

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

GCWN PRACTICAL ASSIGNMENT

Version 3.1

© SANS Institute 2003, Author retains full rights.

Option 2 – Securing a Windows 2000 DC with Exchange 2000 using Security Templates

May 2003
Prepared by: Gabriele Tansini

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ABSTRACT 2
CASE STUDY 2
Company Description 2
Domain Infrastructure 3
Client Configuration 4
Network Configuration 4
Physical Security 4
Resource/Asset that must be protected 4
SERVER CONFIGURATION 6
Hardware 6
Software 7
Considerations on applications installed 8
Consideration on future applications/modifications 9
Server Installation 10
CHOOSING THE TEMPLATE 11
Template Chosen 11
Tools Used to apply the template 12
Considerations about Security Policies Application on DCs 13
How the template will be enforced on DCs 13
TEMPLATE SETTINGS 14
Account Policies 14
Local Policies 16
Event Log 23
Restricted Groups 24
System Services 25
Registry Settings 28
File System Settings 29
APPLYING AND TESTING THE TEMPLATE 29
Monitoring Template Application 29
Testing Template Security Settings 31
Testing System's Functionality 33
CONCLUSIONS 43
APPENDIX A: SOME DEFINITIONS 45
APPENDIX B: CONSIDERATIONS ON MY SYSTEM'S ROLES 47
APPENDIX C: BRIEF DESCRIPTION OF FIREWALL CONFIGURATION 51
APPENDIX D: REFERENCES AND ADDITIONAL READINGS 52

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ABSTRACT

Windows 2000 has introduced a lot of utilities to ease the configuration of security. Security policies are among these. They are used to configure security on Windows 2000 systems and give the administrator the opportunity to export these settings in template. This option helps the administrator to test security policies before applying them to the production environment. This document discusses how to choose the correct settings for the needs of small legal office.

It is divided into 6 sections:

- "Case Study" covers the description of the environment where the server will work.
- "Server Configuration" covers the system characteristics: Hardware, Software and Installation with some considerations on the applications installed.
- "Choosing the Template" covers how the template has been chosen and how it will be implemented.
- "Template Settings" describes how I configured the template and comments to explain my decisions.
- "Testing the Template" describes the testing of the template.
- "Conclusions" is a brief comment of the project with some personal considerations.

There are also 4 Appendixes:

- Appendix A provides a list of definitions that can be useful to understand the document.
- Appendix B describes the roles covered by a single Domain Controller with Exchange 2000.
- Appendix C provides a brief description of Firewall Configuration.
- Appendix D provides references and additional readings.

CASE STUDY

Company Description

Note: "XYZ & Associates" is a fake name to identify a small legal office. Any reference or similarity to any company past, present or future is purely accidental.

The XYZ & Associates is a legal office based in only one site. There are 5 partners with 2/3 associates and 1 personal assistant each. A system administrator has been hired to manage the network. As consultant, my first task is to implement a consistent security policy on the DC.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Users have been trained to use Office 2000 (Word, Excel, PowerPoint and Outlook) and Internet Explorer. They have received a basic training on security (a few hours). The policies which I will use must be both secure and user-friendly to be accepted and used in the properly by users. After a meeting with management and the system administrator we have defined the following needs in terms of security:

1. The System Administrator must have the capacity to manage every aspect of the AD and Exchange architectures.
2. Every partner must have the right to manage accounts.
3. Principal Groups membership must be maintained as stable as possible.
4. A strict password and account lockout policy must be implemented.
5. A strict auditing must be implemented on administrative tasks and logon events.
6. Unused services must be disabled.
7. DNS must be configured to accept only approved updates.
8. Exchange 2000 must accept only MAPI connection from clients.
9. Exchange 2000 OWA may be used for testing reasons only on the local machine.
10. Policies must grant the correct functionality of programs installed on the system.

Domain Infrastructure

The company is configured as a "contained domain" where Internet connectivity is provided by an external ISP. The ISP will provide security on the following components: WAN Link, Mail Forwarder, External DNS, Web Site (hosted by the ISP) and External Router. A Symantec Enterprise Firewall ver.7.0 will be installed to enforce security at "Network" and "Application" level (Please check Appendix C for a brief description of firewall configuration). All documents will be stored in separate file server appliance (NetApp Filer) and they will be protected against viruses with Symantec Scan Engine for NetApp Filer. XYZ & Associates owns only one server and all internal services will be installed on it.

The Server will have the following roles:

1. Schema Master.
2. Domain Naming Master.
3. Infrastructure Master.
4. PDC Emulator.
5. RID Master.
6. Global Catalog.
7. Internal Mail Server.
8. Internal DNS Server.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Active Directory will be configured in “Native Mode” because both servers and clients are installed with Windows 2000.
The Exchange infrastructure will be configured in “Native Mode” because 1 Exchange 2000 server composes the Exchange organization and the compatibility with Exchange 5.5 is not needed.

Client Configuration

All clients have Windows 2000 with SP3 with Office 2000 SR-1. Outlook will connect to Exchange using MAPI mode. Symantec Antivirus 8.01 in managed mode with the Exchange snap-in will be installed to provide preemptive security against malicious code on every computer. On the administrator’s computer there will be the Antivirus server component with the administrative console which will provide centralized definition update and product management. The informations stored into the clients will be protected using EFS and they will be automatically synchronized with file server when connected to the network. The recovery key will be available only to the administrator and to the partners.

Network Configuration

XYZ & Associates has an Ethernet 100Mb/s Network with IP addresses 192.168.30.0/24. The clients will have a fixed IP address. The connectivity to the provider is supplied by an external router, which is configured to NAT internal addresses and to channel inbound and outbound SMTP traffic to Internal Mail Server. The ISP provides the Router and the system administrator cannot change its configuration. The DC IP Address is 192.168.30.200. The Router IP address is 192.168.30.1.

Physical Security

The DC will be located in a separate room. Administrator and partners will have a personal code to access the room. The access to the room will be logged by an access control system that will automatically print the information on a printer located in another protected room. The DC will be closed in a rack that can be opened using a key located in the company’s safe (a copy of the key will be deposited in a bank). Every system will be connected to a UPS. The room’s temperature will be constantly controlled by two air conditioners and a fire alarm will guarantee the protection against fires.

Resource/Asset that must be protected

Before choosing a template I must define what are exactly the resources/assets that must be protected and how tight must be the protection.

File/Documents: A legal office contains a big quantity of confidential informations that span between client informations to internal memorandum

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

about cases. All documents will be stored in the Filer. ACLs for folders will be modified by the administrator with previous written permission of one of the partners.

E-Mail: XYZ needs e-mail to communicate internally and with customers in an effective way. In many countries the digital certificates are considered a valid proof of identity with a legal value; for this reason every XYZ's employee will be provided with a digital certificate provided by VeriSign. This will provide protection against impersonation attacks and unauthorized reading of mail. The administrator will modify permissions on mailboxes only after partner's written permission. For example the partner's personal assistants will be granted the "read" and "send as" permissions on partner's mailboxes.

Computing Resources: I must protect my system from every attack that may provoke an unauthorized use of computing resources.

Main Threats

In an environment like XYZ my main concern are internal threats. The limited exposition to Internet limits greatly the probability of an external attack. This is a list of the threats that I consider more relevant. Risk has been calculated checking the probability of success and the loss generated by every attack.

DoS: A DoS is an attack on a network or computer, the primary aim of which is to disrupt access to a given service. It is relatively simple to exploit and may provoke significant losses. Networks like XYZ's are more exposed than others to this kind of threat because the single DC represents a SPOF (Single point of Failure). Important services like authentication, messaging, name resolution and others will not be available if this system is offline. A significant problem to prevent a DoS is that this condition may be generated involuntarily by a non-malicious user. It is impossible to avoid completely a DoS. Therefore, in order to secure my system, I will set limits and warnings to be prompted immediately when the environment is reaching this condition. Antivirus policies will be set to quarantine attachments bigger than 5 MB or compressed files with more than 10 nested levels. Exchange will be set to send mails in case of low disk space (1 GB), continuous SMTP queue growth (20 min.), processor usage (90% for more than 20 min.). The mail server used for the notifications will be the firewall SMTP daemon in order to grant the mail delivery even when the Exchange SMTP service is down. Some scripts will be created to start/stop services, start backup operations or virus definitions download.

Disgruntled Employees: Disgruntled employees may be more difficult to manage than other threats. In a place like XYZ, where many people work only for few months, we can find easily this kind of threat. The problem represented by them is that they are informed about the environment and they have already a limited access to internal resources. This situation makes easier for them to perform

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

privilege escalation attacks and covering their tracks. They may steal documents (customer informations), resources (unauthorized applications that may stress the network like games or file-sharing programs), or abuse of their mail capabilities (SPAM, mails with unauthorized content, etc…). Documents will be protected by a consistent set of ACLs and audits. User rights and Security options will protect me from stealing of resources. The Antivirus/Filtering for Exchange will prevent users to send/receive unauthorized content.

Malicious Code: The antivirus should solve malicious code problem but it represents a consistent threat. Viruses and Worms can spread easily among systems and may heavily damage them.

SERVER CONFIGURATION

Hardware

Important Note: This computer will be used to test Security Policies before applying them to a production environment. This hardware configuration does **not** provide any type of fault tolerance. To provide an easy redeployment of the server in case of unsuccessful policy application, I will use disk images created using Symantec Ghost Corporate Edition.

Motherboard:
ASUS P4S533-MX (Please refer to ASUS Web site for complete Specifications)

Processor:
Intel Pentium 4 2 GHz

Memory:
1 GB RAM

Video Adapter:
SIS 651

Audio Adapter:
ADI AD 1980 6-channel CODEC

LAN:
SIS 962L Integrated 10/100 Mbps Fast Ethernet

Hard Disk:
Maxtor 2F040J0 40 GB size

CD-ROM:
Samsung DVD-ROM SD-616Q

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Philips CDRW 2412A

Software

Important: System has been installed on March 2003. Patches and Programs installed are those available until that date.

Operating System:
Windows 2000 Advanced Server (Ver.5.00.2195) with Service Pack 3.

Groupware:
Exchange 2000 Enterprise Edition with Service Pack 3 (build 6249.4)

Internet Browser:
Internet Explorer Ver.6.0.2800.1106 128bit Cipher with Service Pack 1 and Q810847 and Q813951 patches.

Antivirus:
Symantec Antivirus Corporate Edition ver.8.01 build 425a (English) in unmanaged mode.

Antivirus (Mail Server):
Symantec Antivirus for MS Exchange 2000 ver.3.01.10 build 104 (English)

Other Products:
WinZip ver. 8.1 SR1 (5266)
Symantec Liveupdate ver. 1.80
Adobe Acrobat Reader ver. 5.1.0 date 09/17/2002
SiS Utility Tray Version ver. 2.07s
C-Media Audio Drivers
Windows Media Player ver. 9.00.00.2980

Patches Installed:

Q322842 A Lock Occurs Between Two Threads of System GDI in Windows 2000
Q322913 WM_TIMER Messages May Stop Being Delivered to Programs in Windows 2000
Q323172 MS02-048: Flaw in Certificate Enrollment Control May Cause Digital Certificates to Be Deleted
Q324096 MS02-053: Request to SmartHTML Interpreter May Monopolize Web Server CPU Resources
Q324380 MS02-051: Cryptographic Flaw in RDP Protocol Can Cause Information Disclosure
Q326830 MS02-045: Unchecked Buffer in Network Share Provider May Lead to Denial-of-Service

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Q326886 MS02-042: Flaw in Network Connection Manager Can Cause Rights Elevation
Q327696 MS02-062: October 2002 Cumulative Patch for Internet Information Services
Q329115 MS02-050: Certificate Validation Flaw Might Permit Identity Spoofing
Q329834 MS02-063: Unchecked Buffer in PPTP Implementation May Permit Denial-of-Service Attacks
Q328310 MS02-071: Flaw in Windows WM_TIMER Message Handling Can Enable Privilege Elevation
Q329170 MS02-070: Flaw in SMB Signing May Permit Group Policy to Be Modified
Q810833 MS03-001: Unchecked Buffer in the Locator Service Might Permit Code to Run
Q815021 MS03-007: Unchecked Buffer in Windows Component May Cause Web Server Compromise

Considerations on applications installed

WinZip: WinZip does not have major security issues.

Internet Explorer: In this environment IE will be used only to administer SAV for Exchange or Outlook Web Access for testing purposes. It will not be used to access external sites.

Acrobat Reader: Acrobat Reader has been installed to open PDF files. The source of these files will be always trusted.

Windows Media Player: WMP is an application used to view/play many different file types (i.e. WMF, WAV, MPG, AVI, MIDI, MP3, etc…). It is a component integrated in the operating system. It will not be used.

