DMZ to Desktop
Windows Server & Desktop Lockdown

Rick Kingslan
Microsoft MVP, CISSP, MCSE, MCT
West Corporation

What's a 'Microsoft MVP'?

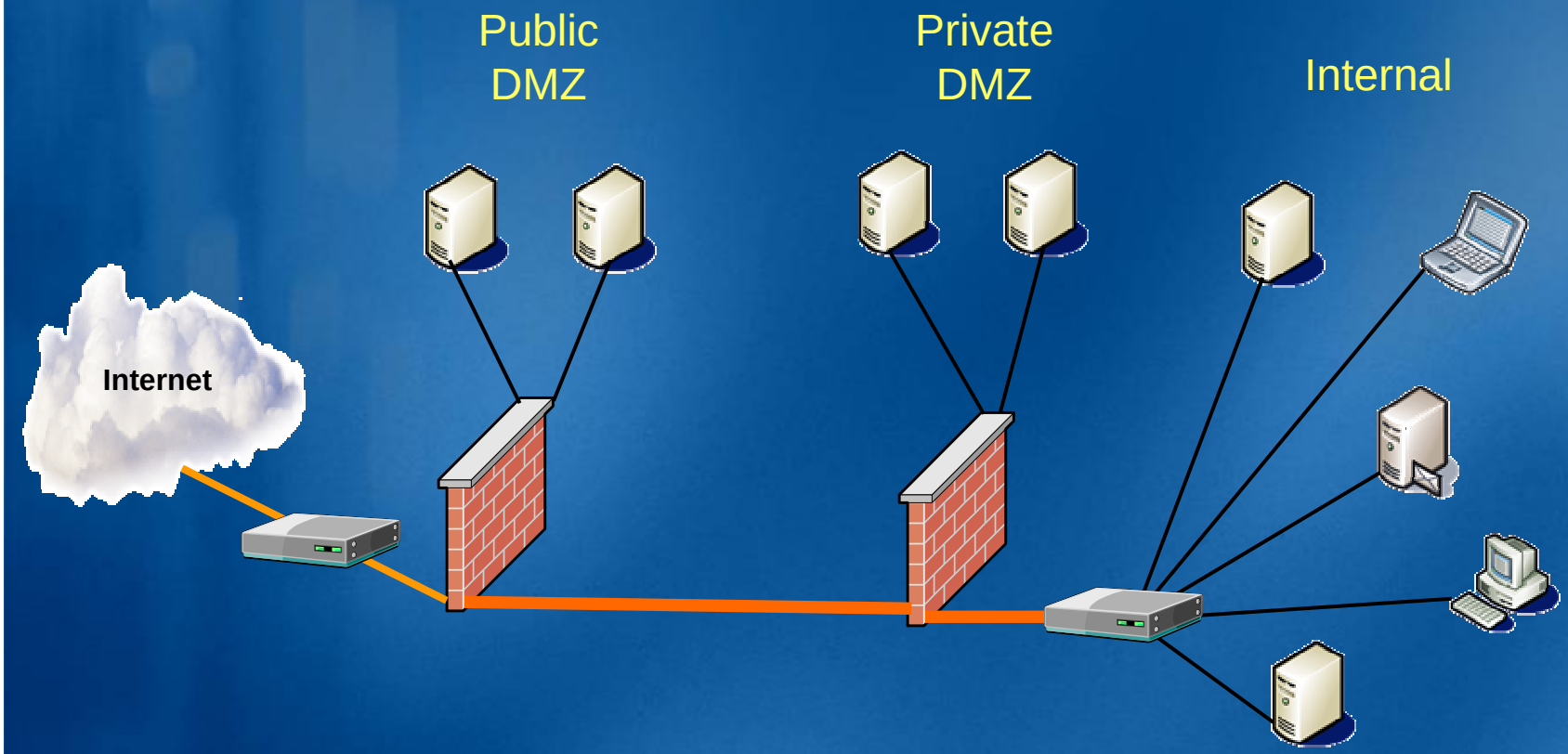
- Peer recognition award
- Commitment to Community
- Customer support – online and offline
- Authors, enthusiasts, developers, technical and business decision makers

Agenda

- Layout of Fictional Environment
- Windows Server Security
- Windows Server Security Guides
- Windows 2000/XP Security
- Security Threats and Countermeasures
- Conclusions
- Resources

Environment

East Incorporated



DMZ Rules

- **Public DMZ systems are not trusted**
- **Private DMZ Systems are more trusted**
- **Internal network is completely trusted**
- **Well, almost……**

All of this is based upon good practice in Firewall, DMZ Host and the Internal server consistency, as well as strong security practice and policy – backed by Management and confirmed by audits.

Lockdown of DMZ Hosts

- Hosts are *not* Domain Members
- Lockdown is accomplished by Local Policy
- Security Configuration and Analysis tool
- IPSec filters for port:host communication control
- Only ‘Necessary’ Services are on
- Windows 2003 Server – use the FIREWALL!

