MINISTRY OF ICT Smart Thailand

EGA

e-Government Agency

Electronic Government Agency (Public Organization)

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

การปิดจุดอ่อนวินโดวส์

(Windows Hardening)

วัตถุประสงค์การปิดจุดอ่อน

(Harden Objectives)

เพื่อเป็นแนวทางในการกำหนดค่าความปลอดภัยให้กับระบบที่กำลังจะติดตั้งใช้งานจริง หรือการปรับปรุงแก้ไขเครื่องให้บริการที่เกิดมีจุดอ่อนให้มีการป้องกันที่เข้มแข็งขึ้น

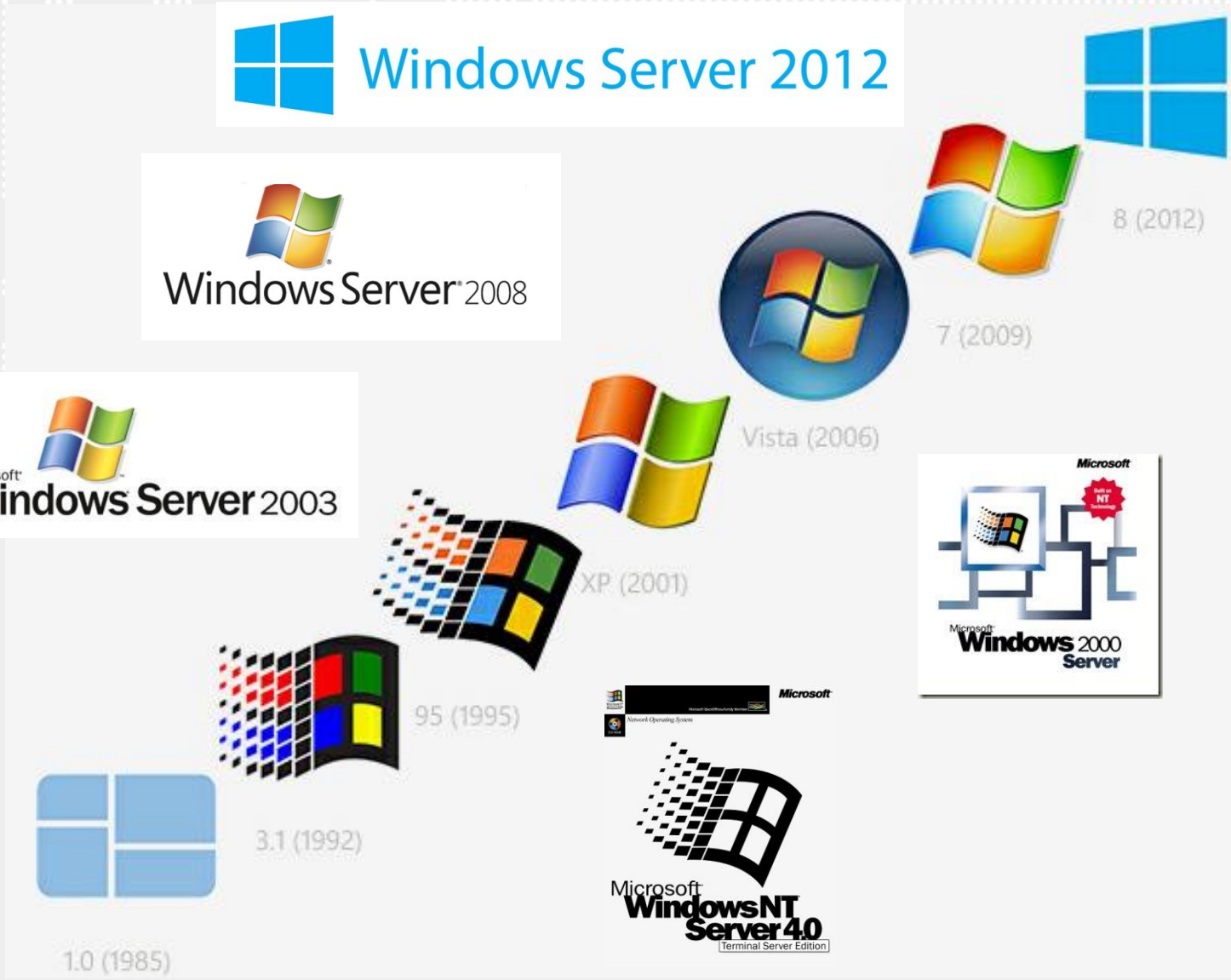
Hardening

- 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***

MS Windows Server



MS Windows Server 2012

Microsoft Corporation

The National Institute of
Standards and Technology (NIST)

Center for Internet Security (CIS)