Symantec Liveupdate 1.80: Liveupdate is a program shipped with every Symantec product to manage the automatic download and installation of updates. It will be scheduled to run every hour to check for new virus definitions and updates. A script will be added to the Exchange Monitoring system to start it immediately in case of suspect server activity to improve the probability to stop a mass mailer virus infection since its beginning.

Sis Utility and C-Media: These are the drivers respectively for video and audio chipsets (integrated in the motherboard).

Symantec Antivirus: This product will be used to avoid infection from different types of malicious code (virus, Trojan horses, worms, etc.). This product protects only the local machine's file system and the e-mails received using Outlook in MAPI mode or Lotus. The mail client add-on will not be installed on the server, as

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

there is no need. In order to ensure the correct functionality of Exchange, the following files/folders will be added to the exclusion list:

- M: (Exchange Installable File System)
- Exchange databases (Default location: Exchsrvr\Mdbdata)
- Exchange MTA Files (Default location: Exchsrvr\Mtadata)
- Exchange Temporary files (tmp.edb)
- Additional Log Files (Default location: Exchsrvr\server_name.log)
- Virtual Server folder (Default location: Exchsrvr\Mailroot)
- Site Replication Service (SRS) Files (Default location: Exchsrvr\Srsdata)
- IIS system files (c:\winnt\system32\inetsrv)

In order to ensure the correct functionality of SAV for Exchange, the following folder will be added to the exclusion list:

- C:\Program Files\Symantec\temp

Symantec Antivirus/Filtering for MS Exchange 2000: This product has been designed to protect Exchange from all mail-based threats (malware in the attachments, malformed MIME headers, scripts embedded in HTML mails) and to provide content management features. It uses the Windows embedded VSAPI 2.0 to better integrate with Exchange. It performs the following modifications to the system:

- It adds a SAVFMSE Admins group (global security group). This group will contain the accounts, which will have administrative access to the product.
- It adds a SAVFMSE Viewers group (global security group). This group will contain the accounts, which will have the rights to view the product settings.
- Security is established on the "HKEY_LOCAL_MACHINE \ Software \ Symantec \ SAVFMSE \ 3.0" registry key granting access to the two security groups.
- Adds a new Web Site on IIS to host the user interface. This site is configured to the "Medium (pooled)" application protection and "Integrated Windows Authentication". This web site will be contacted by using port 8081. In order to tighten security I will modify "IP Address and Domain Restriction" to block access to every IP address except localhost.

Consideration on future applications/modifications

A separate system will be used to test any modification to the production environment (drivers, applications, patches, AD modifications).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Server Installation

The server has been installed on a separate network to avoid any risk of infection/compromising. The patches have been downloaded and installed from a CD.

Installation Procedure

1. Low-level format (I generated 3 partitions: C: 15GB NTFS, D: 14 GB NTFS, E: 10 GB FAT32).
2. Scanned MBR to be sure that no MBR viruses are present.
3. Installed Windows 2000 Server:
    a. System Partition = C:
    b. Path = C:\Winnt
    c. Components Added to the standard installation:
        i. SMTP
        ii. NNTP
        iii. DNS
4. Applied Service Pack 3.
5. Started DCPromo:
    a. Domain Name: xyz.com
    b. NetBIOS Name: xyz
    c. DNS to be used: Local Machine.
6. Reboot.
7. Applied Service Pack 3.
8. Operating System Patches and Program Upgrades Installed (See software configuration for the complete list).
9. Installed and updated manually Antivirus Client.
10. Reboot.
11. Run *forestprep* command to prepare the schema naming context for Exchange using the administrator account.
12. Run *domainprep* command to prepare the domain naming context for Exchange using the administrator account. In this way exchserv will be the administrator of the Exchange Organization.
13. Run Exchange Setup to install the product. This part of the Exchange installation modifies the Configuration Naming Context.
14. Reboot.
15. Applied Exchange Service Pack 3.
16. Reboot.
17. Configured Exchange exclusions of SAV Corporate Edition.
18. Install SAV for Exchange.
19. Reboot.
20. Configured SAV for Exchange exclusions of SAV Corporate Edition.
21. Checked the event viewer to look for errors or warnings.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In the Event Viewer I found the following errors and warnings:

System Log:

1. Event ID 101

   Source: W3SVC

   Description: The server was unable to add the virtual root '/Exadmin' for the directory'\\.\BackOfficeStorage' due to the following error: the system cannot find the path specified. The data is the error code.

   This Warning can be ignored as in the KB article Q259373.

2. Event ID 5782

   Source: Net logon

   Description: Dynamic registration or deregistration of one or more DNS records failed with the following error: No DNS servers configured with local system.

   This Warning can be ignored because it is due to the fact that the server's IP configuration is pointing to a server that don't support dynamic updates (in this case the ISP External DNS Server).

Application Log:

1. Event ID 1000

   Source: Userenv

   Description: Windows cannot unload your registry file. If you have a roaming profile, your settings are not replicated.

   This warning has been solved using the KB article Q319006.

2. Event ID 2102, 2104, 8250. These events will be ignored because they are generated by the application of Exchange service pack. (KB article Q322837)

CHOOSING THE TEMPLATE

Template Chosen

I have decided to use the standard NSA templates for DCs (w2kdc.inf). This template has been developed by the NSA to enforce security on DCs. It

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

represents a good start to configure security in my environment because it provides generic hardening for DCs giving me more time to define details. I decided to modify it for the following reasons:

- The XYZ DC provides a lot of services that in standard conditions wouldn't be in a DC (like Exchange) while the template is thought for DCs only.
- This template has been created to configure DC security for US government's contractors. Sometimes it is too strict for my environment.
- Some sections like "Group Membership" or "System Services" are not covered. It is difficult to define standard sets of configurations for these sections because there are too many variables involved that not always are related directly with the system (Company Policies or Organizational Charts).

I will modify the followings:

- Account Policy must be modified to adapt them to the XYZ environment. I will loosen my Account Policies to help XYZ untrained users to maintain an acceptable level of security without making things too difficult for them.
- I will define a strict Group Membership because I will need to limit "privilege escalation" attacks. This kind of attacks may provoke great losses in terms of access to informations or use of computing resources.
- User Rights Assignments will be modified to adapt the template for a system with Exchange 2000 installed.
- I will not modify Auditing Policies because they already respond to my needs. The logs generated will be useful as proofs in a court or for a successful incident handling.
- Security Options will be slightly modified to change "administrator" and "guest" account names and to display a message for legal reasons.
- Event Log policies will be modified because they may generate unwanted DoS conditions (by filling up the disk or shutting down the system when the log is full). This could help an attacker that wants to cover his tracks.
- I will modify permission on system services and startup option in order to grant that the most important services will not be modified incorrectly. An incorrect configuration may provoke problems.
- File System policies will not be changed because I consider them already appropriate for my system.
- Registry policies will remain unchanged with the exception of one setting to guarantee Exchange operations.

Tools Used to apply the template

I will use the Security Configuration and Analysis tool (SCA) supplied by Microsoft to have a complete overview of the settings modified by the NSA template and by my subsequent variations. This is the graphical version of the "secedit" command line utility.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

With the SCA I will be able to perform the following tasks:

1. Analyze the Security Policies applied to the system.
2. Apply to the system a previously prepared template.
3. Force the immediate reapplication of security policies.
4. Export the system's configuration to a template that could be applied to similar ones.
5. Validate the syntax of a template.

This tool creates a database that can be compared with the security policies applied to the system. In this way I will be able to simulate my settings' effect before their effective application. I will import the NSA template in the database. Then I will modify it to answer specifically to my needs.

Considerations about Security Policies Application on DCs

Security Policies are applied to DCs in a way similar to group policies with some significant differences. DCs share the same account database therefore some of their settings are stored in the Domain Security Policy.
These settings are:

1. The "Account Policies" section.
2. Three settings of the "Security Options" section:
    a. Automatically Log off users when logon time expires.
    b. Rename Administrator Account.
    c. Rename Guest Account.

(Please check the following TechNet Article for further informations: Q259576: Group Policy Application Rules for Domain Controllers)

How the template will be enforced on DCs

The template must be applied continuously in order to be effective. Security Policies are a subset of Active Directory Group Policies. I will have to change some settings in "Group Policies" to be sure that my policies will be reapplied periodically.
Here is the procedure to force continuous policy application:

1. Open "Active Directory Users and Computers" Snap-in.
2. Right Click on the domain name.
3. Click on "Properties".
4. Click on the "Group Policy" tab.
5. Highlight "Default Domain Policy" and click on the "Edit" button.
6. Double Click on "Computer Configuration".
7. Double Click on "Administrative Templates".
8. Double Click on "System".

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

9. Click on “Group Policy”.
10. Enable “Group Policy Refresh interval for computers” and set it to 15 min with random interval of 30 min.
11. Enable “Group Policy Refresh interval for Domain Controllers” and set it to 5 min.
12. Enable “Security Policy Processing” and check “Process even if the Group Policy objects have not changed”.
13. Open a DOS window and execute the following command: “secedit /refreshpolicy machine_policy /enforce”. This will apply the modifications immediately.

The settings in the procedure are not the defaults. In a small environment like XYZ’s, where there is a single DC, group policies can be applied with low intervals. My modifications will guarantee the enforcement of group policies every 5 minutes on DCs and every 15 minutes on domain computers. The “security policy processing” setting will guarantee the application of security policies even in case of no changes.
Intervals and forced security policy application may generate issues in replication and resources consume (higher bandwidth usage and higher processor usage). In my environment this is not an issue.

TEMPLATE SETTINGS

Account Policies

Account Policies are used to enforce rules such as: password history, account lockout, Kerberos ticket lifetime and others. Account Policies have been defined in the “Domain Security Policy” for the reasons explained in the previous section. It is important to understand that applying the policies at domain level will enforce them on all the members of the XYZ domain. Account Policies are composed by the following subsets: Password policy, Account Lockout policy and Kerberos policy.

Password Policy

Password policies are used to decrease the attacker’s chance to guess a password using dictionary or brute-force attacks (password length and complexity). If the password is found they will limit the usability of the valid password (password age and history). The NSA policy is too strict for untrained users like XYZ; therefore I have decided to reduce the security level to improve user-friendliness.

Policy	NSA Template Value	Modified Template
Enforce Password History	24 Passwords	15 Passwords
Maximum Password Age	90 Days	42 Days
Minimum Password Age	1 Day	1 Day
Minimum Password Length	12 Chars	8 Characters

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Passwords must meet complexity requirements	Enabled	Enabled
Store passwords using reversible encryption for all users in the domain	Disabled	Disabled

The policy "Enforce Password History" ensures that users will not re-use the last 15 passwords. The possibility that an attacker has a valid password is high, however the users will eventually experience less issues in remembering their password set. As well untrained users will find this process approachable. In order to limit the increased attacker's chance to get a valid password I decided to reduce the "maximum password age" to 42 days. This setting will force users to change their password constantly without generating difficulties in remembering the password itself. This will probably avoid that users will choose password related to month and seasons. If an attacker gets a valid password, it will be valid, as a maximum, 42 days. The "minimum password age" policy avoids that users change their password more than 15 times in the same day to circumvent the password history policy. On one hand the minimum password length of 8 characters will increase the possibility of brute-force cracking with programs such as L0phtCrack, on the other hand it will improve the password manageability for end-users. The complexity requirement policy will force users to choose for their passwords at least three of the following characters:

1. Upper case letters.
2. Lower case letters.
3. Numbers.
4. Non-alphanumeric characters (such as £, $, %, etc…).

This will reduce the possibility of success of dictionary-based attacks and will enlarge the set of characters to be checked in brute-force attacks by making them time wise longer to be exploited.

Account Lockout Policy

Account Lockout policy is used to block password guessing attacks which are exploited on-line (if an attacker will check the user account database offline this policy will be ineffective because it is not applicable). Account Lockout policies may be unnecessary if the password policies are well configured. In large environments, they may be a source of issues (it generates too many calls to the internal helpdesk). However I've decided to implement them to discourage simple password guessing attacks.

Policy	NSA Template Value	Modified Template
Account Lockout Duration	15 Min.	30 Min.
Account Lockout Threshold	3 Attempts	3 Attempts
Reset Account Lockout Counter	15 Min.	15 Min.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

After		

If a user will provide the system with 3 incorrect passwords in a range of 15 minutes his account will be blocked for 30 minutes (The user can not logon even if the correct password is provided). These settings, combined with password policies, will make almost impossible a password guessing attack directed against an account.

Important: The built-in administrator account cannot be locked out only for network logons. Interactive logons will always be possible. If the administrator account is locked, it will only be released by using the passprop.exe tool provided with the Windows 2000 Server Resource Kit.

Kerberos Policy

The standard authentication protocol for Windows 2000 is Kerberos V.5. Kerberos authentication is based on tickets. These policies enforce the ticket management settings. I took the decision of not changing them.