Host Release to Production

- Requirements are gathered for application
- Initial Baseline Lockdown is done
- ALL current patches are installed
  - Read to be ‘Applicable patches’
- Application is installed
- Final lockdown, with IPSec filters
- Application testing
- Certified OS is sent to InfoSec for Accreditation
- Ports are opened in Firewall
  * Tip: Vuln Scan BEFORE sendng to InfoSec!

IPSec Filters

- Windows 2000 uses the IPSecpol tool
  - **http://tinyurl.com/4xh8j**
- Windows 2003 uses NETSH
- Both are managed and monitored through the IPSec Policy snap-in

Windows 2000 IPSec with IPSecPol tool

ipsecpol -w REG -p "Packet Filter" -r "SNMP Server" -f 10.0.0.0/255.0.0.0+0:161:UDP -n PASS

ipsecpol -w REG -p "Packet Filter" -r "MOM Monitoring" -f 0+10.0.35.215/255.255.255.255:1270:TCP -n PASS

ipsecpol -w REG -p "Packet Filter" -r "Terminal Server" -f *+0:3389:TCP -n PASS

ipsecpol -w REG -p "Packet Filter" -r "HTTP Server" -f *+0:80:TCP -n PASS

ipsecpol -w REG -p "Packet Filter" -r "HTTPS Server" -f *+0:443:TCP -n PASS

ipsecpol -w REG -p "Packet Filter" -r "All Inbound Traffic" -f *+0 -n BLOCK

Wndows 2003 IPSec with NETSH

:IPSec Policy Definition
netsh ipsec static add policy name="Packet Filters - IIS" description="Server Hardening Policy" assign=no

:IPSec Filter List Definitions
netsh ipsec static add filterlist name="HTTP Server" description="Server Hardening"
netsh ipsec static add filterlist name="HTTPS Server" description="Server Hardening"
netsh ipsec static add filterlist name="Terminal Server" description="Server Hardening“

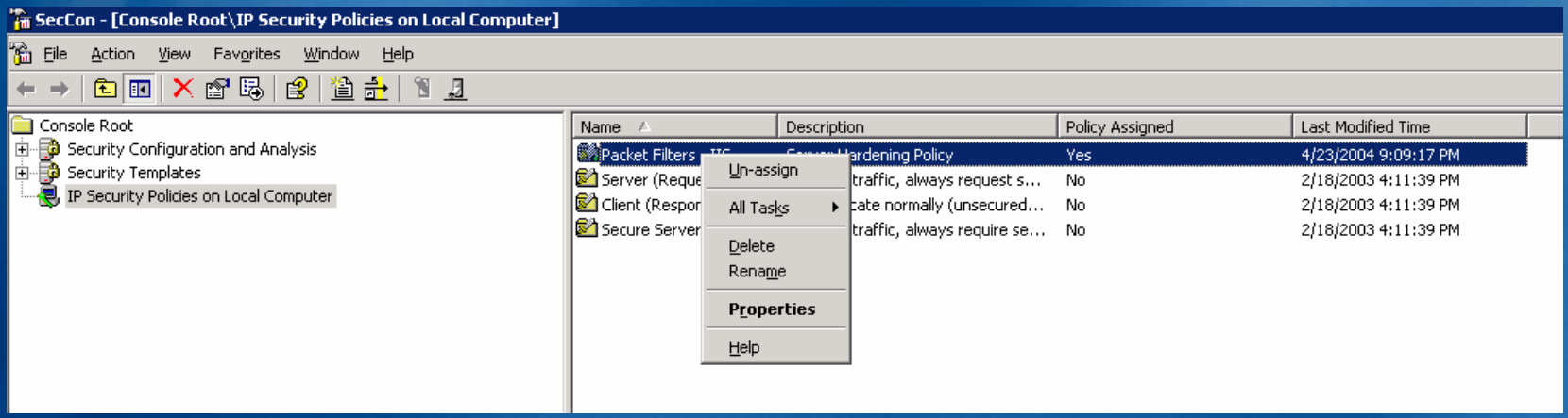
:IPSec Filter Action Definitions
netsh ipsec static add filteraction name=SecPermit description="Allows Traffic to Pass" action=permit
netsh ipsec static add filteraction name=Block description="Blocks Traffic" action=block

:IPSec Filter Definitions
netsh ipsec static add filter filterlist="HTTP Server" srcaddr=any dstaddr=me description="HTTP Traffic" protocol=TCP srcport=0 dstport=80
netsh ipsec static add filter filterlist="HTTPS Server" srcaddr=any dstaddr=me description="HTTPS Traffic" protocol=TCP srcport=0 dstport=443
netsh ipsec static add filter filterlist="Terminal Server" srcaddr=any dstaddr=me description="Terminal Server Traffic" protocol=TCP srcport=0 dstport=3389
netsh ipsec static add filter filterlist="ALL Inbound Traffic" srcaddr=any dstaddr=me description="ALL Inbound Traffic" protocol=any srcport=0 dstport=0

:IPSec Rule Definitions
netsh ipsec static add rule name="HTTP Server Rule" policy="Packet Filters - IIS" filterlist="HTTP Server" kerberos=yes filteraction=SecPermit
netsh ipsec static add rule name="HTTPS Server Rule" policy="Packet Filters - IIS" filterlist="HTTPS Server" kerberos=yes filteraction=SecPermit
netsh ipsec static add rule name="Terminal Server Rule" policy="Packet Filters - IIS" filterlist="Terminal Server" kerberos=yes filteraction=SecPermit
netsh ipsec static add rule name="ALL Inbound Traffic Rule" policy="Packet Filters - IIS" filterlist="ALL Inbound Traffic" kerberos=yes filteraction=Block

IPSec Policy Management Tool

From here, you can assign, manage, modify your policy in a GUI tool – great for fine tuning, not great for creating complex rules. Win2k and Win2k3 both.



