

EGA e-Government Agency Electronic Government Agency (Public Organization) สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)



การปิดจุดอ่อนวินโดวส์

(Windows Hardening)



วัตถุประสงค์การปิดจุดอ่อน

(Harden Objectives)

เพื่อเป็นแนวทางในการกำหนดค่าความปลอดภัยให้กับระบบที่ กำลังจะติดตั้งใช้งานจริง หรือการปรับปรุงแก้ไขเครื่องให้บริการที่เกิดมี จุดอ่อนให้มีการป้องกันที่เข้มแข็งขึ้น



Hardening

Systems (MS Windows, Linux, Network Devices)

Application (Mysql, SQL Server, Web Application ...)



Microsoft Windows Server 2012 Hardening

- Account Policies
- Audit Policy
- Security Options
- Windows Components
- Web Server recomend
- Microsoft Baseline Security Analyzer







Microsoft Corporation



National Institute of Standards and Technology U.S. Department of Commerce

The National Institute of Standards and Technology (NIST)

Center for Internet Security (CIS)





Member Server

- AD Certificate Services
- DHCP Server
- DNS Server
- File Server
- Hyper-V
- Network Policy and Access Services
- Print Server
- Remote Access Services
- Remote Desktop Services
- Web Server









Security Settings

Account Policies





* 'O' Administrator unlock manually http://www.cisecurity.org/





EX : Set 'Minimum password length' to '14 or more character(s)'

https://howsecureismypassword.net/

HOW SECURE IS MY PASSWORD?



SHOW SETTINGS

It would take a desktop PC about 6 million years to crack your password

[Tweet Result]

SHOW DETAILS



EGA EGA E-Government Agency T H A I L A N D

Set 'Enforce password history' to '24 or more password(s)'



Set 'Password must meet complexity requirements' to 'Enabled'

English uppercase characters (A through Z) English lowercase characters (a through z) Base 10 digits (0 through 9) Non-alphabetic characters (for example, !, \$, #, %)



'kov[l,soj;p'ko4k8iy{ งานอบรมหน่วยงานภาครัฐ

Set 'Store passwords using reversible encryption' to 'Disabled'





Set 'Audit Policy: Account Logon: Credential Validation' to 'Success and Failure' Set 'Audit Policy: Account Logon: Kerberos Authentication Service' to 'No Auditing' Set 'Audit Policy: Account Logon: Kerberos Service Ticket Operations' to 'No Auditing' Set 'Audit Policy: Account Logon: Other Account Logon Events' to 'No Auditing' Set 'Audit Policy: Account Management: Application Group Management' to 'No Auditing'

Configure 'Audit Policy: Account Management: Computer Account Management' Set 'Audit Policy: Account Management: Distribution Group Management' to 'No Auditing'

Set 'Audit Policy: Account Management: Other Account Management Events' to 'Success and Failure'

Set 'Audit Policy: Account Management: Security Group Management' to 'Success and Failure' http://www.cisecurity.org/

Set 'Audit Policy: Account Management: User Account Management' to 'Success and Failure' Set 'Audit Policy: Detailed Tracking: DPAPI Activity' to 'No Auditing' Set 'Audit Policy: Detailed Tracking: Process Creation' to 'Success' Set 'Audit Policy: Detailed Tracking: Process Termination' to 'No Auditing' Set 'Audit Policy: Detailed Tracking: RPC Events' to 'No Auditing' Set 'Audit Policy: Logon-Logoff: Account Lockout' to 'No Auditing' Set 'Audit Policy: Logon-Logoff: IPsec Extended Mode' to 'No Auditing' Set 'Audit Policy: Logon-Logoff: IPsec Main Mode' to 'No Auditing'

Set 'Audit Policy: Logon-Logoff: IPsec Quick Mode' to 'No Auditing'

Set 'Audit Policy: Logon-Logoff: Logoff' to 'Success'