Policy	NSA Template Value	Modified Template
Enforce User Logon Restriction	Enable	Enable
Max. Lifetime for Service Ticket	600 Min.	600 Min.
Max. Lifetime for User Ticket	10 hours	10 hours
Max. Lifetime for User Ticket Renewal	7 days	7 days
Max. Tolerance for Computer Clock Synchronization	5 min.	5 min.

Local Policies

Local Policies permit to define auditing, to provide rights to users/groups based on their role, to manage settings, which were usually enabled by modifying registry keys. Part of these policies is defined both in the Domain and Domain Controller security policies too, therefore to avoid conflicts I will configure them at Domain Controller security level. By setting them at this level they will be automatically applied to every domain controller in the XYZ domain. Local policies are, by definition, related only to the system to which they are applied. But, if the computer is a DC, they influence the domain. For example: “Auditing Account Logon Events”, if applied to a DC, logs an entry for every user logon in the domain even if it is not an interactive or network logon made directly against the Domain Controller. Local Policies are divided into: Audit Policy, User Rights Assignment and Security Options.

Audit Policy

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Policy	NSA Template Value	Modified Template
Audit Account Logon Events	Success/Failure	Success/Failure
Audit Account Management	Success/Failure	Success/Failure
Audit Directory Service Access	Failure	Failure
Audit Logon Events	Success/Failure	Success/Failure
Audit Object Access	Failure	Failure
Audit Policy Change	Success/Failure	Success/Failure
Audit Privilege Use	Failure	Failure
Audit Process Tracking	No Auditing	No Auditing
Audit System Events	Success/Failure	Success/Failure

Audit Account Logon Events and Audit Logon Events: These policies enable the logging of logon events (both interactive and network). The difference between these policies is slight. Account Logon Events are logged "where the account lives" (The DC) while Logon Events are logged "where the logon occurs". An interactive logon to a workstation of the domain generates 1 "Account Logon Event" on the DC. An interactive logon to the DC generates 1 "Account Logon Event" and 1 "Logon Event". This behavior, in some situations, may generate duplicate entries. I've decided to leave both the settings to success/failure to have the best possible overview of the accesses to my system. An example of Logon Event is event id 540 (Successful Network Logon).
It is interesting to notice the differences in logging successful Logon/Logoff events between Windows NT 4.0 and 2000. NT 4.0 identifies every "successful logon" event with event id 528 while Windows 2000 differentiates them. Event 528 identifies a Successful Interactive Logon, while Event 540 identifies a Successful Network Logon.
Windows 2000 logs a lot of irrelevant 540 events and we have to distinguish between them and relevant ones. This goal may be achieved easily by looking at the event's "User Name" field.
There are three possibilities:

- System: These events can be ignored because they indicate that a system service is connecting to another service on the same system.
- Machinename$: These events can be ignored because they indicate that a remote system service is connected to a system service on the local machine.
- User: These events are important because they tell us that the user logged on the remote machine indicated in the event.

Unsuccessful Logon Events have not changed much between the two operating systems.
Another interesting thing that should be noticed is the logon type in the event description. Different logon types are associated to different numbers.
For example:

- Interactive Logon is type 2.
- Network Logon is type 3.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Batch Logon is type 4.
- Service Logon is type 5.
- Unlocked Workstation is type 7.
- Network logon with a clear-text password is type 8.
- Impersonated Logon is type 9.

Audit Account Management: This setting will log every action that involves account management. I have enabled this policy because the administrator wants to be aware of every action related to the accounts. Every modification to group membership will be documented with a standard module signed by 1 partner. Comparing the modules and the events the administrator will be able to find unauthorized actions and will be able to prosecute them. An example of Account Management event is event id 624 (User Account Created).

Audit Directory Service Access: This option will permit to the administrator to monitor access to Directory Service objects. An example of directory service access is event id 565 (Object Open).

Audit Object Access: This option determines whether to audit the event of a user accessing an object (for example, file, folder, registry key, printer, and so forth) which has its own system access control list (SACL) specified. An example of Object Access is event id 560 (Object Open)

Audit Policy Change: Especially in situations where security is enforced with policies, the administrator wants to know whether policies have been successfully applied or not. Therefore I configured it to audit both successes and failures of these events. An example of Policy Change event is event id 1704 (Security Policy in the Group Policy Objects is applied successfully).

Audit Privilege Use: Audit Privilege Use generates events every time a user exercises a specific user right (for example bypass traverse checking, backup/restore file or folders, debugging programs). An example is event id 576 (Special Privilege Assigned). This option is set to “Failure only” because, in this way, there is the possibility to find unauthorized actions (failures) without filling the log with not relevant events (successes).

Audit Process Tracking: This is set to “No Audit” because it may generate a considerable amount of events. This should be enabled during an incident response. Every process opened by every user will be logged (Category Detailed Tracking). An example of Process Tracking event is event id 592 (New Process Created)

Audit System Events: to “Success/Failure”. This policy has been set to log events like startups (Event ID: 512), service logon processes loaded (Event ID: 515) (i.e. Winlogon\MSGina) and Authentication Packages loaded (Event ID:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

514) (i.e. kerberos.dll for Kerberos authentication). The administrator wants to monitor both successes and failures for this set of events.

User Rights Assignments

The "User Rights Assignments" section of the Security Policies is used to give to a specific user/group the rights to perform a specific action (interactive log on, logon as a service and others). I modified this section at the Domain Controller Security Policy because, if applied locally, it will not be enforced correctly due to the Domain Controller Security Policy inheritance.

Policy	NSA Template Value	Modified Template
Access this computer from the network	Enterprise Domain Controllers, Authenticated Users, Administrators	Enterprise Domain Controllers, Authenticated Users, Administrators
Act as a part of the operating system		
Add workstations to domain		
Backup files and directories	Administrators	Administrators
Bypass traverse checking	Authenticated users	Authenticated users
Change the system time	Administrators	Administrators
Create a pagefile	Administrators	Administrators
Create a token object		
Create a permanent shared object		
Debug programs		
Deny access to this computer from the network		
Deny logon as a batch job		
Deny logon as a service		
Deny logon locally		
Enable computer and user accounts to be trusted for delegation	Administrators	Administrators
Force shutdown from a remote system	Administrators	Administrators
Generate security audits		
Increase quotas	Administrators	Administrators
Increase scheduling priority	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators
Lock pages in memory		
Log on as a batch job		
Log on as a service		
Log on locally	Administrators	Administrators

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Manage auditing and security log	Administrators	Administrators, Exchange Enterprise Servers
Modify firmware environment values	Administrators	Administrators
Profile single process	Administrators	Administrators
Profile system performance	Administrators	Administrators
Remove computer from docking station		
Replace a process level token		
Restore files and directories	Administrators	Administrators
Shut down the system	Administrators	Administrators
Synchronize directory service data		
Take ownership of files or other objects	Administrators	Administrators

I maintained most of the NSA settings without modifications because they satisfy my security needs. Most of the operations defined in this section are sensitive and I think that limiting the permission to the administrators group is the right choice. I don't need to delegate operations because there will be only one persons that will perform them (the system administrator).
I modified only **Manage auditing and security logs** to "Administrators, Exchange Enterprise Servers"
"Exchange Enterprise Servers" group has been added to this setting in order to grant the correct functionality of Exchange as advised by the NSA in the "Exchange_Instruction.htm" document. This document explains how to modify the DC template to let Exchange work correctly.

Security Options

The "Security Options" subset permits to modify some system settings that are defined by registry keys. The NSA security options were already appropriate for my needs so I have added only modification to values, which were set to "not defined" in the template.

Policy	NSA Template Value	Modified Template
Add. Restr. For Anonymous Connections	No Access without explicit anonymous permission	No Access without explicit anonymous permission
Allow Server Operators to schedule tasks (DC only)	Disabled	Disabled
Allow System to be shut down without log on	Disabled	Disabled
Allowed to eject removable NTFS Media	Administrators	Administrators
Amount of idle time required before disconnecting session	30 Min.	30 Min.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit the access of global system objects	Enabled	Enabled
Audit use of Backup and Restore privilege	Enabled	Enabled
Automatically log off user when logon time expires	Enabled	Disabled
Automatically log off user when logon time expires (Local)	Enabled	Enabled
Clear Virtual Memory file when shut down	Enabled	Enabled
Digitally Sign Client Communication (always)	Disabled	Disabled
Digitally Sign Client Communication (when possible)	Enabled	Enabled
Digitally Sign Server Communication (always)	Disabled	Disabled
Digitally Sign Server Communication (when possible)	Enabled	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled	Disabled
Don't display last user name in logon screen	Enabled	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only / refuse LM & NTLM	Send NTLMv2 response only / refuse LM & NTLM
Message text for users attempting to log on	Not Defined	See Below
Message title for users attempting to log on	Not Defined	See Below
Number of previous logons to cache (not available for DC)	0 logons	0 logons
Prevent system maintenance of computer account password	Disabled	Disabled
Prevent Users from installing printer drivers	Enabled	Enabled
Prompt user to change password before expiration	14 days	14 days
Recovery Console: Allow automatic administrative logon	Disabled	Disabled
Recovery Console: Allow floppy copy and access to all drive and folders	Disabled	Disabled
Rename Administrator Account	Not Defined	Commander
Rename Guest Account	Not Defined	Recruit
Restrict CD-Rom access to locally logged-on users only	Enabled	Enabled
Restrict Floppy access to locally	Enabled	Enabled

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

logged-on users only		
Secure Channel: Digitally Encrypt or Sign secure channel data (always)	Disabled	Disabled
Secure Channel: Digitally Encrypt secure channel data (when possible)	Enabled	Enabled
Secure Channel: Digitally Sign secure channel data (when possible)	Enabled	Enabled
Secure Channel: Require strong (Windows 2000 or later) session key	Disabled	Disabled
Send unencrypted password to connect to 3rd party SMB servers	Disabled	Disabled
Shut down system immediately if unable to log security audits	Enabled	Disabled
Smart Card Removal Behavior	Lock Workstation	Lock Workstation
Strengthen default permission of global system objects	Enabled	Enabled
Unsigned driver installation behavior	Warn but allow installation	Warn but allow installation
Unsigned non-driver installation behavior	Warn but allow installation	Warn but allow installation

I have added a message for users attempting to log on for legal reasons. In many countries it is mandatory to add a legal disclaimer in order to prosecute a person. If, when accessing a system, it is not displayed a logon advisory or worse it is displayed a welcome screen, this may not permit a legal prosecution of the attacker. (CIAC Information Bulletin A-22)

Title: XYZ & Associates Log on Advisory

Message: This is a private computer system protected by a security system. Access to and use of this facility requires explicit, written, current authorization and is strictly limited to purpose of XYZ & Associates business. Unauthorized or attempt at unauthorized access, use, copying, alteration, destruction, or damage to its data, programs or equipment may violate the applicable law and may result in criminal prosecution or civil liability, or both.

Rename Administrator Account: Commander

Rename Guest Account: Recruit

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

I renamed the administrator and guest accounts in order to avoid attacks made directly against them. If an attacker will check SIDs this settings will not be useful as the administrator's SID is fixed (it always finish with the 500 value).

I have set to "Disabled" the "Shut down system immediately if unable to log security audits" in order to avoid unwanted system shutdowns.

Event Log

Event logs are an excellent source of information both for administrators and hackers. They are important evidences when prosecuting an attacker therefore they must be checked and stored periodically by the administrator. The "Event Log" section of the security templates defines all the aspects of the three main logs: Application, Security and System. It is possible to find additional logs depending on the system function (for example: DNS log, File Replication log and others).

Settings for Event Log

Policy	NSA Template Value	Modified Template
Max. Application log size	4194240 KB	670000 KB
Max. Security log size	4194240 KB	670000 KB
Max. System log size	4194240 KB	670000 KB
Restrict guest access to the application log	Enabled	Enabled
Restrict guest access to the security log	Enabled	Enabled
Restrict guest access to the system log	Enabled	Enabled
Retain Application, Security and System logs	Not Defined	60 days
Retention Method for application log	Manually	By days
Retention Method for security log	Manually	By days
Retention Method for system log	Manually	By days
Shut down computer when the security log is full	Enabled	Disabled

In my case the NSA policy is not applicable. I changed the maximum size of logs to 670 MB instead of 4 GB (maximum size possible) to permit to the administrator to save them on CDs. Logs will be checked at least once per week by the administrator who will subsequently archive them on a magnetic support. I disabled the "Shut down computer if the security log is full" setting because I have only this DC and I cannot risk stopping it. Events in the logs will be deleted only if older than 60 days.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Restricted Groups

"Restricted Groups" is not part of the local security policies therefore I will set memberships at "Domain Controller Security Policy" level.
"Restricted Groups" policy is used to control group membership. Since the XYZ partners will have the account operators' rights, I have decided to use this policy in order to avoid unauthorized membership changes to the most important groups. Although partners know which are the operations that they are allowed to do I want to be sure to avoid errors in group management for this sensitive groups.
The administrator will use different account to accomplish different tasks:

- "Administrator" is a fake account used daily by the system administrator. It is member of the "domain users" group.
- "Corporal" has been created as "Exchange Full Administrator". It is disabled and member of the "Administrators" group.
- "Colonel" is the account that will be used to modify schema. It is disabled and member of the "Schema Admins" group.

