.1.42 Network Access: Do not allow storage of credentials or .NET passports for network authentication	Enabled.	Enabled.	Enabled.	Enabled.
3.2.1.43 Network Access: Let Everyone permissions apply to anonymous users	Disabled	Disabled	Disabled	Disabled
3.2.1.44 Network Access: Named pipes that can be accessed anonymously	<None>	<None>	<None>	<None>

Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
3.2.1.45 Network Access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion
3.2.1.46 Network Access: Remotely accessible registry paths and subpaths	Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfig	Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfig	Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfig	Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\DefaultUserConfig


Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
	lation Software\Microsoft\Windows NT\CurrentVersion\PerfLib System\CurrentControlSet\Services\SysmonLog	Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\PerfLib System\CurrentControlSet\Services\SysmonLog	Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\PerfLib System\CurrentControlSet\Services\SysmonLog	uration Software\Microsoft\Windows NT\CurrentVersion\PerfLib System\CurrentControlSet\Services\SysmonLog
3.2.1.4 / Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	Enabled	Enabled	Enabled
3.2.1.48 Network Access: Shares that can be accessed anonymously	<None>	<None>	<None>	<None>
3.2.1.49 Network Access: Sharing and security model for local accounts	Classic	Classic	Classic	Classic
3.2.1.50 Network Security: Do not store LAN Manager password hash value on next password change	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.51 Network Security: Force logoff when logon hours expire	Enabled	Enabled	Enabled	Enabled
3.2.1.52 Network Security: LAN Manager Authentication Level	Send NTLMv2	Send NTLMv2	Send NTLMv2	Send NTLMv2
3.2.1.53 Network Security: LDAP client signing requirements	Negotiate Signing or Require Signing	Negotiate Signing or Require Signing	Negotiate Signing or Require Signing	Negotiate Signing or Require Signing
3.2.1.54 Network Security: Minimum session security for NTLM SSP based (including secure RPC) clients	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.55 Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>


Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
3.2.1.56 Recovery Console: Allow Automatic Administrative Logon	Disabled	Disabled	Disabled	Disabled
3.2.1.57 Recovery Console: Allow Floppy Copy and Access to All Drives and All Folders	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.58 Shutdown: Allow System to be Shut Down Without Having to Log On	Disabled	Disabled	Disabled	Disabled
3.2.1.59 Shutdown: Clear Virtual Memory	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.60 System cryptography: Force strong key protection for user keys stored on the computer	User must enter a password each time they use a key	User must enter a password each time they use a key	User must enter a password each time they use a key	User must enter a password each time they use a key
3.2.1.61 System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.62 System objects: Default owner for objects created by members of the Administrators group	Object Creator	Object Creator	Object Creator	Object Creator
3.2.1.63 System objects: Require case insensitivity for non-Windows subsystems	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.64 System objects: Strengthen default permissions of internal system objects	Enabled	Enabled	Enabled	Enabled
3.2.1.65 System settings: Optional subsystems	<None>	<None>	<None>	<None>
3.2.1.66 System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.67 MSS: (AFD DynamicBacklogGrowthDelta) Number of connections to create when additional connections are necessary for Winsock applications (10 recommended)	10	10	10	10
3.2.1.68 MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for Winsock applications	Enabled	Enabled	Enabled	Enabled


Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
(recommended)				
3.2.1.69 MSS: (AFD MaximumDynamicBacklog) Maximum number of 'quasi-free' connections for Winsock applications	20000	20000	20000	20000
3.2.1.70 MSS: (AFD MinimumDynamicBacklog) Minimum number of free connections for Winsock applications (20 recommended for systems under attack, 10 otherwise)	20	20	20	20
3.2.1.71 MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Highest Protection, source routing is automatically disabled.	Highest Protection, source routing is automatically disabled.	Highest Protection, source routing is automatically disabled.	Highest Protection, source routing is automatically disabled.
3.2.1.72 MSS: (EnableDeadCXNDetect) Allow automatic detection of dead network gateways (could lead to DoS)	Disabled	Disabled	Disabled	Disabled
3.2.1.73 MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Disabled	Disabled	Disabled	Disabled
3.2.1.74 MSS: (EnableMTUDiscovery) Allow automatic detection of MTU size (possible DoS by an attacker using a small MTU)	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.75 MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Enabled	Enabled	Enabled	Enabled
3.2.1.76 MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)	Disabled	Disabled	Disabled	Disabled
3.2.1.77 MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)	Connections time out sooner if a SYN attack is detected	Connections time out sooner if a SYN attack is detected	Connections time out sooner if a SYN attack is detected	Connections time out sooner if a SYN attack is detected
3.2.1.78 MSS: (TCPMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged	3 & 6 seconds, half-open connections dropped after 21 seconds	3 & 6 seconds, half-open connections dropped after 21 seconds	3 & 6 seconds, half-open connections dropped after 21 seconds	3 & 6 seconds, half-open connections dropped after 21 seconds




