

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.

Securing Windows running Trend Micro Services with Security Templates

GIAC Certified Windows Security Administrator

Version 3.1

Curtis Simonson

March 2003

© SANS Institute 2003, Author retains full rights.

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

Table of Contents

1 Description of System 6
2 Checklists and Templates 11
3 Template Security Settings and suggested changes 12
3.1 Account Policies 13
3.1.1 Password Policies: 13
3.1.2 Account Lockout Policy: 14
3.2 Kerberos Policy 14
3.3 Local Policies 14
3.3.1 Audit Policy 14
3.3.2 User Rights Assignment 15
3.3.3 Security Options 18
3.4 Event Log 21
3.5 Restricted Groups 22
3.6 System Services 22
3.7 Registry 22
3.8 File System 24
4 Steps to perform before applying the Template 27
4.1 Change Management 27
4.2 Back up before making changes 28
4.3 Pre Hardening Benchmarks 30
4.3.1 Pre System Test #1 - Account Password check 30
4.3.2 Pre System Test #2 - Null session check 30
4.3.3 Pre System Test #3 - Security log check 31
4.3.4 Pre System Test #4 - CIS Windows NT/2000 Security Scoring Tool 32
4.3.5 Pre System Test #5 - Web Server Vulnerability Assessment 33
4.3.6 Pre Application Test #1 – OfficeScan – Manage the Console 35

© SANS Institute 2003, Author retains full rights.

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

4.3.7 Pre Application Test #2 – OfficeScan – Force Client manual scan 36

4.3.8 Pre Application Test #3 – Server Protect – Manage the Console 36

4.3.9 Pre Application Test #4 – Server Protect – Force Client manual scan 36

5 Steps to install the template 37

5.1 Apply the template to the server 39

5.2 Harden the IIS Server 39

5.2.1 Remove unneeded Web components 39

5.2.2 Delete unneeded virtual directories 39

5.2.3 Delete unneeded and sample files 40

5.2.4 Disable Internet printing 40

5.2.5 Disable Parent paths 40

5.2.6 Enable Web logging 41

5.2.7 Install URLSCAN.DLL ISAPI Filter 41

5.2.8 Lock down Console file permissions 41

6 Test the Systems Functionality 42

6.1 Post System Test #1 - Account Password check 42

6.2 Post System Test #2 - Null Session check 42

6.3 Post System Test #3 - Security Event Log check 43

6.4 Post System Test #4 – Windows NT/2000 Security Scoring Tool 44

6.5 Post System Test #5 - Web Server Vulnerability Assessment check 45

6.6 Post Application Test #1 – OfficeScan – Manage the Console 45

6.7 Post Application Test #2 – OfficeScan – Force a manual scan of an OfficeScan client 46

6.8 Post Application Test #3 – Server Protect – Manage the Console 47

6.9 Post Application Test #4 – Server Protect – Force a manual scan of Server Protect client 47

7 Evaluate the Template 48

8 Undoing the Template – if required 48

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

9 Conclusion 49
10 Appendix A - URLSCAN.INI 50
11 References 53

© SANS Institute 2003, Author retains full rights.

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

Abstract

This paper will walk you through the steps of hardening a Windows 2000 Server. The server is running two specific enterprise antivirus application consoles. One is called Trend Micro OfficeScan and the other is called Server Protect. The steps include; selecting a suitable security template, discussing the template, making adjustments to the template to match the security requirements of the system, base lining the server before applying the template, discussing change control, performing backups, applying the template, making changes to IIS, testing the system and applications to ensure they continue to function and finally, evaluating the effectiveness of the template.

© SANS Institute 2003, Author retains full rights.

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

1 Description of System

Before hardening a system, it is important to understand the system and the requirements of the applications running on the system. This understanding should include knowing what network based communications are required, what type of authentication is used, what file and registry access is required, and what services are required by the operating system and by applications running on the system.