Windows Server Lockdown

- Use Security Configuration and Analysis
  - Caveat – VERY hard to remove once applied
- Templates from Microsoft, NSA, etc.
- Should utilize a two-step method
  - Baseline policy for ALL systems
  - Role based policy for per role

Baseline Policy Extract #1

```
[Unicode]
Unicode=yes

[Version]
signature="$CHICAGO$"
Revision=1

[Event Audit]
AuditSystemEvents = 1
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 3
AuditPolicyChange = 1
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 3
AuditAccountLogon = 3

[System Access]
EnableGuestAccount = 0

[System Log]
MaximumLogSize = 16384
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

[Security Log]
MaximumLogSize = 81920
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

[Application Log]
MaximumLogSize = 16384
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

[Service General Setting]
"ALG",4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDT
        LOCRSDRCWDWO;;;WD)"
```

Baseline Policy Extract #2

[Privilege Rights]
SeInteractiveLogonRight = *S-1-5-32-547,*S-1-5-32-551,*S-1-5-32-544
SeRemoteInteractiveLogonRight = *S-1-5-32-544
SeDebugPrivilege =
SeDenyNetworkLogonRight = *S-1-5-7,*S-1-5-32-546
SeDenyBatchLogonRight = *S-1-5-32-546
SeDenyRemoteInteractiveLogonRight = *S-1-5-32-546
SeRestorePrivilege = *S-1-5-32-544
SeNetworkLogonRight = *S-1-5-32-544,*S-1-5-11
SeMachineAccountPrivilege = *S-1-5-32-544
SeSystemtimePrivilege = *S-1-5-32-544
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-544

[Registry Values]
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation=4,1
MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode=4,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta=4,10
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog=4,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog=4,20000
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog=4,20
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90
MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand=4,1
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,1
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions=4,3
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted=4,5

Role Policy – IIS Server

[Unicode]
Unicode=yes

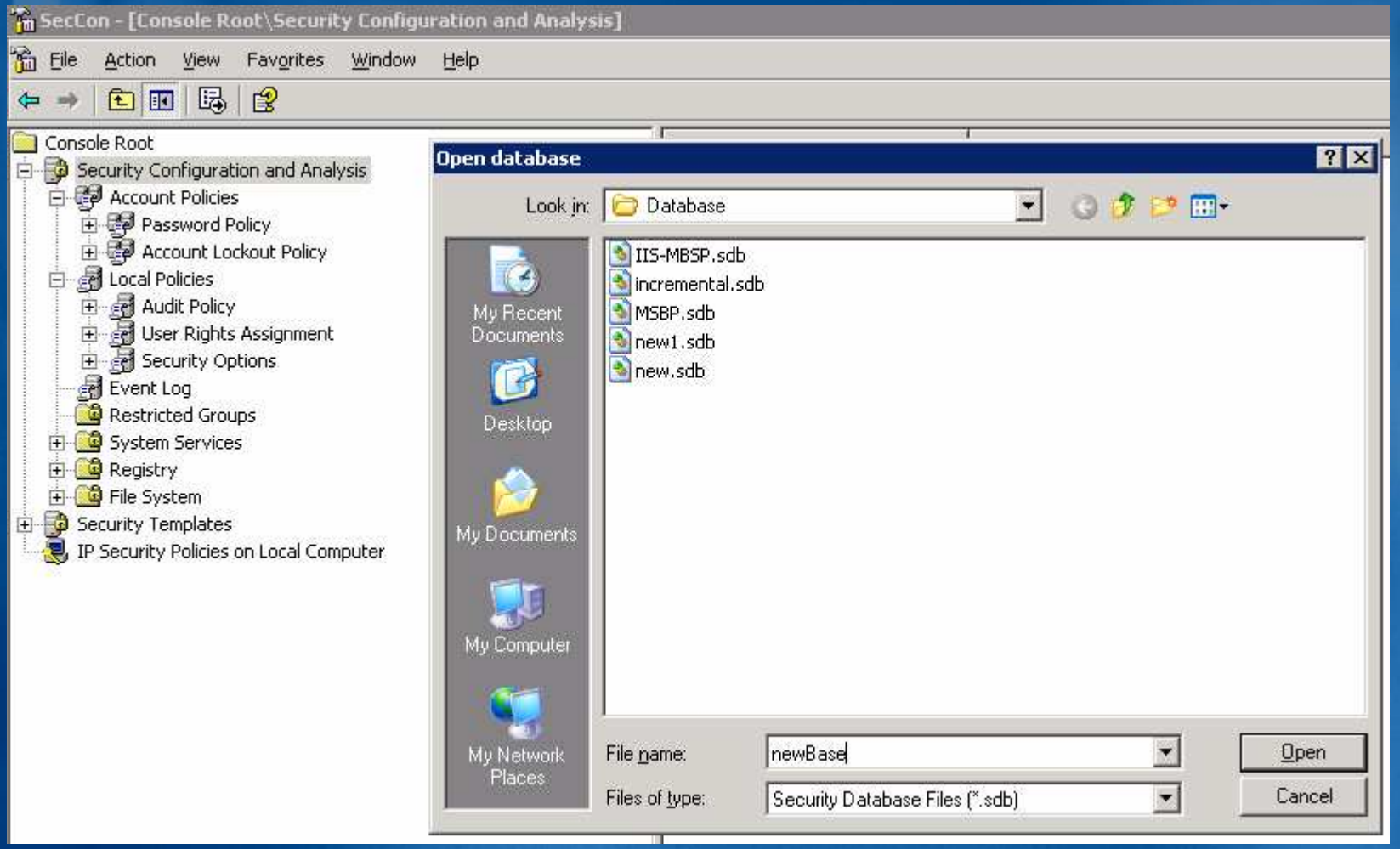
[Version]
signature="$CHICAGO$"
Revision=1

