# Microsoft Windows Security

## ภัคพงศ์ กฤตวัฒน์

#### Senior Instructor (ACIS Professional Center)

Microsoft Certified Trainer, EC-Council Certified Instructor, Certified Wireless Network Trainer



Trainer







ACIS Professional Center Co., Ltd. http://www.acisonline.net



#### Security Intelligence







## **Security Guidance**

	ประเทศ	กับขะบทย⇒   Microsoft.com
Microsoft TechNet	ค้นหา TechNet โดยใช้Bing	
Security TechCenter		
Home Security Bulletins Library	Learn Downloads Troubleshooting Community	
👹 ฉบับสำหรับพิมพ์ 🕂 เพิ่มในรายการโปรด 😥 ส่ง		คลิเ
Security and Updates	TechNet 🕨 TechNet Library 🕨 Security and Updates 🕨 Security Guidance 🕨	
+ Microsoft Forefront		
Windows Rights Management Services	Switch on low bandwidth view	
<ul> <li>Security Guidance</li> </ul>		
Application Security	Security Guidance	
Client Security	Please see the TechNet Security Center for links to technical bulleting, advisories, update	es tools and prescriptive
Data Protection and Privacy	guidance designed to help IT pros keep Microsoft servers, desktops, and applications up	to date and secure.
<ul> <li>Identity and Access Management</li> </ul>		
+ Network Security	จัดการโปรไฟล์ของคุณ   กฎหมาย   ติดต่อเรา	Microsoft
Regulations and Standards	© 2009 Microsoft Corporation สงวนลิขสิทธิ์ ข้อคำหนดการใช้   เครื่องหนายการค้า   คำขี้แจงเกี่ยวกับสิทธิ์ส่วนบุคคล	moroson
Risk Management		
Secure Messaging and Collaboration		
+ Security Columns		
Security Policy and Operations		
Small Business		
Threats and Vulnerabilities		





## Security Compliance Management Toolkit series

- Windows Server 2008
- Windows Server 2003
- Windows Vista
- Windows XP
- Microsoft Office 2007





### **Other Security Guidelines**

- DISA STIGs
- NSA IA Guidance
- The CIS Benchmarks





## DISA (http://www.disa.mil)







**Consent Notice** 

## **DISA STIGS**

- <u>Security Checklists</u>
- <u>Security Readiness</u>
   <u>Review Evaluation</u>
   <u>Scripts</u>
- <u>Security Technical</u> <u>Implementation</u> Guides

#### Security Technical Implementation Guides (STIGS) and Supporting Documents

IA News

Subject Matter Links:

#### STIGS:

- STIG Development Process and Bi-

Information Assurance Support Environment

Monthly Release Update Process

- FSO Release Schedule - Update!

- Security Checklists
- FSO Scan Team Info (DKO account and

CAC login is required)

- Security Readiness Review

Evaluation Scripts

- Security Technical Implementation

Guides (STIGS)

- DRAFT STIGS and Security
- Checklists
- DoD General Purpose STIG,
- Checklist and Tool Compilation CD
- -FSO Whitepapers

Guides in PKI-enabled area (DoD PKI

cert req'd)

Common Control Indentifier (CCI)



What's New

#### STIG-News Mailing List:

Security & Privacy | Accessibility

Subscribe, if you would like to know when the latest STIGs are available.

The STIGs and the NSA Guides are the configuration standards for DOD IA and IAenabled devices/systems.

A Security Checklist (sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration) is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security.

Security Readiness Review Scripts (SRRs) test products for STIG compliance. SRR Scripts are available for all operating systems and databases that have STIGs, and web servers using IIS. The SRR scripts are unlicensed tools developed by the Field Security Office (FSO) and the use of these tools on products is completely at the user's own risk.