In this factitious company, Acme.ca, there are three computers of interest, TrendServer, AppServer1, and Workstation1. The system to be hardened is called TrendServer. It is a Dell 2550 server with a Pentium III processor running at 700 MHz, with one GB or ram and 54 GB of available disk space setup in a Raid level five - array. Partitions are set with an eight GB partition for the operating system installed on drive C: and the rest for the space is allocated to application data on drive D. Both drives are using the NTFS file system. The operating system used is Microsoft Windows 2000 Advanced Server with IIS 5.0 Web Services. Windows 2000 Service Pack 3 has been installed. The web server's root drive is installed on the C: drive with the Trend software installed on D. The other systems used are; AppServer1, a second Windows 2000 Advance Server with Service Pack 3 and Workstation1, a Windows 2000 Professional Workstation with Service Pack 3 used by the Antivirus Administrator. These computers are connected to the inside "Secure" network of the company and are setup in a Windows "Workgroup".

The important applications running on TrendServer are: Trend Micro [1] Server Protect - Information Server (for managing the protection of server clients running Server Protect – Normal Server) version 5.35, Trend Micro Server Protect – Normal Server (for local server protection), and Trend Micro - OfficeScan Corporate Edition version 5.5 Management Server (for managing the protection of Windows 9X, 2000 and XP OfficeScan clients).

This Server provides a key role in the company's security strategy by providing automated antivirus updates to workstations and servers, reporting computers with out-of-date virus signatures, alerting when virus outbreaks occur, and provides centralized antivirus logging. Microsoft IIS is required for the management of the Trend Micro OfficeScan console and in this case is used for the deployment of program and signature updates to OfficeScan web-based clients.

The level of security required on this system is medium based on its role in the company. It is located in a secure room where only trusted administrators have physical access.

Network communications required for these applications are:

OfficeScan:

- The *OfficeScan* Management Console running on TrendServer listens on ports 1079 and 1080 tcp and port 80 through the IIS web server.

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

- The *OfficeScan* client software protecting Workstation1 listens on port 52031 tcp. The *OfficeScan* Client can get updates from the Management Server via port 80 tcp.

- The Antivirus Administrator uses IE 6 web browser on Workstation1 to access the OfficeScan Management Console by accessing the web pages at http://Trendserver/Officescan via port 80 tcp. A combination of Anonymous and Integrated Windows authentication is required to manage the console.
- The OfficeScan Management Console connects to Trend Micro's web site for antivirus signature and program updates over port 80 tcp.

Server Protect:

- The Trend "Server Protect Information Server" listens on ports [2] 3000-3009 upd for the broadcast of a Management Console starting. It also listens on ports 5005 – 5014 tcp, which are used for communications between the Management Console and the Information Server.

- Server Protect installed as a Normal Server on AppServer1 listens on port 5168 tcp.

- The Server Protect Information Server and Server Protect Normal Server communicate with each other over ports 137 upd, 138 upd, and 139 tcp but will use 445 tcp if secure channel communication is turned on. They will also use ports 3628 and 5168 tcp.

- The Antivirus Administrator uses a local version of the Server Protect Management Console on Workstation1 to connect to and manage the Server Protect Information Server on TrendServer. When this application is launched, it broadcasts on 3000-3009 upd and listens on ports 1000-1009 tcp.

- The Server Protect Information Server communicates with Trend Micro's web site for antivirus signature and program updates over port 80 tcp.

- Other ports used are 1921 tcp and sometimes 9921 tcp for Netware Servers.

This is seen by using the FPORT [3] utility, the listening ports on TrendServer are:

```
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com
Pid   Process            Port  Proto Path
1420  inetinfo       ->  25    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
1380  wins           ->  42    TCP   C:\WINNT\System32\wins.exe
1408  dns            ->  53    TCP   C:\WINNT\System32\dns.exe
1420  inetinfo       ->  80    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
424   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
1420  inetinfo       ->  443   TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
```