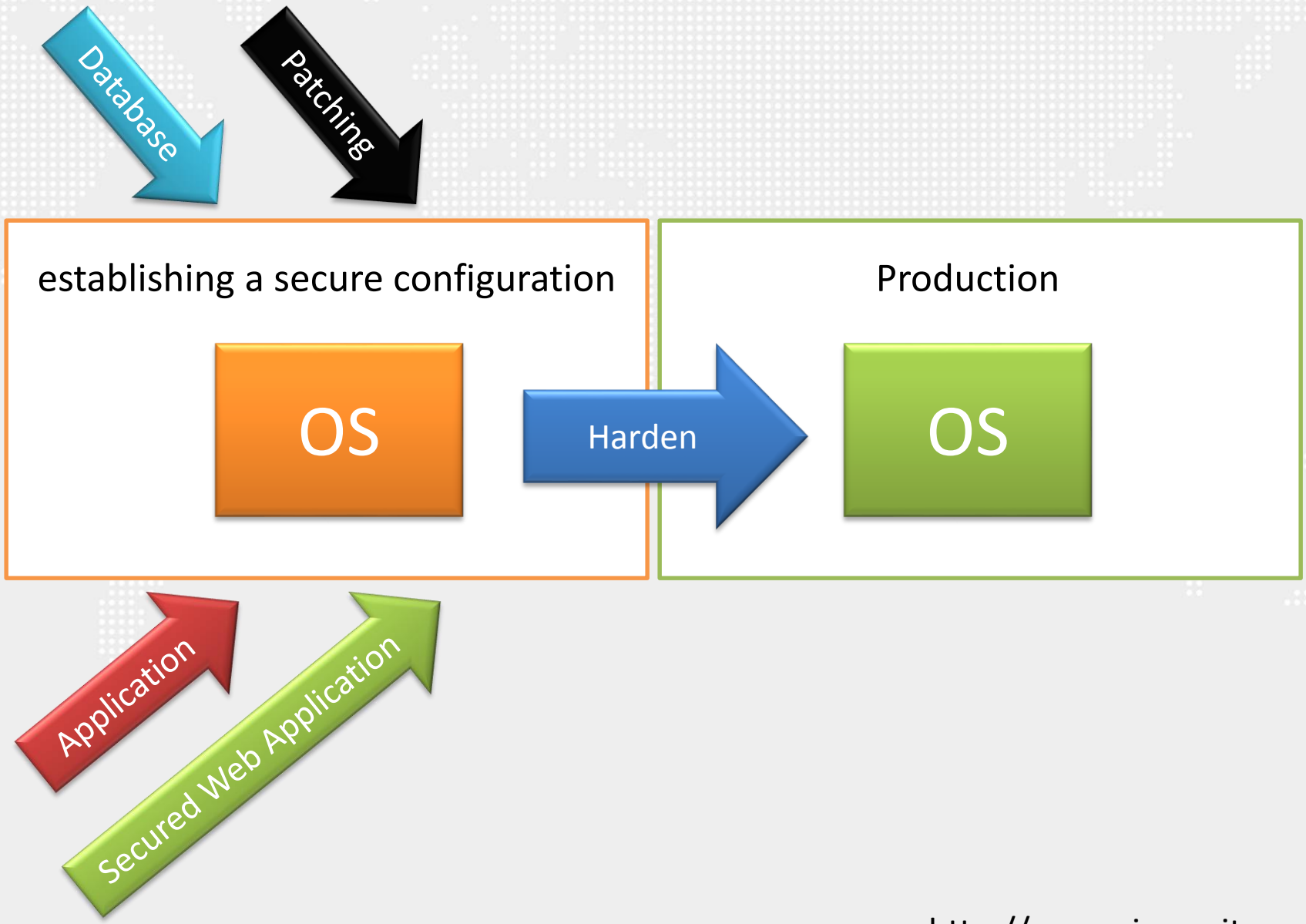
http://www.cisecurity.org/

MS Windows Server 2012

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

MS Windows Server 2012



http://www.cisecurity.org/

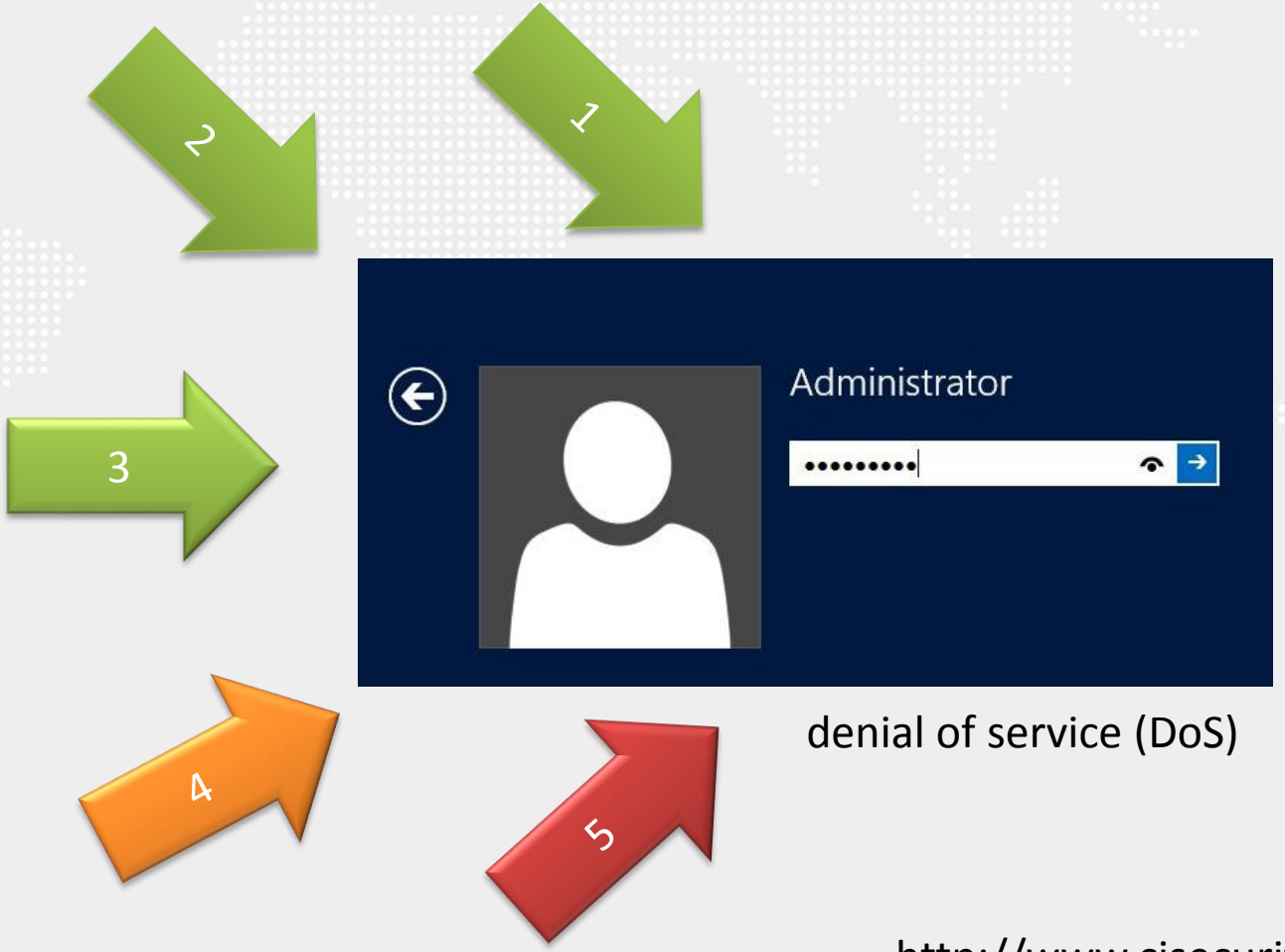
Security Settings

Account Policies

MS Windows Server 2012

Account Policies

Set 'Account lockout threshold' to '5 invalid logon attempt(s)'



denial of service (DoS)

http://www.cisecurity.org/

MS Windows Server 2012

Account Policies

Set 'Account lockout duration' to '15 or more minute(s)'