Questions or comments? Please contact DISA Field Security Operations (FSO) Helpdesk Email: <u>fso\_spt@disa.mil</u>

http://iase.disa.mil/stigs/





## NSA (http://www.nsa.gov)







## Center for Internet Security (http://www.cisecurity.org)

the CEN INTERN	ITER for ET SECURITY	SITE MAP CONTACT US PRIVACY POLICY
HOME WHAT'S NE	W WHAT IS CIS? BENCHMARKS/TOOLS OTHER RESOURCES JO	IN US TESTIMONIALS FAQ
Members Site 🕦	Measurably reducing risk through collaboration, consensus & practical security management	ANNOUNCEMENTS )
Become a CIS member Click here for more info	The Center for Internet Security (CIS) is a not-for-profit organization that helps enterprises reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls, and provides enterprises with resources for measuring information	SECURITY METRICS Well-defined metrics are essential to determine which security practices are wordth the investment _ listen to this CIS
CIS Members Worldwide Click here for more into	security status and making rational security investment decisions.	podcast and download the transcripts on Security Metrics.
Find Out How To Get In Click here for more into	NVOIVEd! 40 consensus Security Configuration Benchmarks for Operating Systems, Middleware, Software Applications and Network Devices.	CIS MEMBER AND DEVELOPER UPDATE Learn about NEW resources CIS is developing to help Members and the IT security community. Click Here to
US Federal government agency licens Click here for more info	se. Click Here to download the Benchmarks.	view or download the web cast.  CIS WEB EVENT:
CIS certifies commercial	CIS Configuration Benchmark Scoring Tools	CIS web event on Configuration Management - What is it and How Do
Click here for more into		Baptie and Company. Click Here to register for the event.
CIS licenses resources for commercial use. Click here for more into	Consensus Based Metrics for Information Security Click Here for more information.	CIS WEB EVENT ON PROTECTING INFORMATION CIS web event archive on Protecting





## Hardening Concept

- Reduce Attack Surface
- Defense In Depth
- Least Privilege
- Fail to Secure Mode





#### **Attack Surface**

## The "Attack Surface" is the sum of the ways in which an attacker can get at you

Smaller Attack Surface is better

Which one has the Smaller attack surface?







## **Understand Your Attack Surface**

- Networking protocols that are enabled by default
- Network Endpoints
- Code that auto-starts or will execute when accessed
  - Examples: Services, daemons, ISAPI filters and applications,
     SOAP services, and Web roots
- Reusable components
  - ActiveX controls, COM objects, and .NET Framework assemblies, especially those marked with the AllowParticallyTrustedCallersAttribute)
- Process identities for all the code you run



User accounts installed



## HARDENING



ACIS Professional Center Co., Ltd. http://www.acisonline.net

















Defense in Depth

## HARDENING





## **Defense In Depth**

- Don't count on one line of defense for everything
  - What if the attacker penetrates that defense?
  - Contain the damage
- An example Nuclear Plants
  - "Multiple redundant safety systems. Nuclear plants are designed according to a "defense in depth" philosophy that requires redundant, diverse, reliable safety systems. Two or more safety systems perform key functions independently, such that, if one fails, there is always another to back it up, providing continuous protection. "
    - - Nuclear Energy Institute





#### **Defense in Depth (MS03-007)** Windows Server 2003 Unaffected

The underlying DLL (NTDLL.DLL) not vulnerable (815021)	B Code made more conservative during Security Push
Even if it was vulnerable	IIS 6.0 not running by default on Windows Server 2003
Even if it was running	IIS 6.0 doesn't have WebDAV enabled by default
<i>Even</i> if it did have WebDAV enabled	Maximum URL length in IIS 6.0 is 16kb by default (>64kb needed)
<i>Even</i> if the buffer was large enough	Process halts rather than executes malicious code, due to buffer-overrun detection code (-GS)
<i>Even</i> if it there was an exploitable buffer overrun	Would have occurred in <i>w3wp.exe</i> which is now running as 'network service'