[Profile Description]
Description=Incremental Settings for an IIS Server in an environment with high security requirements.

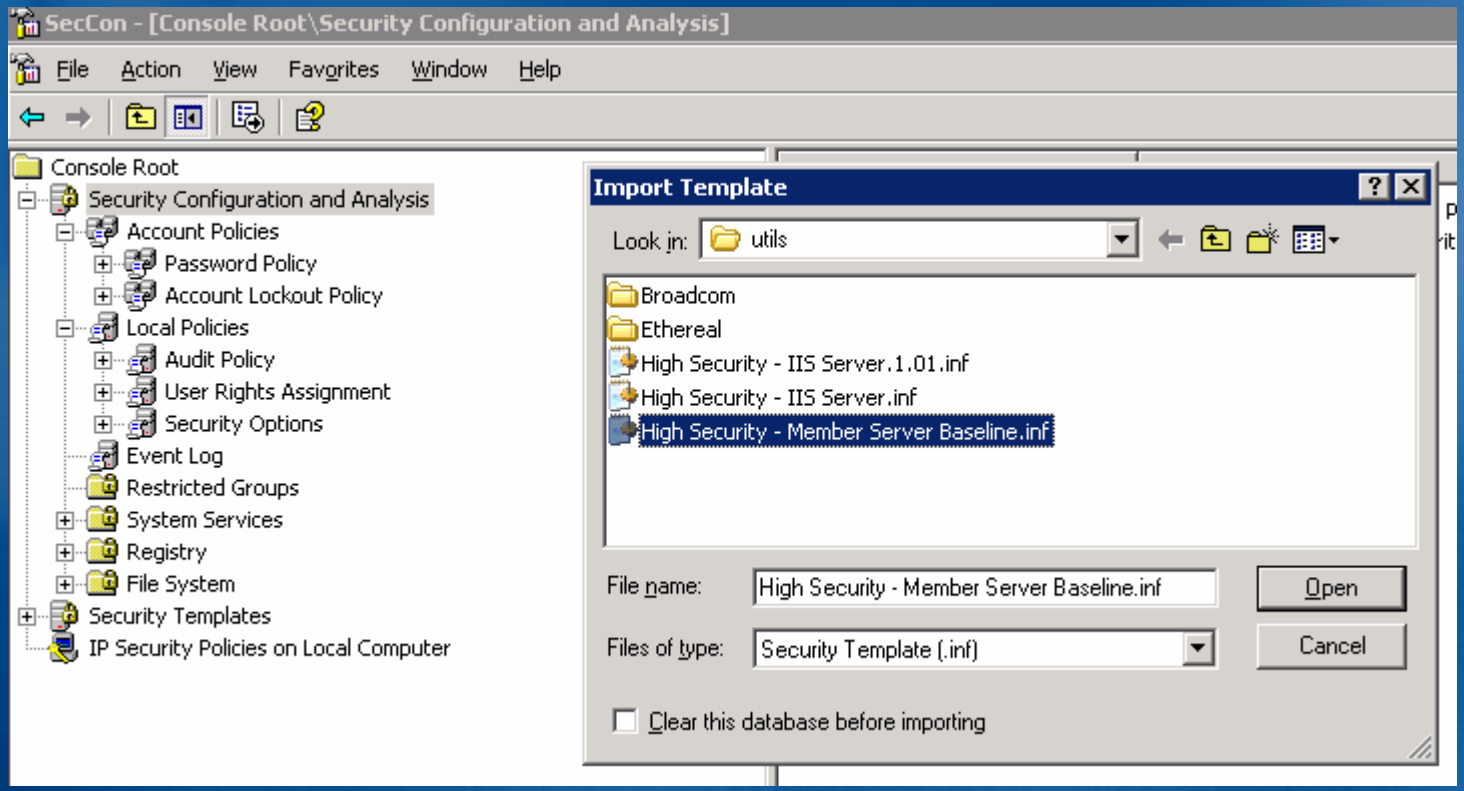
[Privilege Rights]
sedenynetworklogonright = *S-1-5-7