I have decided to enforce the following group memberships:

Group	Members	Member Of
Administrators	Administrator, Corporal, Enterprise Admins, Domain Admins.	
SAVFMSE Admins	Administrator.	
Schema Admins	Colonel	
Domain Admins	Administrator.	Administrators.
Enterprise Admins	No users	No Groups
Account Operators	Partners.	
Partners	Partner1, Partner2, Partner3, Partner4, Partner5.	Account Operators.

Administrators, Domain Admins: These groups have the possibility to manage everything in the domain. I have not changed the standard memberships of these groups. My decision to insert them in the policy is due to the fact that I want to be sure that their group memberships will be maintained. The user "Corporal" has been added for Exchange administration purposes.

Enterprise Admins: Since there is a single domain I will configure the enterprise admin group to be empty and not member of any group.

Schema Admins: The Schema Admins group has the ability to manage the schema partition of AD. They can add/disable attributes or classes in it. Many

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

applications such as Exchange 2000 need to extend the schema in order to work correctly. If performed inappropriately they may have disastrous consequences on AD. I created a user called “Colonel” that will be the unique member of the schema admins group and that will be enabled only when a schema modification will be needed. Schema modifications will be tested in a separate environment kept updated by the administrator.

SAVFMSE Admins: This group’s members have the right to manage the SAV for Exchange settings including enabling/disabling it. The administrator will be the only member of this group.

Account Operators and Partners: The Account Operators group has the right to manage accounts inside the domain. Usually it is empty but the XYZ partners want to be able to manage users therefore I created a Global security group called “Partners” where I inserted the partners accounts and I have added it to the Account Operators.

System Services

The “system services” policy is used to manage the services startup mode and access control lists. The NSA template does not define them. I changed the ACLs to provide only to the “Administrator” and “System” accounts the rights to manage services. There are 3 different startup options:

1. Automatic: The service starts during the startup phase of the system and runs even if no user is logged to the machine.
2. Manual: User may start the service after a successful logon then it continues to run even if the user logs off.
3. Disabled: the service cannot be started during startup or manually by a user. To start it you must change his status to “Manual” or “Automatic”.

These are the services’ startup options that I have forced:

Service	Startup
Automatic Updates	Disabled
DefWatch	Automatic
Clipbook	Disabled
Symantec Antivirus Client	Automatic
Symantec Antivirus/Filtering for MS Exchange 2000	Automatic
DHCP Client	Disabled
Microsoft Exchange IMAP4	Disabled
Microsoft Exchange POP3	Disabled
Telnet	Disabled
Network News Transport Protocol (NNTP)	Disabled

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Distributed File System	Automatic
File Replication	Automatic
Intersite Messaging	Automatic
Kerberos Key Distribution Center	Automatic
Remote Procedure Call (RPC) Locator	Automatic
DNS Server	Automatic
IIS Admin Service	Automatic
NT LM Security Support Provider	Automatic
Microsoft Exchange Information Store	Automatic
Microsoft Exchange Management	Automatic
Microsoft Exchange MTA Stacks	Automatic
Microsoft Exchange Routing Engine	Automatic
Microsoft Exchange System Attendant	Automatic
Simple Mail Transfer Protocol (SMTP)	Automatic
Event Log	Automatic
Net Logon	Automatic
NetMeeting Remote Desktop Sharing	Disabled
Indexing Service	Manual

All services not listed above have been set to "not defined"

Automatic Updates: "Disabled"
This service is installed by default in Service Pack 3. I set it to "disabled" because all updates will be performed manually.

Clipbook: "Disabled"
Clipbook is the service that is used for copy/cut/paste operations. If used incorrectly (for example for copying passwords) it may retain sensitive information. It is less protected than other part of the system therefore an attacker may use it as a source of information during the system inspection part of an attack.

DefWatch, Symantec Antivirus Client and Symantec Antivirus Filtering for MS Exchange 2000: "Automatic".
These are the antivirus services. I want to be sure that these services will not be disabled. If they are disabled it may result in a loss of protection against viruses and other types of malicious code.

DHCP Client: "Disabled"
All Domain Controllers, in order to work correctly, must have a fixed IP address. The DHCP client service checks the network to find DHCP servers that can assign a dynamic IP address. This service is not needed on a machine with static IP address.

Microsoft Exchange IMAP4 and POP3: "Disabled"

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

POP3 and IMAP4 are protocols used to retrieve mails from a mail server. All the XYZ client will use the RPC to connect to the Exchange Server therefore these protocols are not needed.

Telnet: "Disabled"

Telnet service permits to a user to connect remotely to the server and run commands. The administrator will always logon interactively to the machine in order to manage it therefore it is not needed. By default it set to manual but I want be sure that none would be able to start it.

Network News Transport Protocol (NNTP): "Disabled"

The NNTP protocol has been disabled because XYZ will not use internal newsgroups.

Distributed File System, File Replication, Intersite Messaging, Kerberos Key Distribution Center, Remote Procedure Call (RPC) Locator: "Automatic"

These services are needed by DCs in order to work correctly.

IIS Admin Service, Microsoft Exchange Information Store, Microsoft Exchange Management, Microsoft Exchange MTA Stacks, Microsoft Exchange Routing Engine, Microsoft Exchange System Attendant: "Automatic"

These services are needed to guarantee Exchange 2000 operation.

Simple Mail Transfer Protocol (SMTP): "Automatic"

XYZ mail system needs this service in order to send external mails to the firewall SMTP Daemon. I want to highlight that the SMTP service does not influence Exchange 2000 correct operation.

DNS Server: "Automatic"

DNS Server is needed to provide the correct functionality of Active Directory. In the XYZ environment all clients will use this system's DNS to locate AD resources.

NT LM Security Support Provider: "Automatic"

This enables the users to authenticate using NTLM. If this service is stopped users may not be able to access resources.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Event Log: "Automatic"

Event Log service must be started otherwise no events would be logged.

Net Logon: "Automatic"

Net Logon is needed to support pass-through authentication and to handle the registration of SRV records in the DNS.

NetMeeting Remote Desktop Sharing: "Disabled"

This service is a possible backdoor for attackers and it is not needed for any task therefore I decided to disable it.

Indexing Service: "Manual"

Indexing Service is the target of many exploits and it is not needed. I set it to manual because it may be useful to start it temporarily. Indexing will keep performances high if performed regularly.

Registry Settings

The "registry settings" section of the security templates is used to define ACLs on registry keys. This operation can be performed manually by using the regedt32.exe utility.

NSA template modifies permissions on the following hives:

- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS

These modifications are too many to repeat and most of them are environment specific. In my opinion the NSA settings were appropriate for my needs therefore I've decided to not change them with the exception of one value:

HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg

This key defines the users/groups that can access the system using Remote Registry Service. In the NSA template the "backup operators" group receives "Read" permission on this key (it is needed in case of System State Backup). In my environment only the administrator will backup the system therefore I've removed the "backup operators" group from the ACL. At the same time I granted to the "Exchange Domain Servers" Group "Full Control" permissions to grant Exchange operation. This is advised by the NSA's document "Exchange_Instruction.htm" document.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Registry modifications must be applied only after a successful period of testing. My advice is to backup the registry hive where they are performed using the registry editor utility before their application.

File System Settings

The "File System" section controls the ACLs maintain a consistent set of ACLs for the file system. The file system settings are environment specific and it is not possible to generate a template completely reliable. NSA provides a template that sets permissions for files/folders, which will be always present in a standard Windows 2000 installation (English version). Therefore we will find permissions set for the startup files (boot.ini, autoexec.bat, config.sys, io.sys, msdos.sys, ntdetect.com, ntldr) or the "Document and Settings" folder where are located the user profiles but we will not found any permission on files/folders which may be equally sensitive like the folders created by the patches for uninstall operations.

NSA Permissions will be applied at different file system levels defined by the system variables:

- %Program Files%
- %System Directory%
- %System Drive%
- %System Root%

In most of the cases the template will restrict permissions to administrators, System and Creator Owner. This will limit the possibility to access to sensitive information (The boot.ini file or the "repair" folder) and to install unauthorized applications or drivers (Driver installation is also managed in the "security options" section).

APPLYING AND TESTING THE TEMPLATE

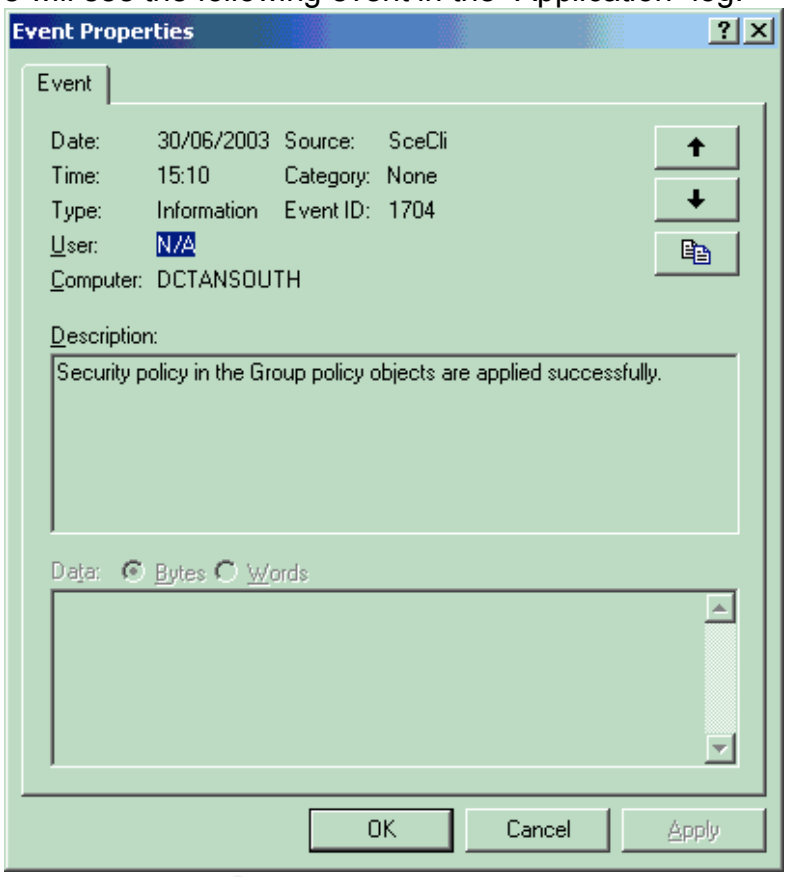
Monitoring Template Application

Security Policies are a subset of AD Group Policies therefore, to monitor if they are applied successfully, I must check if Group Policies are applied correctly. Microsoft has given us different tools to monitor Group Policies application:

1. Event Viewer
2. Secedit.
3. Security Configuration and Analysis Tool
4. GPResult.exe
5. GPOTool.exe

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

EVENT VIEWER: In my configuration I have set the “Audit Policy Change” to “Success/Failure”. This permits me to know if a policy has been applied successfully or not. In the specific case of a successful security policies application we will see the following event in the “Application” log:



SECEDIT.EXE and SECURITY CONFIGURATION and ANALYSIS TOOL: The Secedit.exe command-line tool and its graphic correspondent the security configuration and analysis tool can be used to perform different tasks (Please refer to the “Tool used to apply the template” section for their characteristics). In case of monitoring I can use their analyzing capability to compare my template with the parameters actually set on the system.

GPRESULT.EXE: GPRESULT is a utility used to display useful information about group policies application like:

- Last Group Polices application time.
- Which Group Policies were applied to the system.
- The DC that is the source of the policies.

GPOTOOL.EXE: This resource kit command-line tool is used to monitor the consistency of policy replication between DCs. It also checks the correspondence between policies stored in AD and those applied to the system.