** '0' Administrator unlock manually*

http://www.cisecurity.org/

MS Windows Server 2012

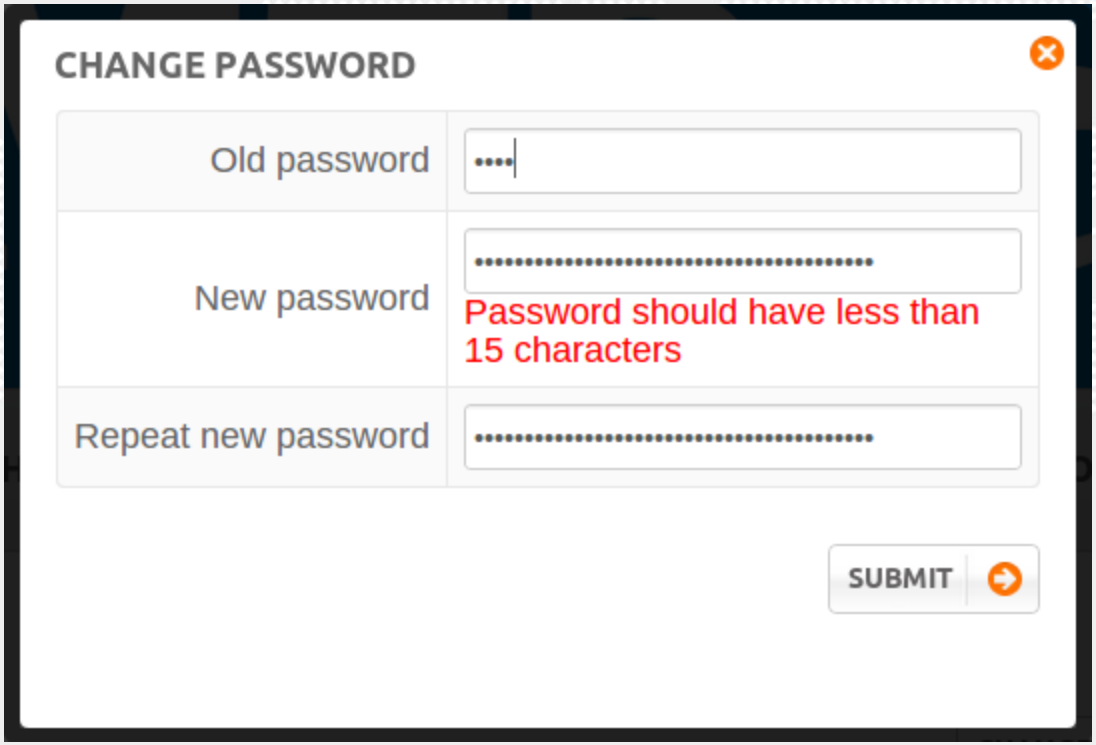
Account Policies

Set 'Reset account lockout counter after' to '15 minute(s)'