Set 'Audit Policy: Logon-Logoff: Logon' to 'Success and Failure

Set 'Audit Policy: Logon-Logoff: Network Policy Server' to 'No Auditing'

Set 'Audit Policy: Account Logon: Other Account Logon Events' to 'No Auditing'

Set 'Audit Policy: Logon-Logoff: Other Logon/Logoff Events' to 'No Auditing'

Set 'Audit Policy: Logon-Logoff: Special Logon' to 'Success'

Set 'Audit Policy: Object Access: Application Generated' to 'No Auditing'

Set 'Audit Policy: Object Access: Central Access Policy Staging' to 'No Auditing'

Set 'Audit Policy: Object Access: Certification Services' to 'No Auditing'

Set 'Audit Policy: Privilege Use: Other Privilege Use Events' to 'No Auditing' Set 'Audit Policy: Privilege Use: Sensitive Privilege Use' to 'Success and Failure' Set 'Audit Policy: Policy Change: Audit Policy Change' to 'Success and Failure' Set 'Audit Policy: System: IPsec Driver' to 'Success and Failure' Set 'Audit Policy: System: Other System Events' to 'No Auditing' Set 'Audit Policy: System: Security State Change' to 'Success and Failure' Set 'Audit Policy: System: Security System Extension' to 'Success and Failure' Set 'Audit Policy: System: System Integrity' to 'Success and Failure'



Advanced Audit Policy Configuration

Control Panel\System and Security\Administrative Tools\Local Security Policy

-		
a	Local Security Policy	
File Action View Help		
🗢 🄿 📶 🖬 🔝		
🚡 Security Settings	Policy	Security Setting
Account Policies	🖾 Audit account logon events	Success, Failure
⊿ Local Policies	🖾 Audit account management	Success, Failure
强 Audit Policy	📓 Audit directory service access	Success, Failure
 User Rights Assignment Security Options Windows Firewall with Advanced Security 	🗟 Audit logon events	Success, Failure
	🗟 Audit object access	Success, Failure
	Audit policy change	Success, Failure
Network List Manager Policies	🗟 Audit privilege use	Success, Failure
Public Key Policies	🗄 Audit process tracking	Success, Failure
Software Restriction Policies	Audit system events	Success, Failure
Application Control Policies		
IP Security Policies on Local Compute		
Advanced Audit Policy Configuration		



Control Panel\System and Security\Administrative Tools\Local Security Policy

a	Local Security Policy					
File Action View Help						
🗢 🔿 🔁 📰 🗙 🗟 🔽 🖬						
🚡 Security Settings	Policy	Security Setting				
Account Policies	B Accounts: Administrator account status	Enabled				
⊿ 📴 Local Policies	📓 Accounts: Block Microsoft accounts	Not Defined				
Audit Policy	B Accounts: Guest account status	Disabled				
User Rights Assignment	B Accounts: Limit local account use of blank passwords to co	Enabled				
Security Options	B Accounts: Rename administrator account	Admin_Cloud				
Windows Firewall with Advanced Security	📓 Accounts: Rename guest account	Guest_Cloud				
Network List Manager Policies	R Audit: Audit the access of alabal system objects	Disabled				

EGA E-Government Agency T H A I L A N D

Accounts

Configure 'Accounts: Rename administrator account'

Configure 'Accounts: Rename guest account'

Set 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled'

EGA e-Government Agency T H A I L A N D

Audit

Set 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' to 'Enabled'

Set 'Audit: Shut down system immediately if unable to log security audits' to 'Disabled'

EGA E-Government Agency T H A I L A N D

Devices

Set 'Devices: Allowed to format and eject removable media' to 'Administrators'

Set 'Devices: Prevent users from installing printer drivers' to 'Enabled'



Domain Member

Set 'Domain member: Digitally encrypt or sign secure channel data (always)' to 'Enabled'

Set 'Domain member: Digitally encrypt secure channel data (when possible)' to 'Enabled'