[Service General Setting]
1="cisvc", 2, ""“ ← start the search engine
2="httpfilter", 2, ← Apply the filter, plus assign specific perms
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
3="iisadmin", 2,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
4="netlogon", 4, ""“ ← kill off Netlogon…. It’s not a domain member, so why do we need it?
5="smtpsvc", 2, ""“ ← start up SMTP Service – we mail out from here
6="w3svc", 2,
"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

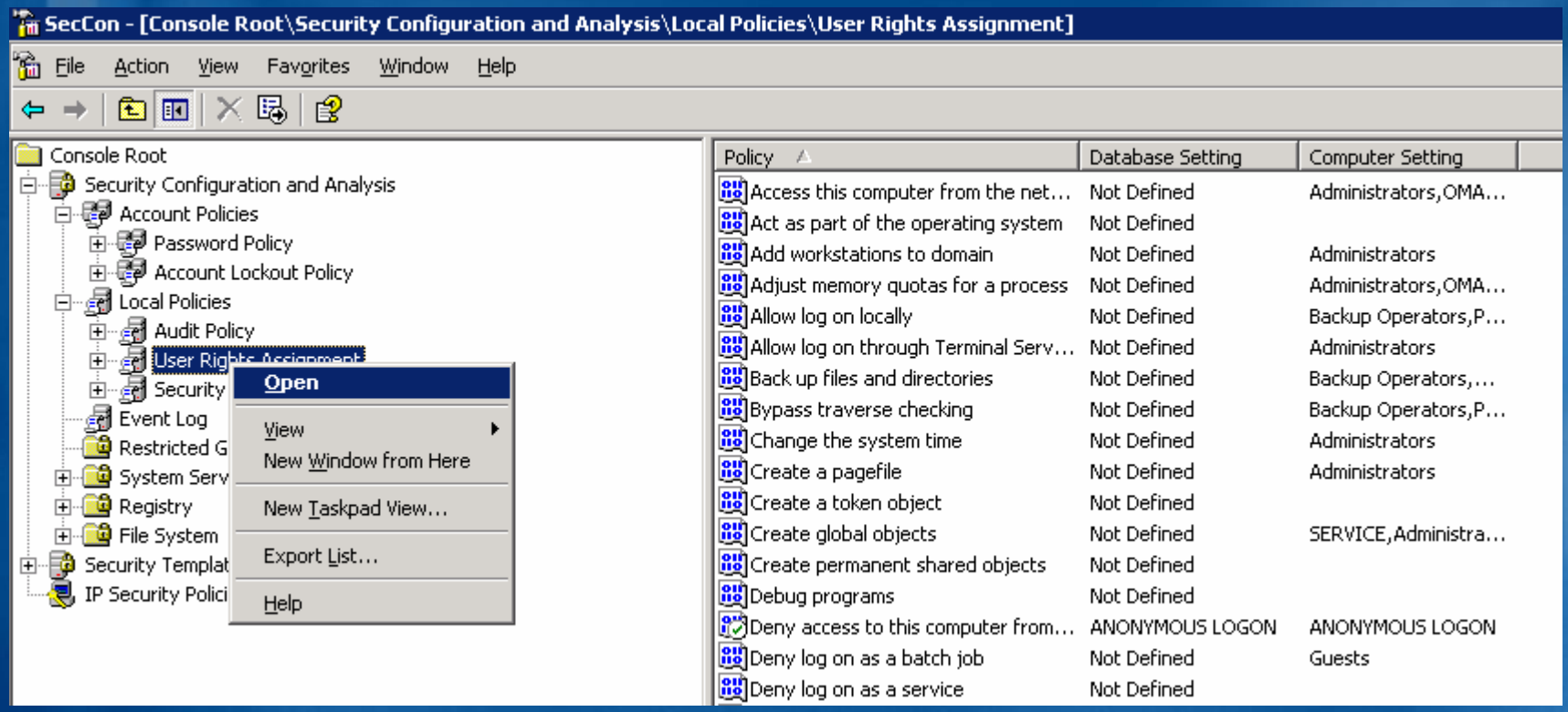
Security Configuration and Lockdown



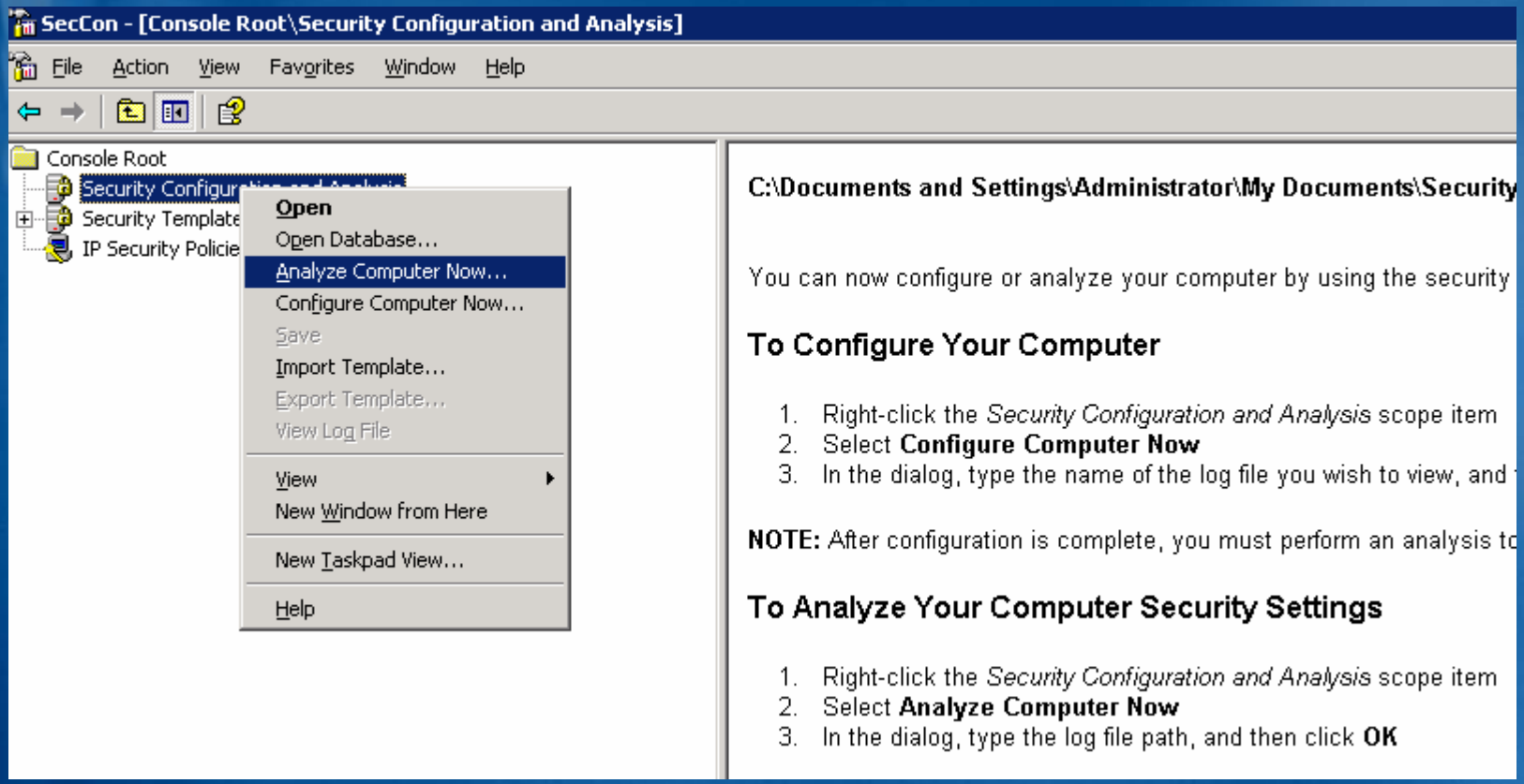
Security Configuration and Lockdown



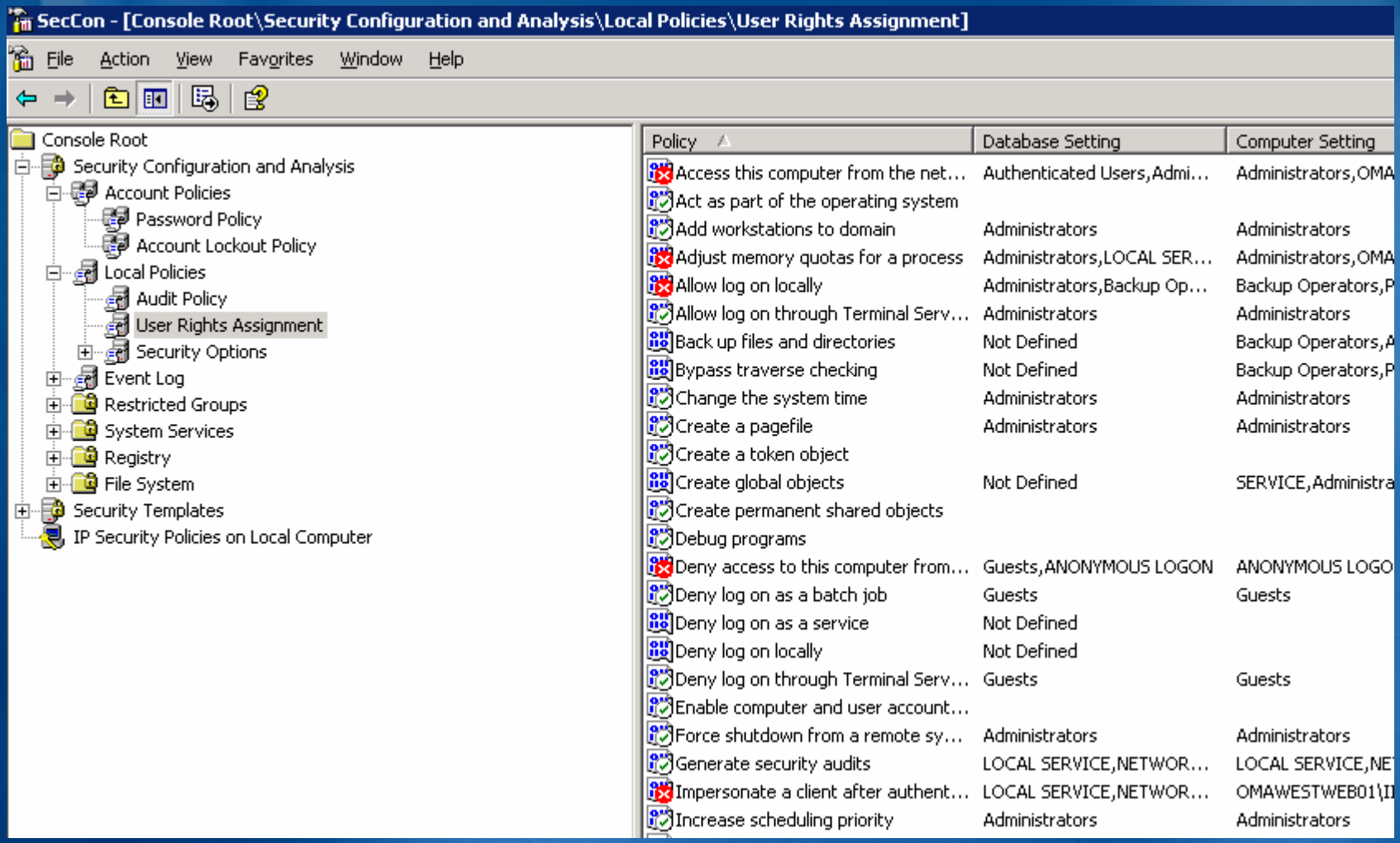
Security Configuration and Lockdown



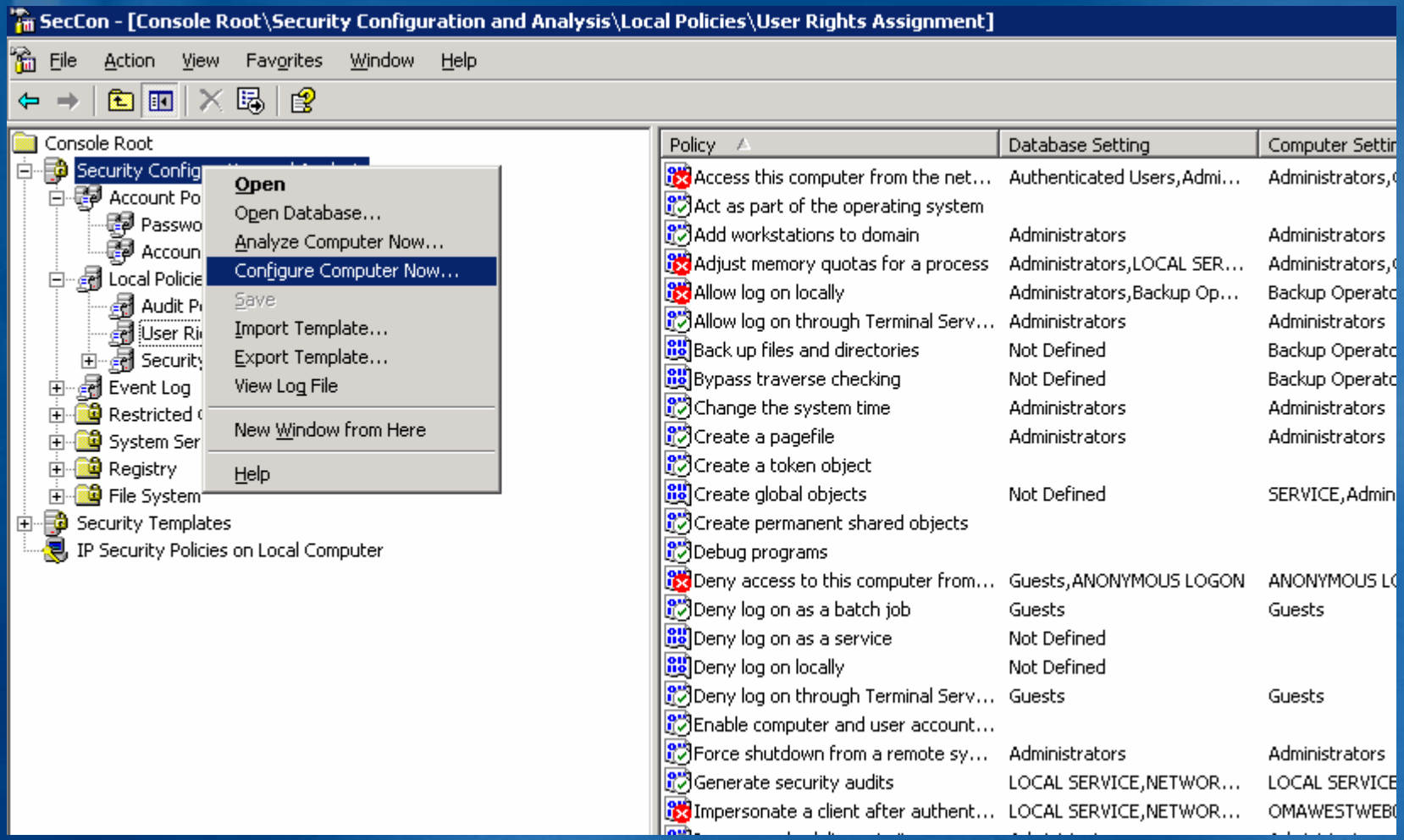
Security Configuration and Lockdown



Security Configuration and Lockdown



Security Configuration and Lockdown



Keys to the Lockdown Process

- Install ONLY what you need.
  - Do not install IIS unless it's a web server or Exchange, for example
- Be consistent on your Baseline policy
  - No deviation makes audits MUCH simpler!
- ALWAYS apply a Role-based policy
  - Every server has a role – define WHAT it will do
  - Multiple Roles can be applied