MS Windows Server 2012

Account Policies

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



MS Windows Server 2012

Account Policies

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

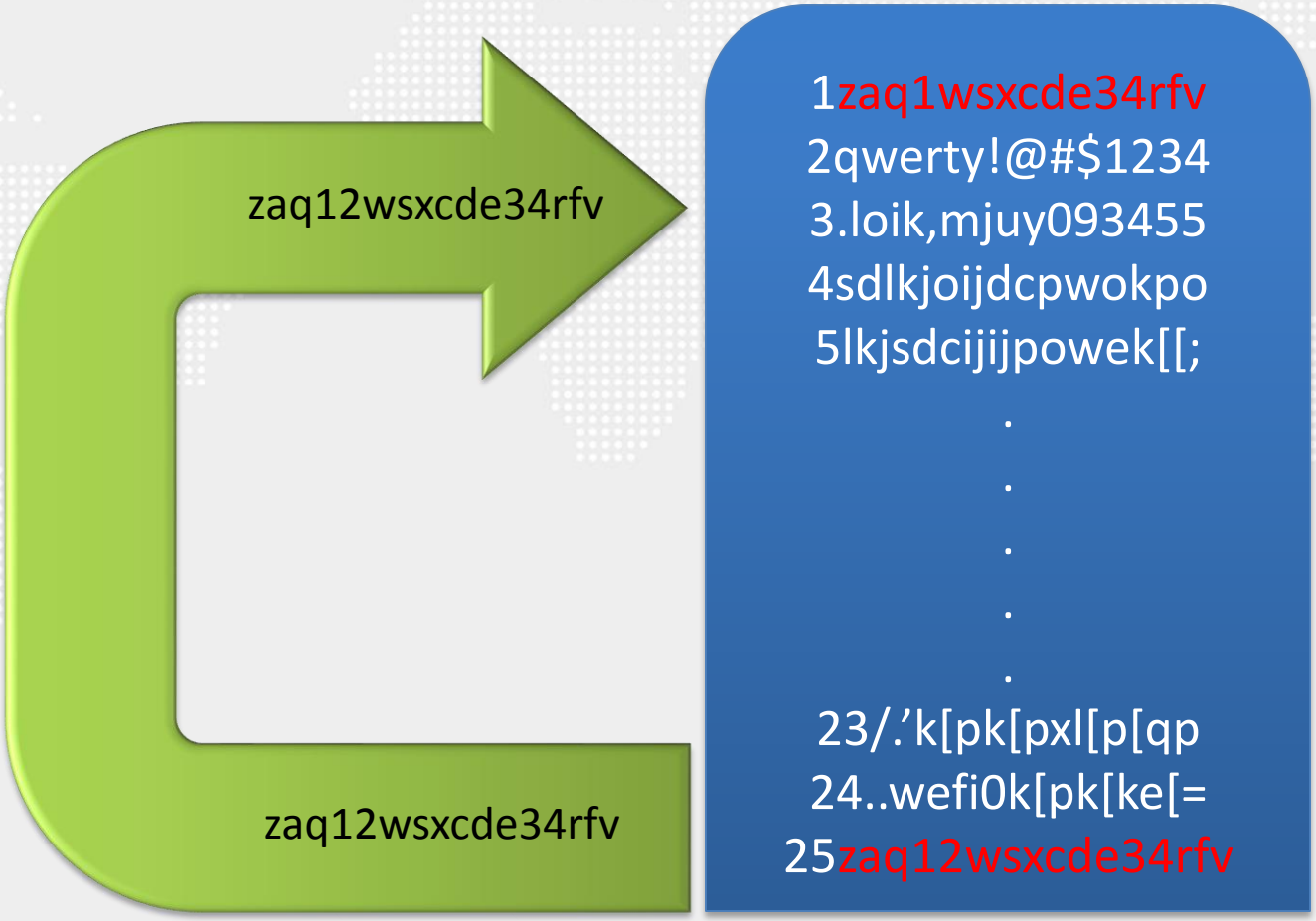
https://howsecureismypassword.net/

http://www.cisecurity.org/

MS Windows Server 2012

Account Policies

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



MS Windows Server 2012

Account Policies

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

http://www.cisecurity.org/

MS Windows Server 2012

Account Policies

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

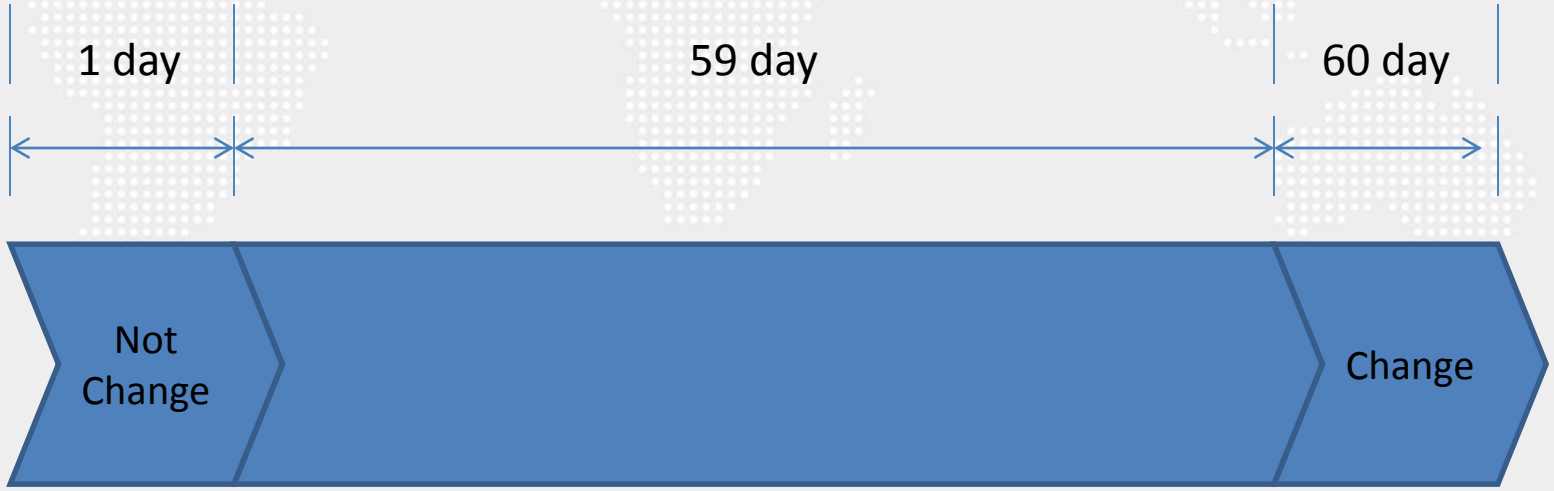
http://www.cisecurity.org/

MS Windows Server 2012

Account Policies

Set 'Minimum password age' to '1 or more day(s)'

Set 'Maximum password age' to '60 or fewer days'



MS Windows Server 2012

Advanced Audit Policy Configuration

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/

MS Windows Server 2012

Advanced Audit Policy Configuration

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'

MS Windows Server 2012

Advanced Audit Policy Configuration

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'

MS Windows Server 2012

Advanced Audit Policy Configuration

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'