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

```
8     System          ->  445   TCP
796   msdtc           ->  1027  TCP   C:\WINNT\System32\msdtc.exe
1176  MSTask          ->  1030  TCP   C:\WINNT\system32\MSTask.exe
1060  ntfrs           ->  1031  TCP   C:\WINNT\system32\ntfrs.exe
1408  dns             ->  1034  TCP   C:\WINNT\System32\dns.exe
1420  inetinfo        ->  1035  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
1380  wins            ->  1037  TCP   C:\WINNT\System32\wins.exe
8     System          ->  1055  TCP
1124  ofcservice      ->  1079  TCP   D:\OFScan\PCCSRV\web\service\ofcservice.exe
1124  ofcservice      ->  1080  TCP   D:\OFScan\PCCSRV\web\service\ofcservice.exe
952   EarthAgent      ->  1921  TCP   C:\Program Files\Trend\SProtect\EarthAgent.exe
796   msdtc           ->  3372  TCP   C:\WINNT\System32\msdtc.exe
952   EarthAgent      ->  3628  TCP   C:\Program Files\Trend\SProtect\EarthAgent.exe
952   EarthAgent      ->  5005  TCP   C:\Program Files\Trend\SProtect\EarthAgent.exe
676   SpntSvc         ->  5168  TCP   C:\Program Files\Trend\SProtect\SpntSvc.exe
1420  inetinfo        ->  7935  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe

1380  wins            ->  42    UDP   C:\WINNT\System32\wins.exe
1408  dns             ->  53    UDP   C:\WINNT\System32\dns.exe
424   svchost         ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System          ->  137   UDP
8     System          ->  138   UDP
8     System          ->  445   UDP
256   lsass           ->  500   UDP   C:\WINNT\system32\lsass.exe
244   services        ->  1029  UDP   C:\WINNT\system32\services.exe
1408  dns             ->  1032  UDP   C:\WINNT\System32\dns.exe
1408  dns             ->  1033  UDP   C:\WINNT\System32\dns.exe
1380  wins            ->  1036  UDP   C:\WINNT\System32\wins.exe
1420  inetinfo        ->  1038  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe
952   EarthAgent      ->  3000  UDP   C:\Program Files\Trend\SProtect\EarthAgent.exe
1420  inetinfo        ->  3456  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe
```

Using the XCACLS.exe utility from the Resource Kit, the default file access security settings required for Trend Micros Server Protect and OfficeScan applications are seen below. I have not shown all the folders and files, I have only shown the most important three folders. Displayed are the users and groups and the permissions currently assigned to them. E.g., BULTIN\Users: R means the local "users" group have Read access. C = change right, F = Full control, OI means Object Inherit (for files); CI means Container Inherit (for folders), IO mean Inherit only (for subfolders). Additional information can be read at http://www.thedance.net/~win95/cacls.html

```
C:\progra~1\Trend
           BUILTIN\Users:R
           BUILTIN\Users:(OI)(CI)(IO)(special access:)
                         GENERIC_READ
                         GENERIC_EXECUTE
           BUILTIN\Power Users:C
           BUILTIN\Power Users:(OI)(CI)(IO)C
           BUILTIN\Administrators:F
           BUILTIN\Administrators:(OI)(CI)(IO)F
           NT AUTHORITY\SYSTEM:F
           NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
           CREATOR OWNER:(OI)(CI)(IO)F
           NT AUTHORITY\TERMINAL SERVER USER:C
           NT AUTHORITY\TERMINAL SERVER USER:(OI)(CI)(IO)C

d:\OFScan\PCCSRV
           BUILTIN\Administrators:(OI)(CI)F
           Everyone:(OI)(CI)R
           TRENDSERVER\IUSR_TRENDSERVER:(OI)(CI)C

d:\OFScan\PCCSRV\Web
           BUILTIN\Administrators:(OI)(CI)F
           Everyone:(OI)(CI)R
           TRENDSERVER\IUSR_TRENDSERVER:(OI)(CI)C
```

Using DumpSec [4], you can list the registry access permissions for discussion purposes.