29



Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
3.2.1.79 MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	3	3	3	3
3.2.1.80 MSS: (TCPMaxPortsExhausted) How many dropped connect requests to initiate SYN attack protection (5 is recommended)	5	5	5	5
3.2.1.81 MSS: Disable autorun for all drives	255, disable autorun for all drives	255, disable autorun for all drives	255, disable autorun for all drives	255, disable autorun for all drives
3.2.1.82 MSS: Enable Safe DLL search mode	Enabled	Enabled	Enabled	Enabled
3.2.1.83 MSS: Enable the computer to stop generating 8.3 style filenames	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.84 MSS: How often keep-alive packets are sent in milliseconds	300000	300000	300000	300000
3.2.1.85 MSS: Percentage threshold for the security event log at which the system will generate a warning	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
3.2.1.86 MSS: The time in seconds before the screen saver grace period expires	0	0	0	0
4 Additional Security Protection				
4.1 Available Services	Permissions of services: Administrators: Full Control; System: Full Control; Interactive: Read	Permissions of services: Administrators: Full Control; System: Full Control; Interactive: Read	Permissions of services: Administrators: Full Control; System: Full Control; Interactive: Read	Permissions of services: Administrators: Full Control; System: Full Control; Interactive: Read
4.1.1 Alerter	Disabled	Disabled	Disabled	Disabled
4.1.2 Client Services for Network	Disabled	Disabled	Disabled	Disabled
4.1.3 Clipbook	Disabled	Disabled	Disabled	Disabled
4.1.4 Fax Service	Disabled	Disabled	Disabled	Disabled
4.1.5 File Replication	Disabled	Disabled	Disabled	Disabled
4.1.6 File Services for Macintosh	Disabled	Disabled	Disabled	Disabled
4.1.7 FTP Publishing Service	Disabled	Disabled	Disabled	Disabled



30



Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
4.1.8 Help and Support	Disabled	Disabled	Disabled	Disabled
4.1.9 HTTP SSL	Enabled	Enabled	Enabled	Enabled
4.1.10 IIS Admin Service	Enabled	Enabled	Enabled	Enabled
4.1.11 Indexing Service	Enabled	Enabled	Enabled	Enabled
4.1.12 License Logging Service	Disabled	Disabled	Disabled	Disabled
4.1.13 Messenger	Disabled	Disabled	Disabled	Disabled
4.1.14 Microsoft POP3 Service	Disabled	Disabled	Disabled	Disabled
4.1.15 NetMeeting Remote Desktop Sharing	Disabled	Disabled	Disabled	Disabled
4.1.16 Network Connections	Manual	Manual	Manual	Manual
4.1.17 Network News Transport Protocol (NNTP)	Disabled	Disabled	Disabled	Disabled
4.1.18 Print Server for Macintosh	Disabled	Disabled	Disabled	Disabled
4.1.19 Print Spooler	Disabled	Disabled	Disabled	Disabled
4.1.20 Remote Access Auto Connection Manager	Disabled	Disabled	Disabled	Disabled
4.1.21 Remote Access Connection Manager	Disabled	Disabled	Disabled	Disabled
4.1.22 Remote Administration Service	Disabled	Disabled	Disabled	Disabled
4.1.23 Remote Desktop HelpSession Manager	Disabled	Disabled	Disabled	Disabled
4.1.24 Remote Installation	Disabled	Disabled	Disabled	Disabled
4.1.25 Remote Procedure Call (RPC) Locator	Disabled	Disabled	Disabled	Disabled
4.1.26 Remote Registry Service	Disabled	Disabled	Disabled	Disabled
4.1.27 Remote Server Manager	Disabled	Disabled	Disabled	Disabled
4.1.28 Remote Server Monitor	Disabled	Disabled	Disabled	Disabled
4.1.29 Remote Storage Notification	Disabled	Disabled	Disabled	Disabled
4.1.30 Remote Storage Server	Disabled	Disabled	Disabled	Disabled
4.1.31 Simple Mail Transfer Protocol (SMTP)	Disabled	Disabled	Disabled	Disabled
4.1.32 Simple Network Management Protocol (SNMP) Service	Disabled	Disabled	Disabled	Disabled
4.1.33 Simple Network Management Protocol (SNMP) Trap	Disabled	Disabled	Disabled	Disabled
4.1.34 Telephony	Disabled	Disabled	Disabled	Disabled
4.1.35 Telnet	Disabled	Disabled	Disabled	Disabled

Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
4.1.36 Terminal Services	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.1.37 Trivial FTP Daemon	Disabled	Disabled	Disabled	Disabled
4.1.38 Volume Shadow Service	Enabled	Enabled	Enabled	Enabled
4.1.39 Wireless Configuration	Disabled	Disabled	Disabled	Disabled
4.1.40 World Wide Web Publishing Services	Disabled	Disabled	Disabled	Disabled
4.1.41 Windows Media Server	Disabled	Disabled	Disabled	Disabled
4.1.42 Data Execution Prevention	Enabled	Enabled	Enabled	Enabled
4.2 User Rights				
4.2.1 Access this computer from the network	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.2.2 Act as part of the operating system	<None>	<None>	<None>	<None>
4.2.3 Add workstations to domain	<<Not Defined>	<<Not Defined>	<<Not Defined>	<<Not Defined>
4.2.4 Adjust memory quotas for a process	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.2.5 Allow log on locally	Administrators	Administrators	Administrators	Administrators
4.2.6 Allow logon through terminal services	Administrators	Administrators	Administrators	Administrators
4.2.7 Back up files and directories	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.2.8 Bypass traverse checking	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.2.9 Change the system time	Administrators	Administrators	Administrators	Administrators
4.2.10 Create a pagefile	Administrators	Administrators	Administrators	Administrators
4.2.11 Create a token object	<None>	<None>	<None>	<None>
4.2.12 Create Global Objects	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.2.13 Create permanent shared objects	<None>	<None>	<None>	<None>
4.2.14 Debug Programs	<None>	<None>	<None>	<None>
4.2.15 Deny access to this computer from the network (minimum)	ANONYMOUS LOGON, Guests	ANONYMOUS LOGON, Guests	ANONYMOUS LOGON, Guests	ANONYMOUS LOGON, Guests
4.2.16 Deny logon as a batch job	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.2.17 Deny logon as a service	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.2.18 Deny logon locally	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.2.19 Deny logon through Terminal Service (minimum)	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.2.20 Enable computer and user accounts to be trusted for delegation	<None>	<None>	<None>	<None>

Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
4.2.21 Force shutdown from a remote system	Administrators	Administrators	Administrators	Administrators
4.2.22 Generate security audits	Local Service, Network Service	Local Service, Network Service	Local Service, Network Service	Local Service, Network Service
4.2.23 Impersonate a client after authentication	SERVICE	SERVICE	SERVICE	SERVICE
4.2.24 Increase scheduling priority	Administrators	Administrators	Administrators	Administrators
4.2.25 Load and unload device drivers	Administrators	Administrators	Administrators	Administrators
4.2.26 Lock pages in memory	Administrators	Administrators	Administrators	Administrators
4.2.27 Log on as a batch job	<None>	<None>	<None>	<None>
4.2.28 Log on as a service	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.2.29 Manage auditing and security log	Administrators	Administrators	Administrators	Administrators
4.2.30 Modify firmware environment values	Administrators	Administrators	Administrators	Administrators
4.2.31 Perform volume maintenance tasks	Administrators	Administrators	Administrators	Administrators
4.2.32 Profile single process	Administrators	Administrators	Administrators	Administrators
4.2.33 Profile system performance	Administrators	Administrators	Administrators	Administrators
4.2.34 Remove computer from docking station	Administrators	Administrators	Administrators	Administrators
4.2.35 Replace a process level token	NETWORK SERVICE, LOCAL SERVICE	NETWORK SERVICE, LOCAL SERVICE	NETWORK SERVICE, LOCAL SERVICE	NETWORK SERVICE, LOCAL SERVICE
4.2.36 Restore files and directories	Administrators	Administrators	Administrators	Administrators
4.2.37 Shut down the system	Administrators	Administrators	Administrators	Administrators
4.2.38 Synchronize directory service data	<None>	<None>	<None>	<None>
4.2.39 Take ownership of file or other objects	Administrators	Administrators	Administrators	Administrators
4.3 Other System Requirements				
4.3.1 Ensure volumes are using the NTFS file system	All volumes	All volumes	All volumes	All volumes
4.3.2 Disable NetBIOS	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.3.3 Enable the Internet Connection Firewall	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.3.4 Restricted Groups	Remote Desktop Users:	Remote Desktop Users:	Remote Desktop Users:	Remote Desktop Users:
	<None>	<None>	<None>	<None>
4.3.5 Antivirus software present	<Not Defined>	<Not Defined>	<Not Defined>	<Not Defined>
4.4 File and Registry Permissions				
4.4.1 File Permissions	Unless stated otherwise,	Unless stated	Unless stated	Unless stated otherwise,

Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
	Administrators or System Full Control is full control for the designated folder and all contents	otherwise, Administrators or System Full Control is full control for the designated folder and all contents	otherwise, Administrators or System Full Control is full control for the designated folder and all contents	Administrators or System Full Control is full control for the designated folder and all contents
4.4.1.1 %SystemDrive%	Administrators: Full; System: Full; Creator Owner: Full; Interactive: Read, Execute	Administrators: Full; System: Full; Creator Owner: Full; Interactive: Read, Execute	Administrators: Full; System: Full; Creator Owner: Full; Interactive: Read, Execute	Administrators: Full; System: Full; Creator Owner: Full; Interactive: Read, Execute
4.4.1.2 %SystemRoot%\system32\at.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.3 %SystemRoot%\system32\attrib.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.4 %SystemRoot%\system32\cacls.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.5 %SystemRoot%\system32\debug.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.6 %SystemRoot%\system32\drwtsn32.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.7 %SystemRoot%\system32\drwtsn32.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.8 %SystemRoot%\system32\edlin.exe	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full
4.4.1.9 %SystemRoot%\system32\eventcreate.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.10 %SystemRoot%\system32\eventtriggers.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.11 %SystemRoot%\system32\ftp.exe	Administrators: Full; System: Full; Interactive:	Administrators: Full; System: Full;	Administrators: Full; System: Full;	Administrators: Full; System: Full;

Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
4.4.1.12 %SystemRoot%\system32\net.exe	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full
4.4.1.13 %SystemRoot%\system32\net1.exe	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full
4.4.1.14 %SystemRoot%\system32\neth.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.15 %SystemRoot%\system32\rpc.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.16 %SystemRoot%\system32\reg.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.17 %SystemRoot%\regedit.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.18 %SystemRoot%\system32\regedt32.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.19 %SystemRoot%\system32\regsvr32.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.20 %SystemRoot%\system32\rexec.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.21 %SystemRoot%\system32\rsh.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.22 %SystemRoot%\system32\runas.exe	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full
4.4.1.23 %SystemRoot%\system32\sc.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.24 %SystemRoot%\system32\subst.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.1.25 %SystemRoot%\system32\telnet.exe	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full

Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
4.4.1.26 %SystemRoot%\system32\http.exe	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full	Administrators: Full; System: Full; Interactive: Full
4.4.1.27 %SystemRoot%\system32\tlntsvr.exe	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full	Administrators: Full; System: Full
4.4.2 Registry Permissions	Unless stated otherwise, Administrators or System Full Control is full control for the designated key and all subkeys. Creator Owner Full Control is for subkeys only. Users permissions are for current key, subkeys, and values.	Unless stated otherwise, Administrators or System Full Control is full control for the designated key and all subkeys. Creator Owner Full Control is for subkeys only. Users permissions are for current key, subkeys, and values.	Unless stated otherwise, Administrators or System Full Control is full control for the designated key and all subkeys. Creator Owner Full Control is for subkeys only. Users permissions are for current key, subkeys, and values.	Unless stated otherwise, Administrators or System Full Control is full control for the designated key and all subkeys. Creator Owner Full Control is for subkeys only. Users permissions are for current key, subkeys, and values.
4.4.2.1 HKLM\Software	Administrators: Full; System: Full; Creator Owner: Full; Users, Read	Administrators: Full; System: Full; Creator Owner: Full; Users, Read	Administrators: Full; System: Full; Creator Owner: Full; Users, Read	Administrators: Full; System: Full; Creator Owner: Full; Users, Read
4.4.2.2 HKLM\Software\Microsoft\Windows\CurrentVersion\Installer	Administrators: Full; System: Full; Users: Read	Administrators: Full; System: Full; Users: Read	Administrators: Full; System: Full; Users: Read	Administrators: Full; System: Full; Users: Read
4.4.2.3 HKLM\Software\Microsoft\Windows\CurrentVersion\Policies	Administrators: Full; System: Full; Authenticated Users: Read	Administrators: Full; System: Full; Authenticated Users: Read	Administrators: Full; System: Full; Authenticated Users: Read	Administrators: Full; System: Full; Authenticated Users: Read
4.4.2.4 HKLM\System	Administrators: Full; System: Full; Creator Owner: Full; Users, Read	Administrators: Full; System: Full; Creator Owner: Full; Users, Read	Administrators: Full; System: Full; Creator Owner: Full; Users, Read	Administrators: Full; System: Full; Creator Owner: Full; Users, Read