Least Privilege

## HARDENING





## Least Privilege

- A defense in depth measure
- Code should run with only the permissions it requires
- Attackers can only do whatever the code was already allowed to do
- Recommendations
  - Use least privilege accounts
  - Use code access security
  - Write Apps that non-admins can actually use





Fail To Secure Mode

## HARDENING





## **Fail To Secure Mode**

- Watch out for exceptions
- Never initialize variables to success results







#### **Secure baseline**

- Settings for applications and services
- Operating system components
- Permissions and rights
- Administrative procedures
- Physical access





### **Server Hardening - Templates**

- Predefined Security Templates
- Security Guide Templates
- Industrial Templates
  - SANS
  - CIAC
  - -NSA
  - DoD DISA
- Custom Templates







### **Demo: Security Template**

Console1 - [Console Root\Security Templates\D:\Libraries	\Documents\Security\Templates\My Template\Local Policies\Security Options]		
🚟 File Action View Favorites Window Help			_ & ×
Console Root	Policy	Computer Setting	Actions
Security Templates	🖾 Accounts: Administrator account status	Not Defined	Security Options
D:\Libraries\Documents\Security\Templates	📓 Accounts: Guest account status	Not Defined	More Actions
A Account Policies	Accounts: Limit local account use of blank passwords to console logon only	Not Defined	
Bassword Policy	📓 Accounts: Rename administrator account	Not Defined	
Account Lockout Policy	📓 Accounts: Rename guest account	Not Defined	
E Kerberos Policy	📓 Audit: Audit the access of global system objects	Not Defined	=
▲ 📓 Local Policies	📓 Audit: Audit the use of Backup and Restore privilege	Not Defined	
Audit Policy	📓 Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category	Not Defined	
📲 User Rights Assignment	📖 Audit: Shut down system immediately if unable to log security audits	Not Defined	
Security Options	📖 DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	
Event Log	📖 DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	
Restricted Groups	📖 Devices: Allow undock without having to log on	Not Defined	
🔂 System Services	B Devices: Allowed to format and eject removable media	Not Defined	
📴 Registry	B Devices: Prevent users from installing printer drivers	Not Defined	
📴 File System	B Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined	
	B Devices: Restrict floppy access to locally logged-on user only	Not Defined	
	B Domain controller: Allow server operators to schedule tasks	Not Defined	
	B Domain controller: LDAP server signing requirements	Not Defined	
	B Domain controller: Refuse machine account password changes	Not Defined	
	📓 Domain member: Digitally encrypt or sign secure channel data (always)	Not Defined	
	B Domain member: Digitally encrypt secure channel data (when possible)	Not Defined	
	B Domain member: Digitally sign secure channel data (when possible)	Not Defined	
	📖 Domain member: Disable machine account password changes	Not Defined	
	📖 Domain member: Maximum machine account password age	Not Defined	
	📓 Domain member: Require strong (Windows 2000 or later) session key	Not Defined	
	📓 Interactive logon: Display user information when the session is locked	Not Defined	
	📖 Interactive logon: Do not display last user name	Not Defined	
	B Interactive logon: Do not require CTRL+ALT+DEL	Not Defined	
	📓 Interactive logon: Message text for users attempting to log on	Not Defined	
	Interactive logon: Message title for users attempting to log on	Not Defined	
	B Interactive logon: Number of previous logons to cache (in case domain controller is not available)	Not Defined	
	Interactive logon: Prompt user to change password before expiration	Not Defined	
	Interactive Legens Pequire Domain Controller authentication to unlock workstation	Not Defined	· •
		•	





## **Template Deployment**



- Test before deployment
- Periodic analysis
  - Security Configuration and Analysis snap-in
  - Scripting (Secedit.exe)
- Deployment Methods
  - Group Policy (Active Directory)
  - Security Configuration and Analysis snap-in
  - Scripting (Secedit.exe)





### **GPOAccelerator**

 A tool that you can use to create all the Group Policy objects (GPOs) you need to deploy your chosen security configuration.