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

```
2003-01-28 6:19 PM - Somarsoft DumpSec (formerly DumpAcl) - \\TRENDSERVER (local)
Path (exception keys)          Account                  Own     Key      Inheritable
HKEY_LOCAL_MACHINE             SYSTEM                           all        all
HKEY_LOCAL_MACHINE             TRENDSERVER\Administrators   o   all        all
HKEY_LOCAL_MACHINE             Everyone                         read(QENR) read(QENR)
HKEY_LOCAL_MACHINE             RESTRICTED                       read(QENR) read(QENR)
HKEY_LOCAL_MACHINE\SAM\SAM                                   ==>access denied
HKEY_LOCAL_MACHINE\SECURITY                                  ==>access denied
HKEY_LOCAL_MACHINE\SOFTWARE    TRENDSERVER\Users                read(QENR) read(QENR)
HKEY_LOCAL_MACHINE\SOFTWARE    TRENDSERVER\Power Users    EN D  R QSCEN D  R
HKEY_LOCAL_MACHINE\SOFTWARE    TRENDSERVER\Administrators   o   all        all
HKEY_LOCAL_MACHINE\SOFTWARE    SYSTEM                           all        all
HKEY_LOCAL_MACHINE\SOFTWARE    CREATOR OWNER                                all
HKEY_LOCAL_MACHINE\SOFTWARE    TERMINAL SERVER USER  SCEN D  R QSCEN D  R
```

Using the MMC to view the Service security settings, we see that these applications use “Local System”:

```
OfficeScan Master Service           Local System
D:\OFScan\PCCSRV\web\service\ofcservice.exe

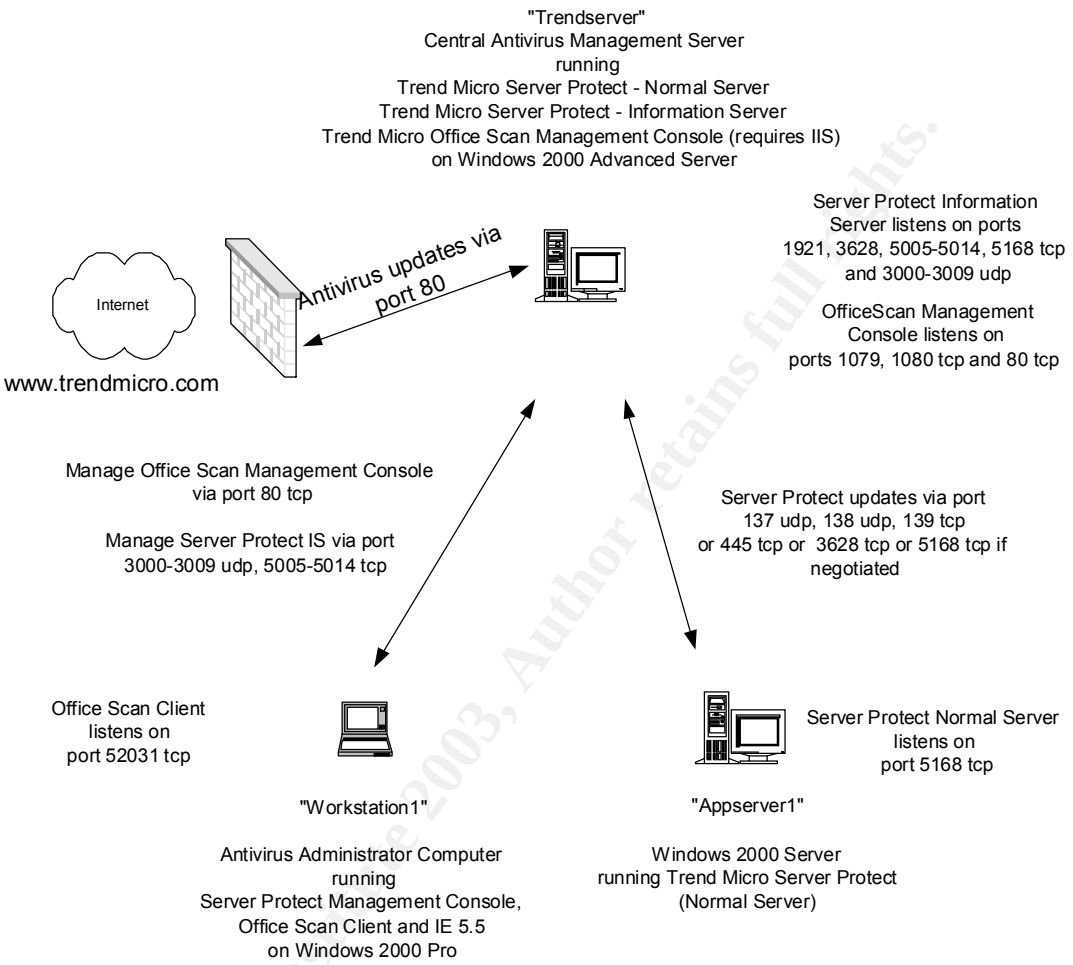
Trend ServerProtect                 Local System
C:\Program Files\Trend\SProtect\SpntSvc.exe

Trend ServerProtect Agent           Local System
C:\Program Files\Trend\SProtect\EarthAgent.exe
```