Set 'Domain member: Digitally sign secure channel data (when possible)' to 'Enabled'

Set 'Domain member: Disable machine account password changes' to 'Disabled'

EGA EGOVERNMENT Agency T H A I L A N D

Interactive logon

Configure 'Interactive logon: Message text for users attempting to log on'

Configure 'Interactive logon: Message title for users attempting to log on'

Warning

===== UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. ===== ,You must have explicit permission to access or configure this device., All activities performed on this device may be logged"," and violations, of this policy may result in disciplinary action"," and may be reported, to law enforcement. There is no right to privacy on this device.

ОК

EGA e-Government Agency T H A I L A N D

Interactive logon

Set 'Interactive logon: Do not display last user name' to 'Enabled'

Set 'Interactive logon: Do not require CTRL+ALT+DEL' to 'Disabled'

Set 'Interactive logon: Machine inactivity limit' to '900 or fewer seconds'

Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'

EGA e-Government Agency T H A I L A N D

Interactive logon

Set 'Interactive logon: Prompt user to change password before expiration' to '14 or more day(s)'

Set 'Interactive logon: Machine account lockout threshold' to 10 or fewer invalid logon attempts



http://www.cisecurity.org/

Microsoft network client

Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled'

Set 'Microsoft network client: Digitally sign communications (if server agrees)' to 'Enabled'

Set 'Microsoft network client: Send unencrypted password to third-party SMB servers' to 'Disabled'



Microsoft network server

Set 'Microsoft network server: Amount of idle time required before suspending session' to '15 or fewer minute(s)'

Set 'Microsoft network server: Digitally sign communications (always)' to 'Enabled'

Set 'Microsoft network server: Digitally sign communications (if client agrees)' to 'Enabled'

Set 'Microsoft network server: Disconnect clients when logon hours expire' to 'Enabled'



Network access

Set 'Network access: Allow anonymous SID/Name translation' to 'Disabled'

Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'

Set 'Network access: Do not allow anonymous enumeration of SAM accounts' to 'Enabled'

Set 'Network access: Let Everyone permissions apply to anonymous users' to 'Disabled'

Set 'Network access: Remotely accessible registry paths and sub-paths' to 'System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Softwar



http://www.cisecurity.org/

Network access

Set 'Network access: Remotely accessible registry paths' to 'System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion'

Set 'Network access: Restrict anonymous access to Named Pipes and Shares' to 'Enabled'



Network Security

Set 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled'

Set 'Network security: Allow LocalSystem NULL session fallback' to 'Disabled'

Set 'Network security: Do not store LAN Manager hash value on next password change' to 'Enabled'

Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'

Set 'Network security: LDAP client signing requirements' to 'Negotiate signing'

Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption'



Network Security

Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security, Require 128-bit encryption'



Recovery console

Set 'Recovery console: Allow automatic administrative logon' to 'Disabled'



Shutdown

Set 'Shutdown: Allow system to be shut down without having to log on' to 'Disabled'

Set 'Shutdown: Clear virtual memory pagefile' to 'Disabled'



System cryptography

Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled'

Set 'System objects: Strengthen default permissions of internal system objects



http://www.cisecurity.org/

System settings

Set 'System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies' to 'Enabled'



User Account Control

Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled'

Set 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' to 'Disabled'

Set 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' to 'Prompt for consent for non-Windows binaries'

Set 'User Account Control: Behavior of the elevation prompt for standard users' to 'Prompt for credentials'

Set 'User Account Control: Detect application installations and prompt for elevation' to 'Enabled'



User Account Control

Set 'User Account Control: Only elevate executables that are signed and validated' to 'Disabled'

Set 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' to 'Enabled'

Set 'User Account Control: Run all administrators in Admin Approval Mode' to 'Enabled'

Set 'User Account Control: Switch to the secure desktop when prompting for elevation' to 'Enabled'