#### **GPOAccelerator**





## **GPOAccelerator (cont)**

💁 Administrator: Gl	POAccelerator Command-line
C:\Program Fil Microsoft (R) Copyright (C)	es\GPOAccelerator>GPOAccelerator.wsf Windows Script Host Version 5.7 Microsoft Corporation. All rights reserved.
Create Securit Usage: GPOAcce GPOAcce GPOAcce GPOAcce GPOAcce	y Guide GPOs lerator.wsf {/Enterprise   /SSLF} /Office lerator.wsf {/Enterprise   /SSLF} [/LAB] {/Vista   /XP   /WS08} lerator.wsf {/Enterprise   /SSLF} [{/Desktop   /Laptop}] {/Vista   /XP} lerator.wsf {/ConfigSCE   /ResetSCE} lerator.wsf /Restore {/Vista   /XP}
Options:	
/WS08	: Creates Windows Server 2008 Security Guide GPOs.
/WSØ3	Requires /Enterprise or /SSLF options. : Creates Windows Server 2003 Security Guide GPOs. Requires /Enterprise or /SSLF options.
/Vista	<ul> <li>Creates Windows Vista Security Guide GPOs.</li> <li>Requires /Enterprise or /SSLF options.</li> </ul>
XP	: Creates Windows XP Security Guide GPOs. Requires /Enterprise or /SSLF options.
/Office	: Creates 2007 Office Security Guide GPOs. Requires (Enterprise or (SSLE options
∕OfficeLocal	<ul> <li>Applies 2007 Office Security Guide settings to Local Policy.</li> <li>Requires /Enterprise or /SSLF options.</li> </ul>
∕Lab ∕WSØ8	: Creates OU structure as prescribed in the Windows Server 2008 Security Guide. Requires /Enterprise or /SSLF options.
∕Lab ∕WSØ3	: Creates OU structure as prescribed in the Windows Server 2003 Security Guide. Requires /Enterprise or /SSLF options.
∕Lab ∕Vista	: Creates OU structure as prescribed in the Windows Vista Security Guide Requires (Entempise on (SSLE options
/Lab /XP	: Creates OU structure as prescribed in the Windows XP



#### **Baseline Compliance Management**





#### **Security Baseline Environments**

 The Legacy Client (LC) Environment
 The Enterprise Client (EC) Environment
 The Specialized Security – Limited Functionality (SSLF) Environment













#### Example: OU Structure

#### Windows XP Users OU

This OU contains the user accounts for the EC environment.

#### Windows XP Computers OU

This OU contains child OUs for each type of client in the EC environment.

**Desktop OU**. This OU contains desktop computers that constantly remain connected to the network.

Laptop OU. This OU contains laptop computers for mobile users that are not always connected to the network.









#### Example: The Configure Validation dialog box

	Minimum password length
Description:	"pass phrase" is a better term than "password." "I want to drink a \$5 milkshake" is a valid pass
Build a validation for t	he setting or object property.
Setting/Property:	Minimum password length
Operator:	Greater than or equal to
<u>⊻</u> alue:	8
Expression:	
[Minimum passwore	d length] Greater than or equal to 8
	of noncompliance events for this setting.
5pecify the severity o	





### **Example: Report**

Reports Filtered view, displaying 25 items out of 353		
Look for: desired 💌 in All Columns 💌 Eind Now Clear		
Name		
All compliance evaluation failures for a specified computer		
Compliance details for a configuration baseline		
Compliance details for a configuration baseline by configuration item		
Compliance details for a configuration baseline for a specified computer		
Compliance evaluation errors for a configuration baseline by configuration item on a computer		
Compliance evaluation errors for a configuration baseline on a computer		
Compliance evaluation errors for a configuration item on a computer		
Compliance for a computer by configuration baseline		
Compliance for a computer by configuration item		
Compliance history for a configuration item on a computer		
Computers reporting non-compliance for a specific configuration item validation criteria		
Computers with compliance evaluation failures		
Computers with compliance evaluation failures for a specific configuration baseline		