Setting:	SSL Servers	MSMQ	WWW Servers	Shopping Cart
4.4.2.5 HKLM\System\CurrentControlSet\Enum	Administrators: Full; System: Full; Authenticated Users: Read	Read	Read	Read
4.4.2.6 HKLM\System\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers	Administrators: Full; System: Full; Creator Owner: Full	Administrators: Full; System: Full; Creator Owner: Full	Administrators: Full; System: Full; Creator Owner: Full	Administrators: Full; System: Full; Creator Owner: Full
4.4.2.7 HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities	Administrators: Full; System: Full; Creator Owner: Full	Administrators: Full; System: Full; Creator Owner: Full	Administrators: Full; System: Full; Creator Owner: Full	Administrators: Full; System: Full; Creator Owner: Full
4.4.2.8 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ratings	Administrators: Full; Users: Read	Administrators: Full; Users: Read	Administrators: Full; Users: Read	Administrators: Full; Users: Read
4.4.2.9 HKLM\Software\Microsoft\MSDTC	Administrators: Full; System: Full; Network Service: Queryvalue, Setvalue, Create subkey, Enumerate Subkeys, Notify, Read permissions; Users: Read <Not Defined>	Administrators: Full; System: Full; Network Service: Queryvalue, Setvalue, Create subkey, Enumerate Subkeys, Notify, Read permissions; Users: Read <Not Defined>	Administrators: Full; System: Full; Network Service: Queryvalue, Setvalue, Create subkey, Enumerate Subkeys, Notify, Read permissions; Users: Read <Not Defined>	Administrators: Full; System: Full; Network Service: Queryvalue, Setvalue, Create subkey, Enumerate Subkeys, Notify, Read permissions; Users: Read <Not Defined>
4.4.2.10 HKU\Default\Software\Microsoft\SystemCertificates\Root\ProtectedRoots	Administrators: Full; System: Full; Users: Read	Administrators: Full; System: Full; Users: Read	Administrators: Full; System: Full; Users: Read	Administrators: Full; System: Full; Users: Read
4.4.2.11 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SecEdit	Administrators: Full; System: Full; Users: Read	Administrators: Full; System: Full; Users: Read	Administrators: Full; System: Full; Users: Read	Administrators: Full; System: Full; Users: Read
4.4.3 File and Registry Auditing				
4.4.3.1 %SystemDrive%	Everyone: Failures	Everyone: Failures	Everyone: Failures	Everyone: Failures
4.4.3.2 HKLM\Software	Everyone: Failures	Everyone: Failures	Everyone: Failures	Everyone: Failures
4.4.3.3 HKLM\System	Everyone: Failures	Everyone: Failures	Everyone: Failures	Everyone: Failures

Summary

- ❖ DO NOT USE INDUSTRY STANDARDS WITHOUT TESTING FIRST
- ❖ IDENTIFY INVENTORY OF SERVER / SERVER TYPES
 - ❖ DOMAIN CONTROLLERS
 - ❖ MEMBER SERVERS – WEB SERVER, FILE SERVER, ETC.
- ❖ DEVELOP BASELINE USING INDUSTRY STANDARD AS A GUIDE
- ❖ TEST, TEST, TEST
- ❖ USE AUTOMATED TOOL (E.G., TRIPWIRE)
- ❖ ALL BASELINE SETTINGS SHOULD UNDERGO CHANGE MANAGEMENT PROCEDURES (I.E., REMEDY)
- ❖ OBTAIN WAIVER FOR THOSE SETTINGS YOU HAVE TESTED AND DISAGREE WITH STANDARD
- ❖ RUN SCANS TO ENSURE STANDARD IS MAINTAINED

Miguel (Mike) O. Villegas, CISA, CISSP

Miguel (Mike) O. Villegas is the Director of Information Security at Newegg, Inc. and is responsible for Information Security, Business Continuity Management, and PCI DSS (Payment Card Industry Data Security Standard) compliance. Newegg, Inc. is one of the fastest growing E-Commerce companies established in 2001 and exceeded revenues of over \$2 Billion in 2008.

Mike has over 25 years of Information Systems security and IT audit experience. Mike was previously Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance and was previously a partner at Ernst & Young and Arthur Andersen over their information systems security and IS audit groups over a span of nine years. Mike is a CISA and CISSP.

He was the SF ISACA Chapter President during 2005-2006 and the SF Fall Conference Co-Chair from 2002-2007. He also served for two years as Vice President on the Board of Directors for ISACA International. Currently, Mike is currently a Director in the LA ISACA Chapter, involved with the LA ISACA Spring Conference Committee, and is the CISA Review Course Coordinator.