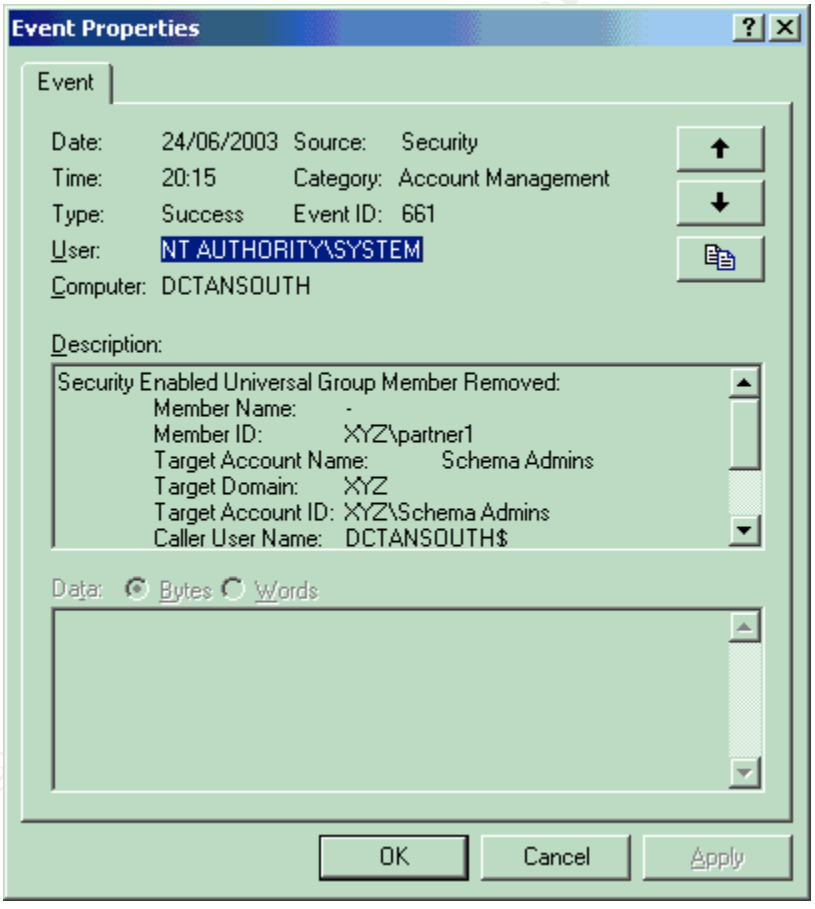
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Testing Template Security Settings

Test 1 (Restricted Groups)

In order to test the "Restricted Groups" section of my policies I added to the "Schema Admins" group the user "Partner1". My policy defines that the "Schema Admins" group will have only the user "Colonel" as member. If my policy has been applied successfully "Partner1" will be removed from the group automatically and an event will be logged in the security log.

During the automatic policy application the following event has been logged:



As you can see in the description "Partner1" has been removed from the group. This demonstrates that the group membership policy has been applied successfully.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

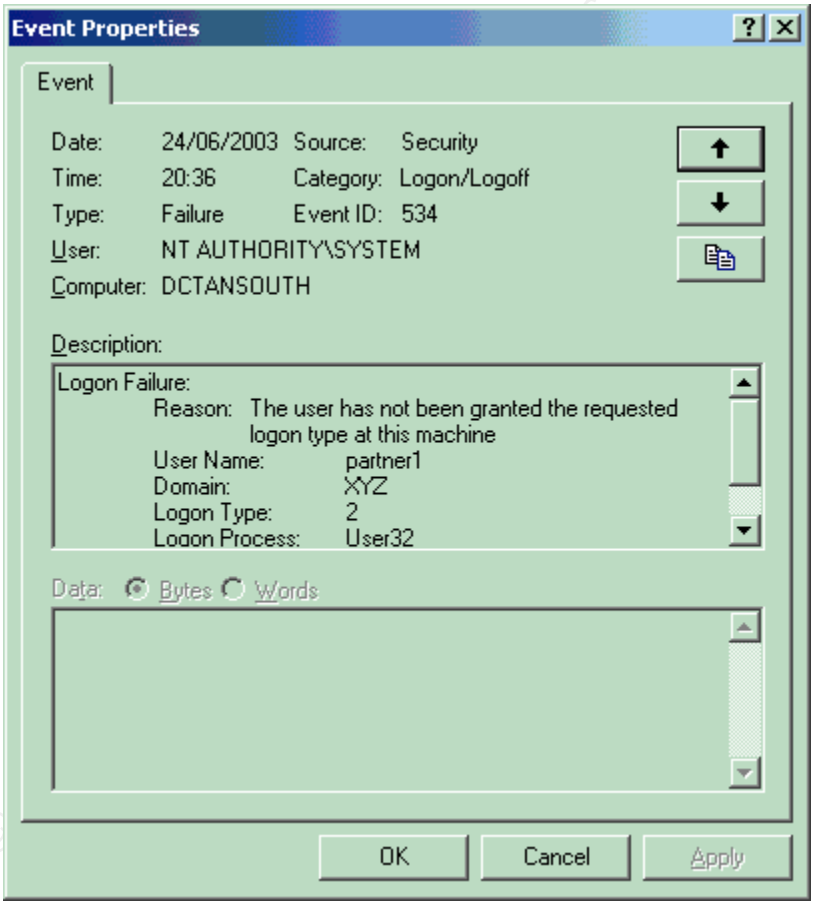
Test 2 (Logon Locally Rights)

I tried to logon interactively to the DC with the user "Partner1" in order to test "Logon Locally" right. In my policy the "Logon Locally" right has been granted only to the members of the "Administrators" group. If my policy has been applied successfully "Partner1" will be notified by the system that it is not authorized to logon and a failed interactive logon event should be logged in the security log.

When I tried to logon as "Partner1" I received the following message:

"The local policy of this system does not permit you to logon interactively"

Looking in the security log I found the following event:



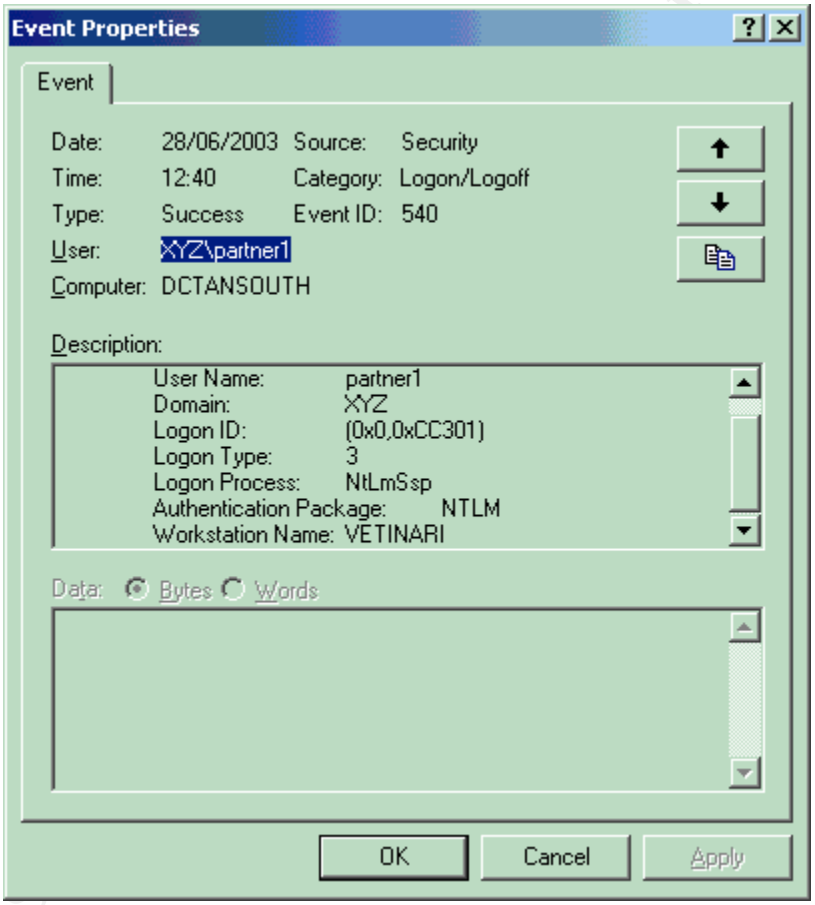
"Partner1" has not been permitted to log on to the system. The message and the event log demonstrate that my policy has been applied successfully.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Test 3 (Access this computer from the Network policy)

In my policy I permitted to the "Authenticated Users" group the permission to "Access this computer from the network". In order to test this policy I created a share "testshare" on the DC. If my policy has been applied successfully "Partner1" should be able to access it and a successful network logon event should be logged on the security log.

The connection with "testshare" was opened and the following event was logged in the security log:



This demonstrates that network logon is still possible therefore my policy has been applied successfully.

Testing System's Functionality

Test 1 (Mail Server Functionalities MAPI/OWA/POP3/IMAP4)

Authenticated Users must be able to access this system in order to send/receive e-mails. Every user will be connected to the mail server using Outlook 2000 in

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

MAPI mode. The administrator will use OWA to test the system. Exchange 2000 provides also POP3 and IMAP4 support but they must be disabled. Therefore, after the application of my policy I must be able to send/receive mail using MAPI or OWA and all POP3/IMAP4 connections should be rejected. If the system is working as expected I will be able to send/receive mails when connected to the mail server with Outlook or OWA and I will receive an error when I will try to connect using either POP3 or IMAP4 protocols. I tried to start all sessions using the account "partner1" logged to a laptop named "Vetinari".

MAPI Session

The MAPI Session generated 2 logon events in the security log:

Event 540: Successful Network Logon
Event 680: Successful Account Logon

In order to monitor the SMTP Traffic flow I checked the following:

- SMTP Virtual Server Log.
- SMTP Headers of messages.

SMTP Virtual Server Log:

#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-06-29 10:35:14
#Fields: date time c-ip cs-username s-sitename s-computername s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status sc-win32-status sc-bytes cs-bytes time-taken cs-version cs-host cs(User-Agent) cs(Cookie) cs(Referer)
2003-06-29 10:35:14 - OutboundConnectionResponse SMTPSVC1 DCTANSOUTH - 25 - - 220+rincewind.discworld.test+Microsoft+ESMTP+MAIL+Service,+Version:+5.0.2195.6713+ready+at++Sun,+29+Jun+2003+11:41:22++0100+ 0 0 124 0 78 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionCommand SMTPSVC1 DCTANSOUTH - 25 EHLO - dctansouth.xyz.com 0 0 4 0 94 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionResponse SMTPSVC1 DCTANSOUTH - 25 - - 250-rincewind.discworld.test+Hello+[192.168.30.200] 0 0 51 0 188 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionCommand SMTPSVC1 DCTANSOUTH - 25 MAIL - FROM:<partner1@xyz.com> 0 0 4 0 188 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionResponse SMTPSVC1 DCTANSOUTH - 25 - - 250+2.1.0+partner1@xyz.com....Sender+OK 0 0 39 0 297 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionCommand SMTPSVC1 DCTANSOUTH - 25 RCPT - TO:<administrator@discworld.test> 0 0 4 0 297 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionResponse SMTPSVC1 DCTANSOUTH - 25 - - 250+2.1.5+administrator@discworld.test+ 0 0 39 0 313 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionCommand SMTPSVC1 DCTANSOUTH - 25 XEXCH50 - 1768+2 0 0 7 0 313 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionResponse SMTPSVC1 DCTANSOUTH - 25 - - 354+Send+binary+data 0 0 20 0 328 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionResponse SMTPSVC1 DCTANSOUTH - 25 - - 250+XEXCH50+OK 0 0 14 0 328 SMTP - - - -

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionCommand SMTPSVC1 DCTANSOUTH - 25 BDAT - 1867+LAST 0 0 4 0 328 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionResponse SMTPSVC1 DCTANSOUTH - 25 - - 250+2.6.0++<C75C6B6CD007A84BACDFC4A26E6FDC7F8654@dctansouth.xyz.com>+Queued +mail+for+delivery 0 0 93 0 485 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionCommand SMTPSVC1 DCTANSOUTH - 25 QUIT - - 0 0 4 0 485 SMTP - - - -
2003-06-29 10:35:14 rincewind.discworld.test OutboundConnectionResponse SMTPSVC1 DCTANSOUTH - 25 - - 221+2.0.0+rincewind.discworld.test+Service+closing+transmission+channel 0 0 71 0 485 SMTP - - - -
2003-06-29 10:35:55 192.168.30.191 rincewind.discworld.test SMTPSVC1 DCTANSOUTH 192.168.30.200 0 EHLO - +rincewind.discworld.test 250 0 322 29 16 SMTP - - - -
2003-06-29 10:35:55 192.168.30.191 rincewind.discworld.test SMTPSVC1 DCTANSOUTH 192.168.30.200 0 MAIL - +FROM:<Administrator@discworld.test> 250 0 53 40 16 SMTP - - - -
2003-06-29 10:35:55 192.168.30.191 rincewind.discworld.test SMTPSVC1 DCTANSOUTH 192.168.30.200 0 RCPT - +TO:<partner1@xyz.com> 250 0 29 26 0 SMTP - - - -
2003-06-29 10:35:55 192.168.30.191 rincewind.discworld.test SMTPSVC1 DCTANSOUTH 192.168.30.200 0 xexch50 - +2256+2 354 0 22 14 0 SMTP - - - -
2003-06-29 10:35:55 192.168.30.191 rincewind.discworld.test SMTPSVC1 DCTANSOUTH 192.168.30.200 0 DATA - +<CAAECA2D07C0C44E82C99AF59D67E1E9EF6E@rincewind.discworld.test> 250 0 101 792 343 SMTP - - - -
2003-06-29 10:35:55 192.168.30.191 rincewind.discworld.test SMTPSVC1 DCTANSOUTH 192.168.30.200 0 QUIT - rincewind.discworld.test 0 437 67 4 0 SMTP - - - -