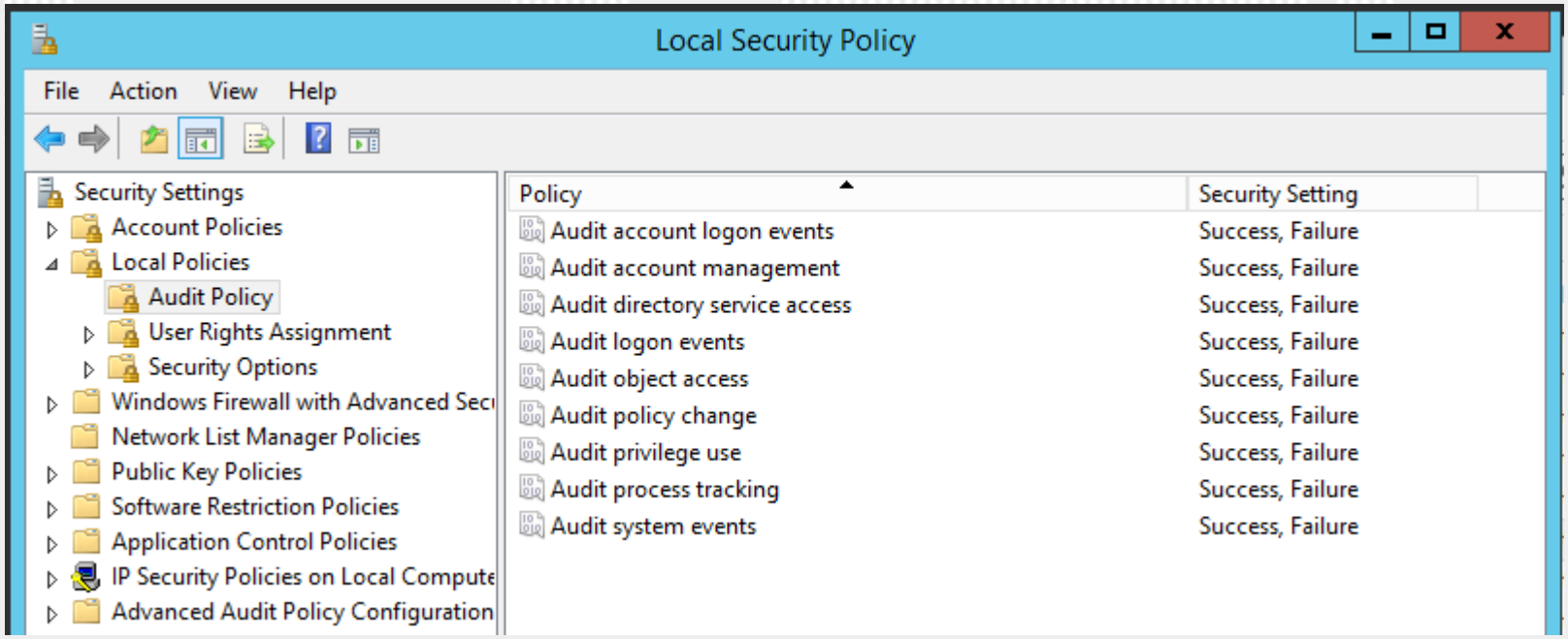
Set 'Audit Policy: System: Security System Extension' to 'Success and Failure'

Set 'Audit Policy: System: System Integrity' to 'Success and Failure'

MS Windows Server 2012

Advanced Audit Policy Configuration

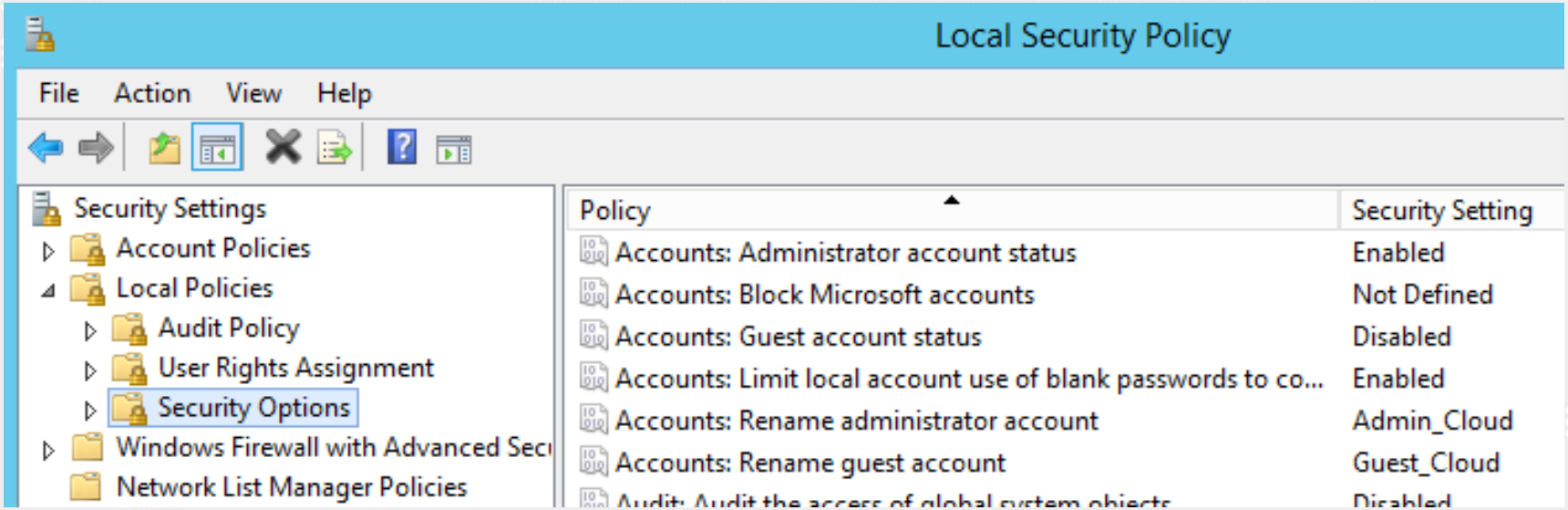
Control Panel\System and Security\Administrative Tools\Local Security Policy



MS Windows Server 2012

Security Options

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



Security Options

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'

Security Options

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'

Security Options

Devices

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

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

Security Options

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'

MS Windows Server 2012

Security Options

Interactive logon

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

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

Security Options

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)'

Security Options

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

Security Options

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'

Security Options

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'

MS Windows Server 2012

Security Options

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

MS Windows Server 2012

Security Options

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'

MS Windows Server 2012

Security Options

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'

MS Windows Server 2012

Security Options

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'

MS Windows Server 2012

Security Options

Recovery console

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

Security Options

Shutdown

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

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

Security Options

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

Security Options

System settings

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

Security Options

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'

Security Options

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 per-user locations' to 'Enabled'

MS Windows Server 2012

Security Options

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'

MS Windows Server 2012

Security Options

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'

Security Options

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'

MS Windows Server 2012

Security Options

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'

MS Windows Server 2012

Security Options

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'

MS Windows Server 2012

Security Options

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'

MS Windows Server 2012

Security Options

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'

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: Display a notification' to 'Yes'

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

MS Windows Server 2012

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)'

http://www.cisecurity.org/

Administrative Templates

Windows Components

MS Windows Server 2012

Windows Components

AutoPlay Policies

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

Windows Components

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'