- Understand the Threats, know the Counter-Measures

Security Expressions

- Pedestal Software
- Very complex, but easy to use tool
- Provides for a log of changes
- This means, if something goes horribly wrong – the problem(s) can be reversed
- Can be scripted, own rules can be created
- Can have separation of duties for mitigating collusion
- Security Config and Analysis – on steroids

Windows Server 2003

- By default:
  - IIS is not installed
  - Most services are OFF by default
  - No more Everyone (FULL)(FULL)
  - IE is in a secured mode
  - Lots more – too much to mention
- Use the Integrated Firewall
  - NETSH is complex – this is pretty straight forward

Threats and Counter-Measures

- Not guidance, but a pointer to the guide
- Describes a series of specific threats to the OS and what to implement to mitigate the threat
- Available from Microsoft at:

http://tinyurl.com/n2yx

- Addresses both Win2k3 and Windows XP

Threat Mitigation for Desktops

- Use integrated or third party firewalls
- Ensure e-mail systems are scanning e-mail, or install scanning on client
- Anti-Virus is a must!
- All applicable patches are installed
- In a AD Domain environment, use Group Policy to force Security Policies
- If necessary, IPSec can be used internally

Domain Level Security

- Password length, complexity, history, frequency
- Lockout settings
- Kerberos settings

- These three are specific on a per Domain basis
- If you need a different Password policy for a subset of groups, you need a new Domain

Other Policy Settings

- Audit settings
- Log settings
- Restricted Groups
- System Services
- Registry
- File System

- All of the above are computer settings

Windows Software Restriction

- Confine execution to specific allowed programs
- Defined by path, hash, Authenticode signing
- Is available in Windows Server 2003, Windows XP
- Allows “run” or “don’t run” settings
- Set in GPO or Local Policy

Two-Factor Authentication

- Smart Card
  - Need some level of Certificate Authority
  - Entry cost is quite low
  - Support built into Windows OS and Active Directory
- USB-based AuthN devices
- Biometrics
  - Fingerprint readers most common
  - OK, so this is really a single-factor

Resources from Microsoft

To locate a partner who can help with Microsoft security:

Microsoft Certified Providers Directory
http://mcspreferral.microsoft.com/

Microsoft Consulting Services