Set 'User Account Control: Virtualize file and registry write failures to peruser locations' to 'Enabled'



User Rights Assignments

Configure 'Deny log on through Remote Desktop Services'

Set 'Access Credential Manager as a trusted caller' to 'No One'

Configure 'Access this computer from the network'

Set 'Act as part of the operating system' to 'No One'

Set 'Adjust memory quotas for a process' to 'Administrators, Local Service, Network Service'

User Rights Assignments

Set 'Allow log on locally' to 'Administrators'

Set 'Allow log on through Remote Desktop Services' to 'Administrators'

Set 'Back up files and directories' to 'Administrators'

Configure 'Bypass traverse checking'

Set 'Change the system time' to 'LOCAL SERVICE, Administrators'



User Rights Assignments

Set 'Change the time zone' to 'LOCAL SERVICE, Administrators'

Set 'Create global objects' to 'Administrators, SERVICE, LOCAL SERVICE, NETWORK SERVICE'

Set 'Back up files and directories' to 'Administrators'

Set 'Deny access to this computer from the network' to 'Guests'

Set 'Deny log on as a batch job' to 'Guests'

User Rights Assignments

Set 'Deny log on as a service' to 'No One'

Set 'Deny log on locally' to 'Guests'

Configure 'Enable computer and user accounts to be trusted for delegation'

Set 'Force shutdown from a remote system' to 'Administrators'

Set 'Generate security audits' to 'Local Service, Network Service'





User Rights Assignments

Set 'Impersonate a client after authentication' to 'Administrators, SERVICE, Local Service, Network Service'

Set 'Increase a process working set' to 'Administrators, Local Service'

Set 'Increase scheduling priority' to 'Administrators'

Set 'Load and unload device drivers' to 'Administrators'

Set 'Lock pages in memory' to 'No One'

User Rights Assignments

Set 'Log on as a batch job' to 'Administrators'

Set 'Manage auditing and security log' to 'Administrators'

Set 'Modify an object label' to 'No One'

Set 'Modify firmware environment values' to 'Administrators'

Set 'Perform volume maintenance tasks' to 'Administrators'



EGA e-Government Agency T H A I L A N D

User Rights Assignments

Set 'Profile single process' to 'Administrators'

Set 'Remove computer from docking station' to 'Administrators'

Set 'Replace a process level token' to 'Local Service, Network Service'

Set 'Restore files and directories' to 'Administrators'

Set 'Shut down the system' to 'Administrators'

MS Windows Server 2012 EGA Windows Firewall With Advanced Security

Public Profile

Set 'Inbound connections' to 'Enabled:Block (default)'

Set 'Windows Firewall: Public: Allow unicast response' to 'No'

Set 'Windows Firewall: Public: Apply local connection security rules' to 'Yes' Set 'Windows Firewall: Public: Apply local firewall rules' to 'Yes (default)'

Set 'Windows Firewall: Public: Apply local firewall rules' to 'Yes (default)'

Set 'Windows Firewall: Public: Display a notification' to 'Yes'

Set 'Windows Firewall: Public: Outbound connections' to 'Allow (default)'



Windows Firewall With Advanced Security

Private Profile

Set 'Inbound connections' to 'Enabled:Block (default)'

Set 'Windows Firewall: Private: Allow unicast response' to 'No'

Set 'Windows Firewall: Private: Apply local connection security rules' to 'Yes (default)'

Set 'Windows Firewall: Private: Apply local firewall rules' to 'Yes (default)'

Set 'Windows Firewall: Private: Display a notification' to 'Yes (default)'

Set 'Windows Firewall: Private: Firewall state' to 'On

Windows Firewall: Private: Outbound connections' to 'Allow (default)'



Administrative Templates

Windows Components

MS Windows Server 2012 Windows Components

EGA E-Government Agency T H A T L A N D

AutoPlay Policies

Set 'Turn off Autoplay on:' to 'Enabled:All drives'