SMTP Headers (from partner1@xyz.com to administrator@discworld.test)

Microsoft Mail Internet Headers Version 2.0
Received: from mail pickup service by rincewind.discworld.test with Microsoft SMTPSVC;
Sun, 15 Jun 2003 17:47:26 +0100
Received: from dctansouth.xyz.com ([192.168.30.200]) by rincewind.discworld.test with Microsoft SMTPSVC(5.0.2195.5329); Sun, 15 Jun 2003 17:47:25 +0100
Subject: test
Date: Sun, 15 Jun 2003 17:41:49 +0100
Message-ID: <C75C6B6CD007A84BACDFC4A26E6FDC7F864C@dctansouth.xyz.com>
X-MS-Has-Attach:
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----_=_NextPart_001_01C3335D.04701DDC"
X-MS-TNEF-Correlator:
Thread-Topic: test
thread-index: AcMzXQdfSWntf/f4TnWbZOU2laEjvA==
Content-Class: urn:content-classes:message
From: "partner1" <partner1@xyz.com>
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
To: <administrator@discworld.test>
Return-Path: <partner1@xyz.com>
X-OriginalArrivalTime: 15 Jun 2003 16:47:25.0558 (UTC) FILETIME=[CCB03160:01C3335D]

SMTP Headers (from administrator@discworld.test to partner1@xyz.com)

Microsoft Mail Internet Headers Version 2.0

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Received: from rincewind.discworld.test ([192.168.30.191]) by dctansouth.xyz.com with Microsoft SMTPSVC(5.0.2195.5329);
Sun, 15 Jun 2003 17:56:17 +0100
Received: from mail pickup service by rincewind.discworld.test with Microsoft SMTPSVC;
Sun, 15 Jun 2003 17:59:53 +0100
Return-Receipt-To: "Administrator" <Administrator@discworld.test>
Subject: RE: test
Date: Sun, 15 Jun 2003 17:59:48 +0100
Message-ID: <CAAECA2D07C0C44E82C99AF59D67E1E906B324@rincewind.discworld.test>
X-MS-Has-Attach:
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----_=_NextPart_001_01C3335F.8763A270"
X-MS-TNEF-Correlator:
Thread-Topic: test
thread-index: AcMzXQdfSWntf/f4TnWbZOU2laEjvAAAbFSA
Content-Class: urn:content-classes:message
From: "Administrator" <Administrator@discworld.test>
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1165
To: "partner1" <partner1@xyz.com>
X-OriginalArrivalTime: 15 Jun 2003 16:59:53.0113 (UTC) FILETIME=[8A440890:01C3335F]
Return-Path: Administrator@discworld.test

As you can see my mail has been correctly sent and its reply has been correctly received.

OWA Session

The OWA Session generated 2 logon events in the security log:

Event 540: Successful Network Logon
Event 680: Successful Account Logon

In order to check if my OWA experience was behaving correctly I checked the logs of my IIS Web Server.

Here is the result:

#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-06-29 09:19:48
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)
2003-06-29 09:19:48 192.168.30.76 - 192.168.30.200 80 GET /exchange - 401 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:21 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchange - 302 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:21 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchange/ - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2003-06-29 09:20:21 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchange/partner1/ Cmd=navbar 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:21 192.168.30.76 - 192.168.30.200 80 GET /exchange/partner1/Inbox/ Cmd=contents 401 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:21 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchange/partner1/Inbox/ Cmd=contents 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:26 192.168.30.76 XYZ\partner1 192.168.30.200 80 SUBSCRIBE /exchange/partner1/Calendar - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:26 192.168.30.76 XYZ\partner1 192.168.30.200 80 SUBSCRIBE /exchange/partner1/Inbox - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:28 192.168.30.76 XYZ\partner1 192.168.30.200 80 SEARCH /exchange/partner1/Calendar - 207 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:28 192.168.30.76 XYZ\partner1 192.168.30.200 80 SEARCH /exchange/partner1/Inbox/ - 207 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchange/partner1/Drafts/ Cmd=new 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/controls/util_Recipients20.js - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/controls/um_ComposeMsg20.js - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/controls/um_ReadMsg20.js - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/controls/frm_ComposeNote20.js - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/img/tool-save.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/img/tool-print.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET +CLR+1.1.4322)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/img/tool-attach.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/img/tool-checknames.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/controls/ctrl_Message20.htc - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/img/tool-highimport.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/img/tool-lowimport.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/img/winme.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:34 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/img/tool-options.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:35 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/controls/ctrl_Message20.htc - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:35 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/CONTROLS/ctrl_FormatBar20.htc - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:35 192.168.30.76 - 192.168.30.200 80 GET /exchweb/CONTROLS/ctrl_FormatBar20.htc - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:35 192.168.30.76 - 192.168.30.200 80 GET /exchweb/img/tool-font.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:35 192.168.30.76 - 192.168.30.200 80 GET /exchweb/img/form-fgcolor.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:35 192.168.30.76 - 192.168.30.200 80 GET /exchweb/img/form-justify_center.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:35 192.168.30.76 - 192.168.30.200 80 GET /exchweb/img/form-justify_left.gif - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2003-06-29 09:20:35 192.168.30.76 - 192.168.30.200 80 GET /exchweb/img/form-justify_right.gif - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:35 192.168.30.76 - 192.168.30.200 80 GET /exchweb/img/form-bullist.gif - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:35 192.168.30.76 - 192.168.30.200 80 GET /exchweb/img/form-numlist.gif - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:35 192.168.30.76 - 192.168.30.200 80 GET /exchweb/img/form-deindent.gif - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:35 192.168.30.76 - 192.168.30.200 80 GET /exchweb/img/form-inindent.gif - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:37 192.168.30.76 - 192.168.30.200 80 GET /exchange/partner1 Cmd=dialog&template=dlg_gal 401
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:37 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchange/partner1 Cmd=dialog&template=dlg_gal 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:37 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/controls/dlg_GAL20.css - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:37 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/controls/dlg_GAL20.js - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:55 192.168.30.76 XYZ\partner1 192.168.30.200 80 POST /exchange/partner1/Drafts - 302
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:55 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchange/partner1/Drafts/No+Subject.EML Cmd=recips 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:20:57 192.168.30.76 XYZ\partner1 192.168.30.200 80 POST /exchange/partner1/Drafts/No+Subject.EML - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:21:03 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchange/partner1/ Cmd=logoff 302
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)
2003-06-29 09:21:03 192.168.30.76 XYZ\partner1 192.168.30.200 80 GET /exchweb/bin/ITN/logoff.asp - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461;+.NET+CLR+1.0.3705;+.NET+CLR+1.1.4322)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

This log demonstrates that I successfully connected to my system using OWA.

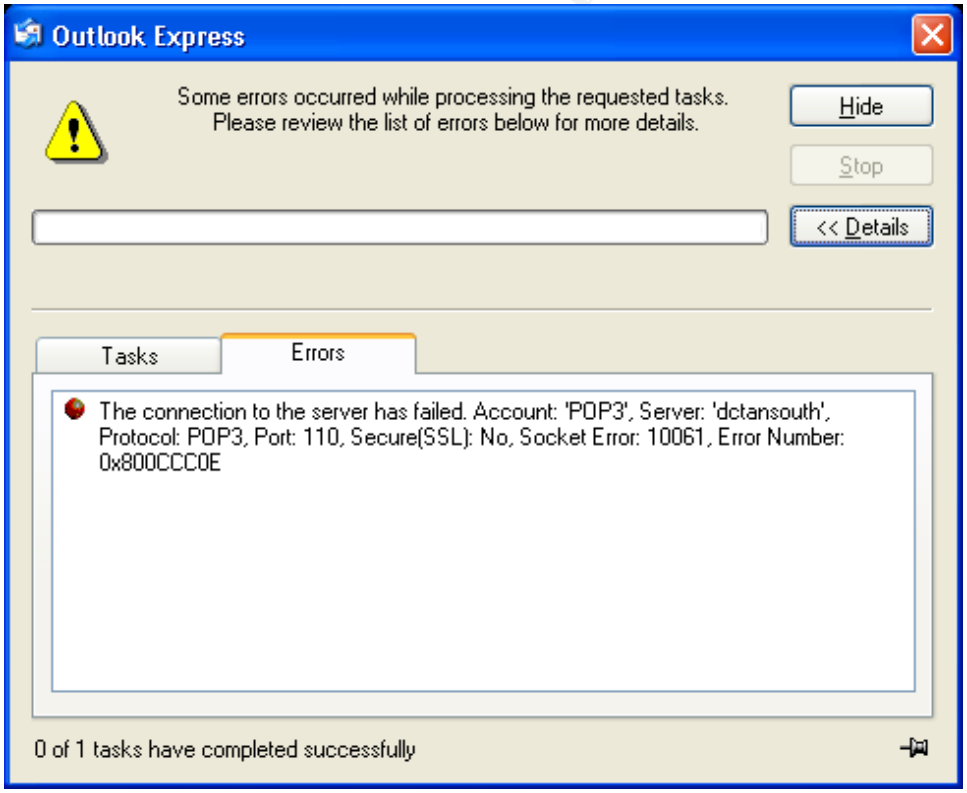
In Appendix D I have added the SMTP Headers of the mail sent and its reply.

POP3 and IMAP4

POP3 and IMAP4 services must not be used to retrieve mail therefore I stopped them in Exchange System Manager and I set them to “disable” in the “System Services” section of security policies.

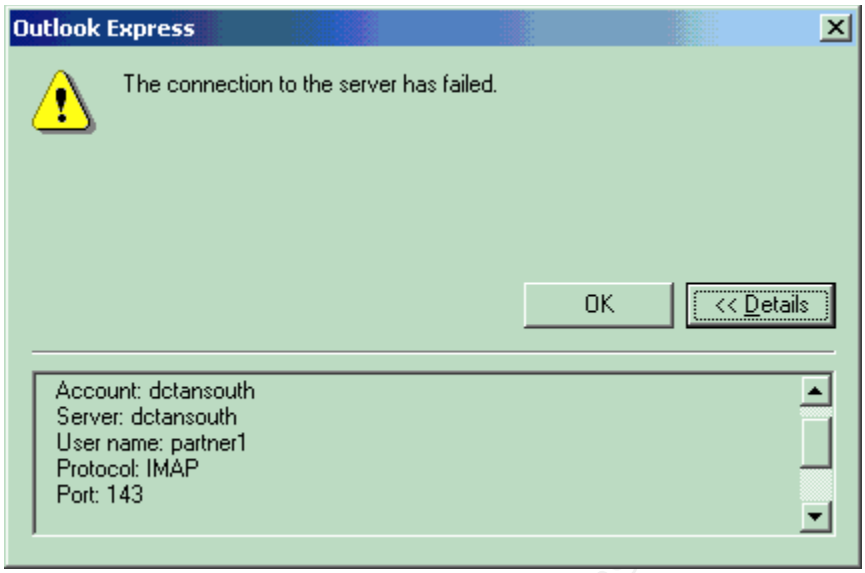
In order to test if they were not running I configured Outlook Express to connect to Exchange as “Partner1” with a POP3 profile and an IMAP4 profile.