http://www.microsoft.com/BUSINESS/services/mcs.asp

For training and certification questions:

Microsoft Training and Certification
http://www.microsoft.com/training

For technical information:

Security information on Microsoft Produts
http://www.microsoft.com/technet/security

Windows Server 2003
http://www.microsoft.com/windowsserver2003/

Threats and Countermeasures in Windows Server 2003 and Windows XP
http://go.microsoft.com/fwlink/?LinkId=15160

MBSA
http://www.microsoft.com/technet/security/tools/Tools/mbsahome.asp

For Security Guidance And Training

Securing Windows 2000 Server Security Solution
http://www.microsoft.com/technet/security/prodtech/Windows/SecWin2k/Default.asp

Windows 2000 Security Hardening Guide
http://www.microsoft.com/technet/security/prodtech/Windows/Win2kHG.asp

Windows Server 2003 Security Guide
http://go.microsoft.com/fwlink/?LinkId=14846

Windows XP Security Guide
http://go.microsoft.com/fwlink/?Linkid=14840

MS Learning

- Microsoft® Windows® Security Resource Kit :0-7356-1868-2

- Microsoft® Windows Server™ 2003 Deployment Kit: A Microsoft Resource Kit ISBN: 0-7356-1486-5

Thank you!


Nebraska
CERT
Conference
2004
Computer Security
and Information Assurance