# Ensuring Secure Computer Configurations within the Federal Government

## FDCC AND SCAP





## Federal Desktop Core Configuration (FDCC)



- Standardized security configuration for Windows
- OMB and the CIO council seek to reduce federal systems vulnerability to individual and state sponsored cyber terrorism
  - "OMB Deep Dive" (Office of President initiative)
    - New government wide program (DOD, Intel, Civilian) that leverages existing components
- Deadline for deployment is February, 2008
- Scope of program requires automation





## Information Security Automation Program (ISAP)

- Interagency (NIST, NSA, DISA, OSD, DHS) response to the need for consistent standards-based vulnerability management in the federal government and private industry.
- Automate the implementation of information system security controls in the IT systems through security-data sharing in standard formats.
- Security Content Automation Protocol (SCAP) is the technical implementation of ISAP





## Security Content Automation Protocol (SCAP)

- Enables standardized and automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA and DoD 8500.2/8510 compliance)
- Enumeration of vulnerabilities, misconfigurations, platforms, and impact
- Machine readable security configuration checklists





## SCAP Components: Six open XML standards

Common Vulnerabilities and Exposures (CVE)	<ul> <li>Dictionary of security related software flaws</li> </ul>
Common Configuration Enumeration (CCE)	<ul> <li>Dictionary of software misconfigurations</li> </ul>
Common Platform Enumeration (CPE)	<ul> <li>Standard nomenclature and dictionary for product naming</li> </ul>
eXtensible Checklist Configuration Description Format (XCCDF)	<ul> <li>Standard XML for specifying checklists</li> </ul>
Open Vulnerability Assessment Language (OVAL)	<ul> <li>Standard XML for checking machine state</li> </ul>
Common Vulnerability Scoring System (CVSS)	<ul> <li>Standard for scoring the impact of vulnerabilities</li> </ul>





#### **SCAP Interoperability**

Software Flaw Management



#### **SCAP Vendors** SPAWAR **McAfee**<sup>®</sup> the **CENTER** for nCırcle° TERNET SECURITY Systems Center ATLANTIC symantec. **Telos** Proactive Network Security NIE, 0 $/\Delta$ Network Security Atlantic Systems Transforming IT Management-Group, Inc. Service-Disabled Veteran-Owned Small Business **QUALYS**° FURTIDET BIGFIX 🔇 Shavlik GIDEON TECHNOLOGIES Enew year assets. Know your risk THE INFORMATION ASSURANCE EXPERTS RAPID7 net 🔟 Attachmate<sup>®</sup> Business Microsoft\* Lumension System Center Triumfant **SECURITY**<sub>M</sub> Configuration Manager ecurity beyond the eda



#### **SCCM and SCAP**







### **SCAP Checklists**

- SCAP Checklists:
  - Windows Vista (FDCC Profile)
  - Windows XP (FDCC Profile)
  - Windows Vista Firewall (FDCC Profile)
  - Windows XP Firewall (FDCC Profile)
  - Windows Server 2003
  - Red Hat Linux
  - Internet Explorer 7 (FDCC Profile)
  - Microsoft Office 2007
  - Symantec Antivirus





## **SCAP Compliance Program**

- Ensuring security tools
  - comply to the NIST Security Content Automation Protocol (SCAP)
  - enable agencies to continuously monitor systems against OMB mandated configuration settings (results mapped to FISMA)
- Supports Multiple Initiatives:
  - OMB FDCC Secure Configuration Effort
  - NIST FISMA Implementation Phase II (also applies to NIST HIPAA work)
  - Information Security Automation Program (ISAP): OSD, DISA, NSA, DHS, NIST
  - OSD Computer Network Defense Pilot
  - NIST Checklist Program
    - NIST National Vulnerability Database