MS Windows Server 2012 Windows Components

EGA e-Government Agency T H A I L A N D

Event Log

Set 'Security: Maximum Log Size (KB)' to 'Enabled: 196608 or greater'

Set 'System: Maximum Log Size (KB)' to 'Enabled:32768 or greater'

Set 'Application: Maximum Log Size (KB)' to 'Enabled:32768 or greater'

Set 'Security: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'

Set 'System: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'

Set 'Application: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'

MS Windows Server 2012 Windows Components



Event Log

Control Panel\System and Security\Administrative Tools\Event Viewer

						0			
1		Even	t Viewer					 x	
File Action View Help									_
Event Viewer (Local)	Application Nu	mber of events: 300					Actions		
⊿ Gustom Views	Level	Date and Time	Source	Event ID	Task C		Application	•	^
Administrative Events	(i) Information	3/18/2015 3:50:47 PM	Deskto	9009	None		open Saved Log		
⊿ 🖺 Windows Logs	(i) Information	3/18/2015 12:55:37 PM	LoadPerf	1000	None		Create Custom View.		
Phication	() Information	3/18/2015 12:55:37 PM	LoadPerf	1001	None		Import Custom View.		
Security		3/18/2015 12:54:44 PM	VSS	8224	None	\sim	Classing		
Sustem	Event 9009, Deskt	op Window Manager				×			
Forwarded Events	General Detail					_	Y Filter Current Log		
Applications and Services Lo	Detail	S					Properties		
📑 Subscriptions	The Desktop	The Desktop Window Manager has exited with code (0xd00002fe)				Ì	🔐 Find		=
					Save All Events As				



		Log Properties - Application (Type: Administrative)	
General	Subscriptions		
Full N	lame:	Application	
Log p	ath:	%SystemRoot%\System32\Winevt\Logs\Application.evtx	
Log s	ize:	1.07 MB(1,118,208 bytes)	
Creat	ed:	Tuesday, November 4, 2014 4:35:48 AM	
Modi	fied:	Wednesday, March 18, 2015 12:52:13 PM	
Acces	ssed:	Tuesday, November 4, 2014 4:35:48 AM	
✓ Ena Maxin Wher	able logging mum log size (K n maximum ever	B): 32768	
۲	Overwrite ever	ts as needed (oldest events first)	
0	Archive the log	when full, do not overwrite events	
0	Do not overwri	te events (Clear logs manually)	
		Clearlog	
		OK Cancel Apply	



http://../../../../windows\systems32\cmd.exe



Microsoft Baseline Security Analyzer



http://www.microsoft.com/en-us/download/details.aspx?id=7558

Microsoft Baseline Security Analyze	٢	
🍥 🔮 Microsoft Ba	seline Security Analyzer	Microsoft
Which computer	do you want to scan?	^
Enter the name of the compu	ter or its IP address.	
<u>C</u> omputer name:	WORKGROUP\MACBOOKXP 💉 (this computer)	
IP address:		
Security report name:	%D% - %C% (%T%)	
Options: Check for <u>W</u> indows	%D% = domain, %C% = computer, %T% = date and time, %IP administrative vulnerabilities	% = IP address
Check for weak pas	swords	
Check for IIS admin	strative <u>v</u> ulnerabilities	
Check for SQL admin	histrative vulnerabilities	
Configure comp	uters for Microsoft Update and scanning prerequisites	
Advanced Upda	te Services options:	
🔘 Scan using a	assigned Update Services servers only	~
FileHippo.com	(<u>S</u> tart Scan Cancel



	LAND
and the second	

QUESTION & ANSWER SESSION

Name พงศ์ระพี นาคมณี [Information Security Engineer]

e-mail : pongrapee@ega.or.th tel. : 02-612-6000(4303)



Thank You



website : www.ega.or.th e-mail : helpdesk@ega.or.th Tel. : (+66) 0 2612 6000 Hotline : (+66) 0 2612 6060