When I tried to use the POP3 Outlook Express profile I received a connection error (see picture below). A description of this error may be found in following Microsoft KB article: Outlook Express POP3, Error 0x800ccc0e, Socket Error 10061



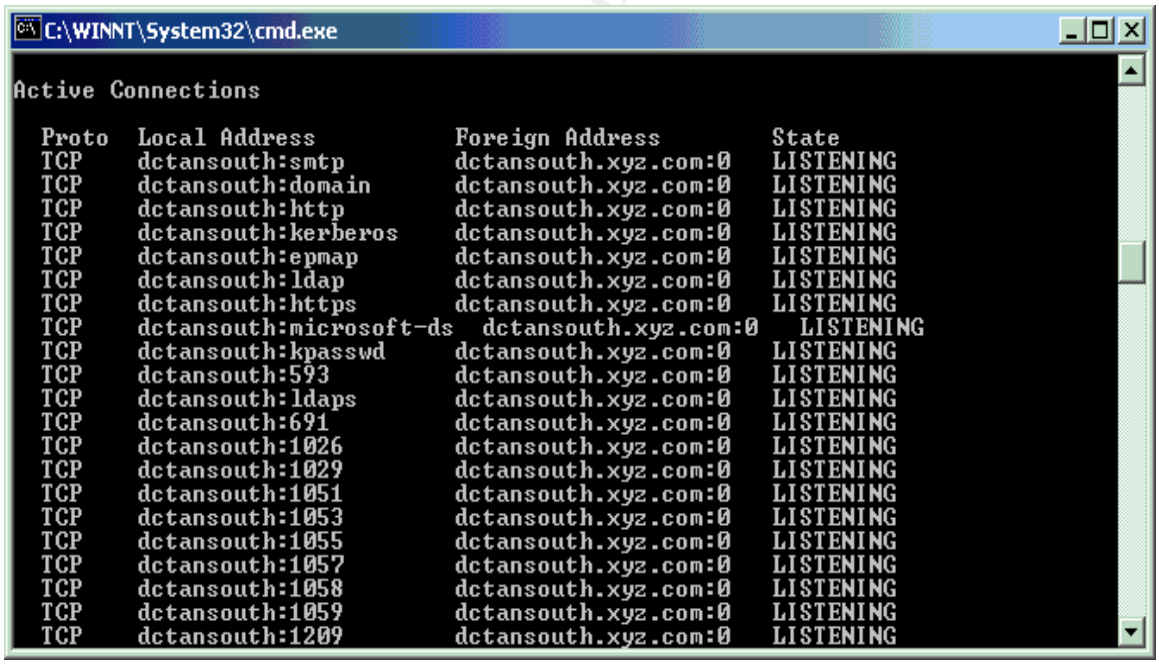
When I tried to use the IMAP4 Outlook Express profile I received a connection error (see picture below).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



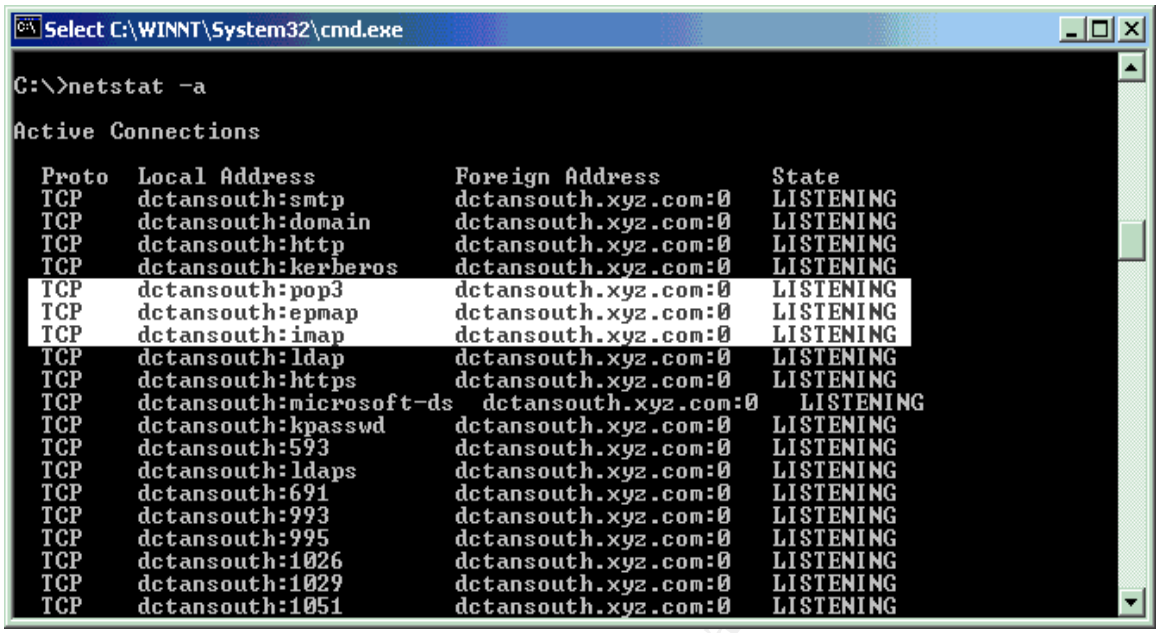
Another evidence that POP3 and IMAP4 services are not running is the output of the “netstat” command run on the DC.

These are the results on my DC:



These are the results on a system with POP3 and IMAP4 enabled:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



As you can see, when the services are started “Netstat” output displays both POP3 and IMAP ports in “Listening” status.

Test 2 (Antivirus Functionalities)

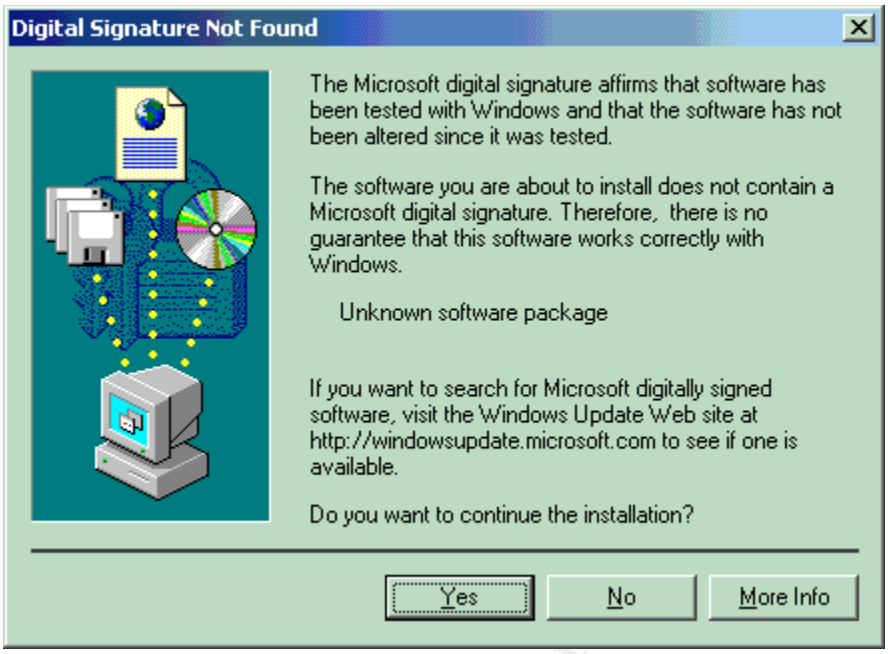
The antivirus products must be able to function. In order to the antivirus products installed on the system I downloaded the EICAR Antivirus Test File from the EICAR Web Site.
I copied the test file on the c:\ drive to test Symantec Antivirus Corporate Ed.
I sent the test file as a mail attachment to one of my users to test Symantec Antivirus Filtering for MS Exchange.
In both cases the string has been detected and deleted/quarantined.
The administrator received an e-mail from the system to be notified of the action as configured in the products.

Test 3 (Patches Application)

The system must be able to receive additional patches. In order to test this feature I tried to install the Exchange 2000 Post SP3 Rollup Patch 6396.1.
To complete this task I logged on the DC as “Commander” (The renamed administrative account).

During the procedure I was prompted to confirm the installation because the package was “unsigned”. This demonstrated that the “Unsigned non-driver installation behavior” policy in the “Security Options” section was applied successfully.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



The installation, in order to continue, needed to stop Exchange Services. The automated procedure went fine demonstrating that the ACLs set using the "System Services" section were applied successfully granting, at the same time, the possibility to install new patches/programs.

The successful installation of the patch was stated by the event id 4359 in the Application Log (Exchange Server Hotfix 813840 was installed)

CONCLUSIONS

The task of securing a system has always been difficult. Nowadays securing a system involves the configuration of hundreds parameters, registry keys, ACLs and others. Many checklists have been released to help administrators but, most of the times, they are targeted to high-level professionals with in-depth knowledge of the systems. Another problem is that they are often long and difficult to follow. But the need for security is not limited to big companies. The owner of a system used in a DDoS attack, even if unaware of it, can be accused of having helped the attacker. The basis of this accuse is that he/she has not protected his/her system enough implicitly inviting the attacker to use the system for his/her needs. Security policies can be a solution to help administrators to approach security configuration in an easier way. Here you have some of their most interesting features:

- They can be managed from a single console (The security configuration and analysis tool).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- They can be deployed easily (I can create a template and apply it manually or deploying it automatically using Group Policies in AD).
- Once applied, they are continuously enforced on the systems.
- They can be tested easily.
- They include hundreds of parameters that, without them, should be located in many different places.
- They can be used incrementally (I can apply more than one template to the same system).
- Last but not least they are free and already integrated in the system.

Security Policies have been really useful to configure my operating system but they lack of important sections. I cannot use them to manage even the most basic security settings for services like Exchange, DNS and IIS. This is a limitation to their capabilities that obliged me to resort to checklists and 3rd party tools in order to complete my tasks. The fact that these important services are not monitored by policies will oblige the administrator to check often their configuration manually. This is a problem because the manual check may not be accurate and could be difficult to perform regularly. This may be solved running scheduled scripts but they may be inaccurate and the scripts could be difficult to modify by the administrator. According to me policies are not a sufficient tool to secure a system like mine but they surely guarantee a good security standard for my system. They limit the settings that I will have to check manually every time limiting the probability of human errors. I am inclined to think this cannot be considered a real limitation. Even if they cannot cover completely my system's configuration they are a good starting point for many administrators. It could be interesting to have the possibility to install additional policies while installing applications but this introduces many other possible problems:

- Securing some Exchange 2000 configurations means acting directly on the configuration or schema containers of AD.
- More policies mean more replication traffic between DCs.
- Their attributes are defined in the schema therefore a schema extension could be needed with all its implications.

Microsoft extended them with Windows 2003 giving us an even more advanced capability to manage security settings but thinking that they will ever be the jack-of-all-trades security tool may remain a dream. In conclusion policies do not satisfy my needs completely but they helped me much to complete the task of securing a DC with Exchange 2000 installed.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

APPENDIX A: SOME DEFINITIONS

This is a quick summary of the terminology that I have used in this document.

Contained Domain Model [(1)]:
A Contained Domain is a Microsoft Windows 2000 domain that does not extend across any networks not controlled by the organization. For example, a Protected Network could be considered a LAN protected by a firewall and a router. Any domain that does not extend past this firewall or router would be considered contained. Microsoft defines a site as any part of a network that is connected by a WAN link. Based on this definition, a Contained Domain is any domain that does not cover more than one site as long as the entire site is controlled by the organization defining the network architecture.

Internet [(1)]:
Almost everyone today is aware of the Internet, but it is often confused with the World Wide Web (WWW, or "the web"). The web is part of the Internet, as are USENET (newsgroups) and ISPs (Internet Service Providers) such as AOL (America On Line), CompuServe and MSN (Microsoft Network). As the "World Wide Web" implies, the Internet spans the world. Anyone can connect to the Internet. Hackers, whether they are domestic or foreign, hobbyist, script-kiddies or professionals, scan systems looking for vulnerable computers. Once they find them, they take advantage of the vulnerabilities and can then deface web pages, take out servers (Denial of Service attacks), retrieve sensitive data or use the system to attack other systems. In short, the Internet is an environment that cannot be blindly trusted. The Internet provides a convenient medium to connect to other networks, but it does not provide reliable security features, such as user authentication and validation, server validation, or protection from hostile users or software.

Domain Controller [(1)]:
Domain Controller 1 represents the first domain controller installed in a domain. By default this domain controller has special functionality including schema master, PDC emulator, etc. Therefore, it is recommended that this host have more protection and not be used for simple user authentication, but for domain administration purposes. If the Protected Network is a site in a larger domain, this domain controller will be replaced with a Corporate Domain Controller. If any of the master tokens, like schema master, have been moved from this domain controller then extra protection should be placed on that domain controller as well.

Internal DNS Server [(2)]:

[1] Microsoft Windows 2000 Network Architecture Guide, NSA
[2] Microsoft Windows 2000 Network Architecture Guide, NSA

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Internal DNS Server provides the functionality required by Windows 2000 for registering domain services and clients in the domain. This server is extremely important because it holds a complete map of the domain. Therefore, this server should not share any information with the External DNS Server. Since there may be requirements for reverse lookup zones to include clients in the Protected Network, the reverse lookup zone on the internal server may need to be passed to the External DNS Server. The functionality of this server may be included on a domain controller. However, if DNS data is required externally, a specific, non-domain controller based DNS should be established to communicate the information to the external server. Like domain controllers, the better connection clients have to the internal DNS server, the better the network will perform.

