Security Hardening

General Information				
System / Project Name		**IP Address(es)**		
Host Name		**Subnet Mask(s)**		
Model/Type		**Default Gateway(s)**		
Operating System		**DNS Server(s)**		
Service Pack Release		**Domain / Workgroup**		

Sign-Off

Technical Provider	Information Security Approval
Signature :_____	Signature : _____
Name:_____	Name: _____
Role : _____	Role : _____
Company : _____	Company : _____
Date : _____	Date : _____

Microsoft Windows 2008 R2

Version - Release Levels/applicable to:

- Microsoft Windows Server 2008R2, Standard Edition
- Microsoft Windows Server 2008R2, Enterprise Edition
- Microsoft Windows Server 2008R2, Datacenter Edition
- Microsoft Windows Server 2008R2, Web Edition

1. System Setup

1.1 Account Policies (secpol.msc)

1.1.1 Password Policies

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
Enforce password history	24 (Domain), 0	5		✓
Maximum password age	42 days	90 days		✓
Minimum password age	1 days	1 days		✓
Minimum password length	0 characters	8 characters		✓
Password must meet complexity requirements	Disabled	Enabled		✓

1.1.2 Account Lockout Policy

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
Account lockout duration	Not Applicable	30 minutes		✓
Account lockout threshold	0 attempts	5 attempts		✓
Reset account lockout counter after	Not Applicable	30 minutes		✓

1.2 Local Policies (secpol.msc)

1.2.1 Audit Policy

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
Audit account logon events	Not Defined	Success, Failure		✓
Audit account management	Not Defined	Success, Failure		✓
Audit directory service access	Not Defined	Failure		✓
Audit logon events	Not Defined	Success, Failure		✓
Audit object access	Not Defined	Failure		✓
Audit policy change	Not Defined	Success, Failure		✓
Audit privilege use	Not Defined	Not Defined		✓
Audit process tracking	Not Defined	Not Defined		✓
Audit system events	Not Defined	Success, Failure		✓

1.2.2 Security Options

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
Accounts: Administrator account status	Enabled	Enabled		✓
Accounts: guest account status	Disabled	Disabled		✓
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled		✓
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined	Not Defined		✓
Interactive logon: Do not display last user name	Disabled	Disabled		✓
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Disabled		✓
Interactive logon : Message text for users attempting to log on	-	"This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored		✓

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
		and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials"		
Interactive logon: Message title for users attempting to log on	-	Electronic Transactions Development Agency (Public Organization)		✓
Interactive logon: Prompt user to change password before expiration	5 days	5 days		✓
Microsoft network client: Digitally sign communications (always)	Disabled	Enabled		✓
Microsoft network server: Digitally sign communications (always)	Disabled	Enabled		✓
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet	Not defined		✓
User Account Control : Admin Approval Mode for the Built-in Administrator account	Disabled	Disabled		✓
User Account Control : Behavior of the elevation prompt for standard users	Prompt for credentials	Prompt for credentials		✓

2. System Logs

2.1 Event Log (eventvwr.msc)

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
Application: Maximum Log Size (KB)	20480	307200		✓
Security: Maximum Log Size (KB)	20480	307200		✓
System: Maximum Log Size (KB)	20480	307200		✓

3. Network and Sharing

3.1 Internet Communication (gpedit.msc | Administrative Templates ->System ->Internet Communiction Setting)

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
Turn off the Windows Messenger Customer Experience Improvement Program	Not configure	Enabled		✓

3.2 SMB protocol (regedit)

The SMB protocol provides the basis for Microsoft file and print sharing and many other networking operations, such as remote Windows administration. To help prevent attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets. This policy setting determines whether SMB packet signing must be negotiated before further communication with an SMB client is permitted.

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature	0	1		✓
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature	0	1		✓

3.3 TCP timestamp

The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behaviour of their TCP timestamps.

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
cmd : netsh int tcp set global timestamps=disable (Open CMD With admin option)	Enabled	Disabled		✓

3.4 Network Share (regedit)

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer	Not Configure	0	Create new DWORD Value (if it is not already present) named AutoShareServer and set value 0 (disable network shares)	✓

4. Additional Security Settings

4.1 Autoplay (Control Panel)

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
Turn off Autoplay	Off	On		✓

4.2 Service (services.msc)

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
Dhcp client	Enabled	Disabled		✓
Print Spooler	Enabled	Disabled		✓
Application Layer Gateway Service	Disabled	Disabled		✓
Application Management	Disabled	Disabled		✓
Automatic Updates	Enabled	Enabled	Download and ask for install.	✓
Background Intelligent Transfer Service	Enabled	Enabled		✓
Computer Browser	Disabled	Disabled		✓
Cryptographic Services	Enabled	Enabled		✓
Distributed Transaction Coordinator	Enabled	Enabled		✓
DNS Client	Enabled	Enabled		✓
Net Logon Service	Enabled	Enabled		✓
Network Connections	Enabled	Enabled		✓
Protected Storage	Enabled	Enabled		✓
Remote Access Auto Connection Manager	Enabled	Enabled		✓
Remote Procedure Call	Enabled	Enabled		✓
Remote Registry Service	Enabled	Disabled		✓
Remote Desktop Service	Enabled	Enabled		✓
Security Accounts Manager	Enabled	Enabled		✓
Server	Enabled	Enabled		✓
Shell Hardware Detection	Enabled	Enabled		✓
Task Scheduler	Enabled	Enabled		✓

System Value / Parameter	Default Setting	Recommended Setting	Remarks	Check
Telephony	Enabled	Disabled		✓
Windows Management Instrumentation	Enabled	Enabled		✓
Windows Time	Enabled	Enabled		✓