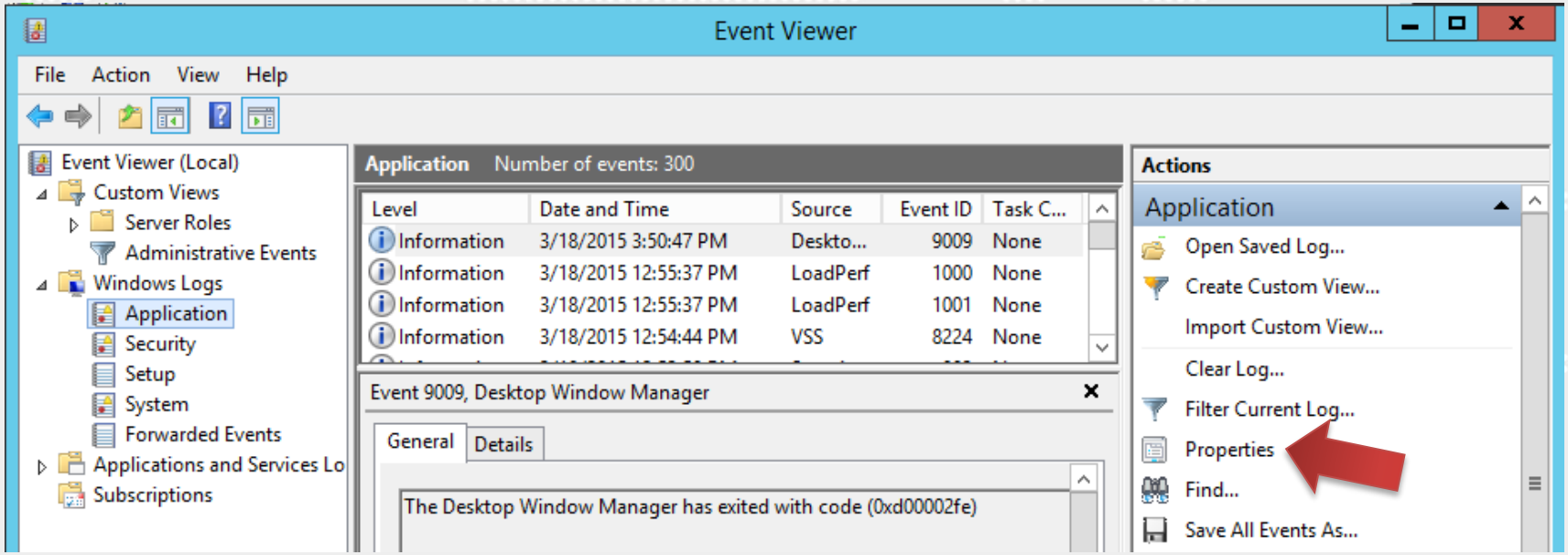
Set 'Application: Control Event Log behavior when the log file reaches its maximum size' to 'Disabled'