Internal Mail Server [(1)]:
Users within the site to both send and receive mail utilize the Internal Mail Server. It should be configured to send all outgoing mail to the mail forwarder. The risks associated with the internal mail server are similar to that described for mail forwarder. Again, content checking and filtering capabilities are critical countermeasures. Additionally, a large concern is preserving data confidentially and integrity by utilizing user authentication and access control mechanisms to limit users to content for which they are authorized access (e.g., their own mailbox). Data encryption can also be utilized for sensitive data with the common options including the S/MIME standard for reader-to-writer data protection or SSL for protecting data in transmission between the client and server (e.g. SMTP over SSL and IMAP over SSL).

Mail Forwarder [(1)]:
There are several risks associated with the receipt of e-mail from potentially untrusted entities outside the site. Chief among these concerns are attacks against the recipient email server itself. Examples of this include attempts to exploit buffer overflows and content driven attacks in the form of malicious code. The Mail Forwarder is simply a mail server that forwards e-mail messages intended for internal users to the internal mail server and accepts mail destined for the external network for delivery. As the Mail Forwarder is the only mail server that is exposed to the external network, precluding direct access to the internal mail server reduces the risks associated with e-mail. This Mail Forwarder, as should be the case for all servers in the DMZ, must not be a member of any internal Windows 2000 domains. This will limit the damage that could result from its compromise. Content checking, initial virus scanning, and filtering ideally should also be performed here to guard against malicious code.

Malicious Mobile Code [(1)]: Malicious mobile code is any software program designed to move from computer to computer and network to network, in order to intentionally modify computer systems without the consent of the owner or operator.

[1] Malicious Mobile Code (Virus Protection for Windows), O'Reilly and Associates

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

APPENDIX B: CONSIDERATIONS ON MY SYSTEM'S ROLES

Domain Controller

In a DC are stored all Active Directory (AD) information related to the domain of which the DC is member. The AD database is composed by 3 distinct naming contexts: Schema, Configuration and Domain Naming. Each of these contexts contains different information, which are all necessary to the correct functioning of the architecture. The schema naming-context defines every object class and attribute that can be stored in AD. The Configuration context contains data such as site definitions, service configuration and replication topology. The Domain Naming context contains all Organizational Units (OUs), Servers, Printers and user account objects of the domain.

Schema Master

The Schema master is the domain controller that controls every operation carried out on the schema naming-context. There is only one schema master per forest. If you want to access the schema configuration to add objects or to change the operation master you must use the active directory schema snap-in. If the schema master is offline any schema modification will not be possible. Object classes and attributes cannot be deleted from the schema even if they have been created by a schema admin. If an object class attribute is not needed it may be disabled. Exchange 2000 adds 155 object classes, 818 attributes to the schema naming-context. Every Exchange class or attribute name begins with "msExch" and "ms-Exch" to be easily recognized.

Note: To enable the "schema management" Snap-in you must register the snap-in with the command "*regsvr32 schmmgmt.dll*". Then add it to a new mmc.

To move this role from one server to another you must use the "schema management" snap-in on the server where you want to move the role.

Many documents state that the Schema object (both classes and attributes) cannot be deleted. For information on deleting AD schema objects please refer to the following article on Windows & .NET Magazine: Your mission: Delete from the AD Schema (Doc ID: 27096)

Domain Naming Master

The Domain Naming Master is the domain controller that controls the addition or removal of domain in the forest. There is only one domain naming master per forest. If the Domain Naming Master is offline you will not be able to add or delete any domain to the forest.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

To move this role from one server to another you must use the "Active Directory Domains and Trusts" snap-in on the server where you want to move the role.

Infrastructure Master

The Infrastructure Master is responsible for updating all inter-domain references whenever an object referenced by another object moves. For example, whenever the members of groups are renamed or changed, the infrastructure master updates the group-to-user references" [(1)]. There is only one Infrastructure Master per domain. In the XYZ environment the Infrastructure master is on the same machine as the Global Catalog. This configuration shouldn't be used in multiple DCs environments. "The infrastructure master role should not be assigned to the domain controller that is hosting the global catalog. If the infrastructure master and global catalog are on the same domain controller, the infrastructure master will not function. The infrastructure master will never find data that is out of date, so will never replicate any changes to the other domain controllers in the domain. If all of the domain controllers in a domain are also hosting the global catalog, all of the domain controllers will have the current data and it does not matter which domain controller holds the infrastructure master role." [(2)]. If the Infrastructure Master is offline every modification to the inter-domain references will not be replicated (i.e. account creation or modification).

To move this role from one server to another you must use the "Active Directory Users and Computers" snap-in on the server where you want to move the role.

PDC Emulator

The PDC emulator has different functions depending if the AD Domain is in mixed mode or native mode:

Mixed Mode:

1. Windows NT PDC processing password changes and replication to the BDCs.

2. Every non-AD aware client (i.e. Win95/98/NT without AD client installed) must connect to the PDC emulator to change passwords.

Native Mode:

1. PDC emulator is the preferential replicator of password changes done on other DCs.

[1] Windows 2000 Security: Technical Reference, Microsoft Press.
[2] Windows 2000 Server Documentation: Global Catalog and Infrastructure master

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2. If a DC receives a logon authentication error it will forward the request to the PDC emulator before rejecting it.

There is only 1 PDC Emulator per domain.

To move this role from one server to another you must use the “Active Directory Users and Computers” snap-in on the server where you want to move the role.

RID Master

The RID Master is responsible for allocating sequences of RIDs to each DC in its domain. Every time that a security principal (user, group or computer) is created it receives a unique identifier which is composed by SID and RID. The SID is a string that is the same for every security principal created in the domain while the RID is unique for every security principal created in the domain. There is only 1 RID Master per domain.

To move this role from one server to another you must use the “Active Directory Users and Computers” snap-in on the server where you want to move the role.

Global Catalog

The Global Catalog (GC) is a database kept on 1 or more domain controller which contains every information about its domain’s NCs and a subset of other domains NCs (only classes and attributes that are marked for GC replication in the “Schema Management” snap-in. GC performs primarily two tasks: logon and querying.
Logon: The GC processes every domain authentication request (interactive to a domain user account, network logon, and computer logon). If a GC is not available only local logon attempts may be processed. The only exception is the “domain administrators” group whose members can logon to the domain even without a GC. If domain is in mixed mode GC is not needed for logon.

Querying: GCs may be used to query search for AD objects without querying every domain individually. This objective is achieved because between GCs there is a subset of objects/attributes that are replicated even beyond domain boundaries. In the “schema management” snap-in it is possible to see what objects/attributes are replicated and, if you want, it is possible to add new ones to the subset. Exchange 2000 marks 270 new attributes for replication.

If you want to assign the GC role to a DC you have to use the “Active Directory Sites and Services” snap-in.

In Exchange 2000 environment the GC plays an important role. MAPI clients and some connectors need to query the directory service in order to find mailboxes and recipients and the GC is the server, which can answer queries made against the entire forest. To redirect directory service request is used the DSProxy

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

module of the Exchange System Attendant service. “Smart” MAPI client like Outlook 2000/XP don’t need to be redirected. They are configured to “remember” the last GC used in order to have faster responses, in case of connection problems with the GC they will query again Exchange to find another one. If no GCs are active in the domain the Exchange architecture won’t work correctly.

Internal DNS Server

To work correctly AD needs a Domain Name System (DNS) server. DNS is used by AD to locate its resources (GCs, DCs, etc.), which are defined using the SRV (Service) record type. To solve/minimize some security and availability problems that were typical of the standard primary and secondary zones (DNS Poisoning, zone data in clear-text files, Network mapping by intercepting DNS zones replication, some types of DNS spoofing attacks) has been added a new type of DNS zone: the AD Integrated zone. This zone may be created only if the DNS is also a DC.

AD Integrated zones are more secure for these reasons:

1. They are stored in the domain naming-context of AD. This means that they become part of AD and they will replicate with it (Domain Naming Context). Every DC in the forest will have a copy of them even if the DNS service is not installed.
2. The “Only Secure Updates” option will be available for Dynamic Updates.

The XYZ DNS strategy is to use an AD Integrated zone stored in the DC and to forward all external name resolution traffic to the ISP’s DNSs. The zone transfer port (53 TCP) will be closed on the gateway while the name resolution port (53 UDP) will be open.

Internal Mail Server

E-mail is one of the most popular forms of communication today. They permit to exchange text messages, programs, pictures and documents. The correct use of this resource may be the factor that defines if a business is successful or not. Every mail sent or received has an implicit intellectual value that renders it an important asset that must be protected. The SMTP protocol has been developed to transmit mail between heterogeneous mail systems. It is defined in the RFC 2821. The incredible diffusion of this form of communication has led to the development of an incredible number of enhancements to its original specifications (for example: HTML messages, embedded multimedia content, embedded ActiveX commands, Web-based e-mail) that generated an incredible number of security issues.

Some examples of these issues are:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1. A malicious user with a protocol analyzer may intercept sensitive information (passwords, source code, confidential documents, etc…) (Packet Sniffing).
2. Malformed packets (i.e. MS02-012 Security Bulletin) or mail flood attacks (i.e. Avalanche 3.7 tool) may generate Denial of Service conditions.
3. Spam/Scam may generate unwanted network traffic and may reduce the employee's productivity (The message may distract your users from their duties).
4. Uncontrolled Mail Relaying may be used to take advantage of your server in a DDoS attack to a 3rd party server or to cause DoS conditions (either using the simple quantity of messages or by provoking your mail domain to be added to the Spam blacklists).
5. Malicious code attached or inserted in a message may be run without user intervention (i.e. the W32/Iirva@mm virus family).

APPENDIX C: BRIEF DESCRIPTION OF FIREWALL CONFIGURATION

Important: The configuration of the firewall is not in the scope of this document. This appendix wants to give an idea of how the firewall works and what will be its configuration.

Symantec Enterprise Firewall 7.0 is an application-level proxy firewall. This family of firewalls provides a set of application-specific inspection modules. Each daemon maintains connection state information and inspects the data stream it subsequently receives during the session.
This works as follows:

- When the firewall system receives a packet, it determines which proxy should process it.
- If it is an initial connection request, the proxy first determines whether it is allowed. If it is allowed, a corresponding connection is established with the intended computer.
  - Therefore, for application-level traffic, there are always 2 connections (TCP) or 2 data streams (UDP). The first one between the firewall and the source and the other one between the firewall and the destination
  - The proxy acts as a transparent intermediary. Neither endpoint is aware that the firewall is intercepting connection requests and taking the appropriate action for those that are allowed.
  - In addition the source and the destination IP addresses can be rewritten.
- For the duration of the session, the proxy is responsible for evaluating any attempt to pass data into or out of the protected network for that session.

The firewall will provide the following advantages:

- User Authentication

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- The firewall is not technically a router therefore it will protect the network against routing-based attacks.
- IP address masking.
- The system where the firewall will reside will be automatically hardened during firewall installation and the configuration will be maintained by a daemon, which will monitor for changes and eventually will disable them.
- Protection against several types of network-level threats, including address spoofing, TCP Syn Flood, and fragmentation-based attacks.

The following protocols will be allowed on the firewall:

- HTTP and HTTPS (HTTPd)
- FTP (FTPd)
- SMTP from Exchange to Mail Forwarder and vice versa (SMTPd)
- DNS queries (DNSd)

APPENDIX D: REFERENCES AND ADDITIONAL READINGS

1) Paul F. Bartock Jr., Paul L. Donahue, Daniel J. Duesterhaus, Julie M. Haney, Prentice S. Hayes, Trent H. Pitsenbarger, 1st Lieutenant Robin G. Stephens, Neil L. Zeiring. Microsoft Windows 2000 Network Architecture Guide. NSA. April 2001. Version 1.0

2) Haney, J. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set. NSA. December 2000. Version 1.2.

3) Stephens, Capt. Robin G. USAF. Guide to Security Microsoft Windows 2000 DNS. NSA. April 2001. Version 1.0.

4) Sanderson, Mark J., Rice, David C. Guide to Securing Microsoft Windows 2000 Active Directory. NSA. December 2000. Version 1.0.

5) Rice, David C. Guide to Securing Microsoft Windows 2000 Schema. NSA. March 2001. Version 1.0.

6) Pitsenbarger, Trent H. Guide to Secure Configuration and Administration of Microsoft Exchange 2000. NSA. August 2002. Version 1.12.

7) Grimes, Roger A., Malicious Mobile Code (Virus Protection for Windows). O'Reilly & Associates. 1st Edition. ISBN:1-56592-682-X

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

8) Internet Security Systems, Inc. Windows 2000 Security, Technical Reference. Microsoft Press. ISBN: 0-7356-0858-X

9) Komar, Brian. Designing Microsoft Windows 2000 Network Security Training Kit. Microsoft Press. ISBN: 0-7356-1134-3

10) Microsoft Corporation and Kay Unkroth. Microsoft Exchange 2000 Server Design and Deployment Training Kit. Microsoft Press. ISBN: 0-7356-1257-9

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.