MS Windows Server 2012

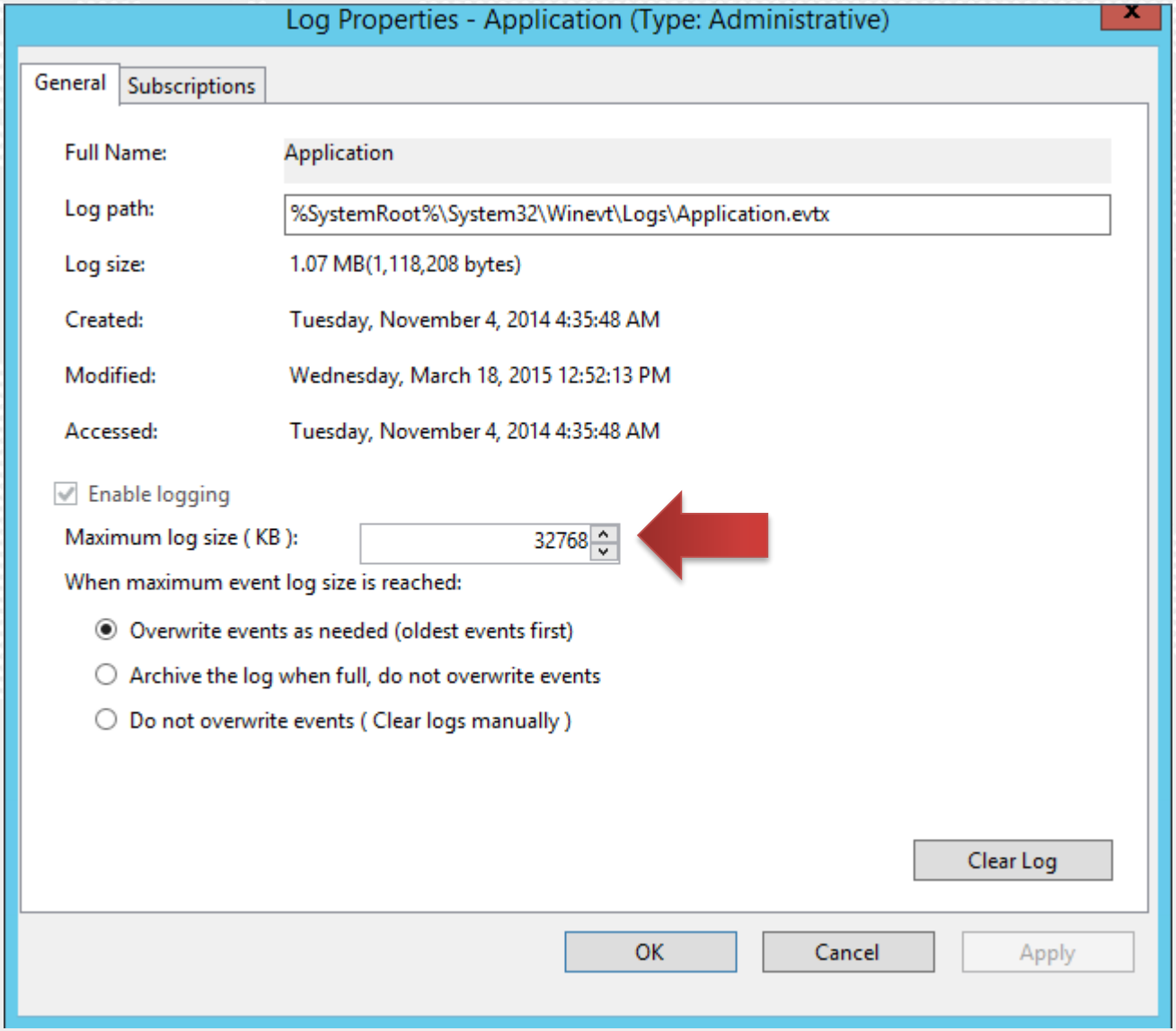
Windows Components

Event Log

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

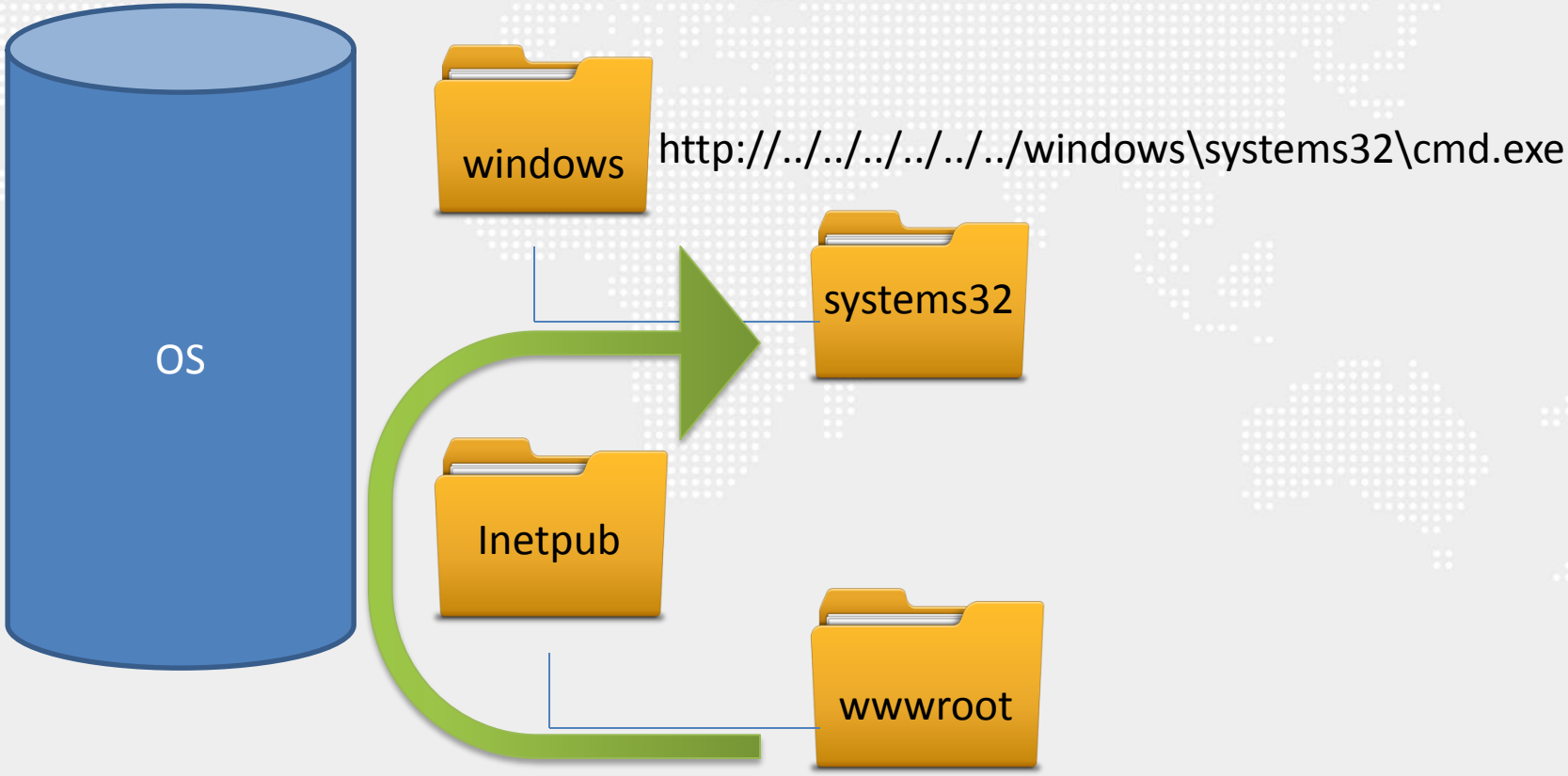


MS Windows Server 2012



MS Windows Server 2012

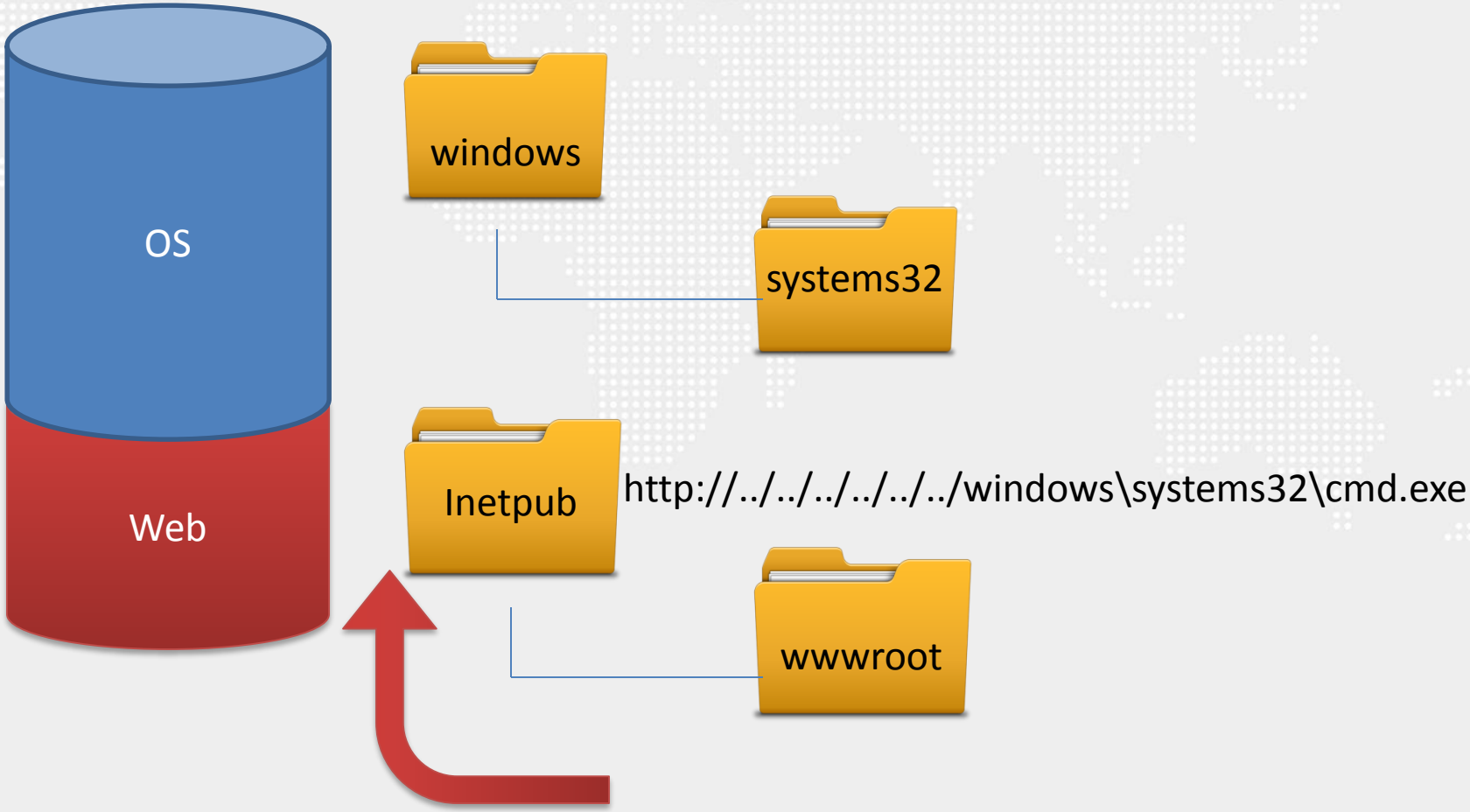
Web Server



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

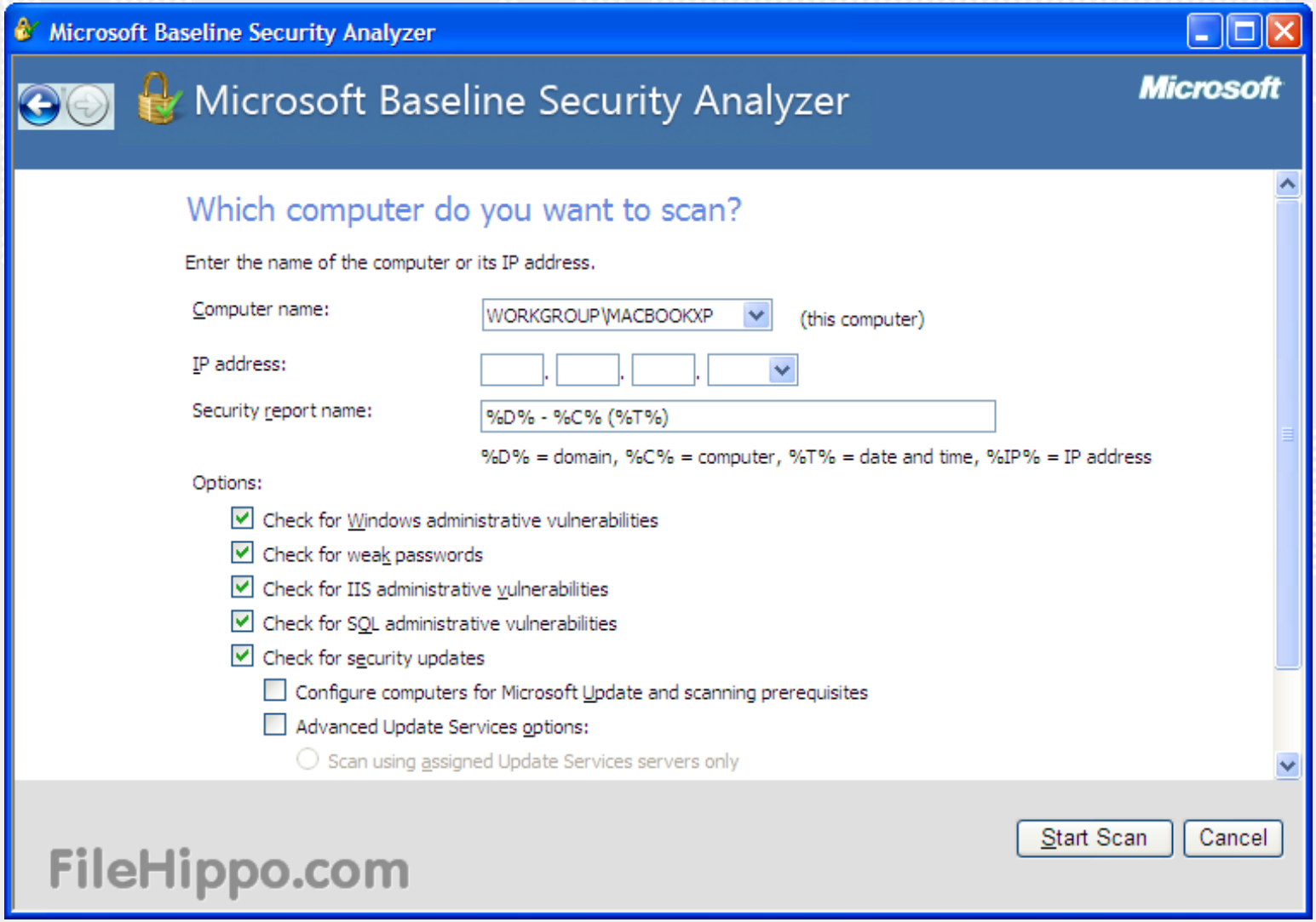
MS Windows Server 2012

Web Server



Microsoft Baseline Security Analyzer

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



QUESTION & ANSWER SESSION

Name พงศ์ระพี นาคมณี [Information Security Engineer]

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

Thank You

Electronic Government Agency (Public Organization)

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