© SANS Institute 2003, Author retains full rights.

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

Acme.ca
Enterprise Antivirus System



© SANS Institute 2003, Author retains full rights.

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

2 Checklists and Templates

Security checklists have been around for a number of years. A number of organizations, including SANS [5] www.sans.org, produce well-documented step-by-step checklists for hardening several types of systems. One of the challenges with manually performing step-by-step procedures on systems is the large amount of time required per system, as there can be over one hundred steps to perform. Another challenge with manual steps is that one wrong setting in the wrong place can render the system inaccessible from the network and from the console. Using templates and other scriptable solutions (including using GPOs in Active Directory, Perl and Visual Basic scripts) provide a much better method for the deployment of hardening tasks as they require a lot less manual interaction and are a lot more accurate when repeated. With a template or scriptable deployment, most of your time will be spent during the selection of the template or script and tuning it to meet your needs. This is where proper training and knowledge are important. You may be tempted to "just pick a template" and hope for the best, when in fact you may break an application or not harden the system enough and leave the system still vulnerable.

For Windows systems, there are several templates to choose from a number of good companies. Microsoft provides several with Windows 2000 Professional, Server, and Domain Controllers. You should be able to find them in the C:\Winnt\SECURITY\templates folder of any Windows 2000 installation. These particular templates are named based on the security level and the system type to which they are to be applied. E.g. BASICWK.INF stands for basic security-workstation class computer, HISECDC.INF stands for high security-Domain Controller'. These samples are a good place to start to understand what is available. In most cases, templates assume a clean Windows 2000 install (not an upgrade from NT 4.0). A caution with the High Security templates is that will set the Lan Manager Authentication level to NTLMv2-only and sets "Secure channel - Always" communications to enable and the server will not communicate with down level windows clients that use LM or NTLM or computers that do not use "Secure channel" communication. For a Microsoft Windows 2000 Server running an IIS 5.0 Web Server, Microsoft has available for download a template called HISECWEB.INF [6] http://www.microsoft.com/downloads/details.aspx?FamilyID=564a8b50-17d7-46f1-9a22-d9637bae9547&DisplayLang=en. Other good templates are available from other organizations such as the Center for Internet Security [7] www.cisecurity.org (free but requires submission of name and e-mail) and the National Security Agency [8] http://nsa2.www.conxion.com/winnt/download.htm

As this server is running MS IIS for the Trend Micro OfficeScan Management Console, we may need to perform additional steps to harden the IIS in addition to the changes made by the template. For this server, I have chosen to start with the **SECUREINTRANETWEBSERVER.INF** template. This template is included in the Windows 2000 Server Resource Kit. This kit can be purchased from Microsoft. The template is found in the IIS.CAB file on the Resource Kit CD. This template looks like it will work well for the function of this server as:

- It will harden the server to reasonable level with one pass

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

- It has a small number of IIS hardening components
- It is designed for an Intranet server (not an Extranet Server)

This template is expected to:

- Close the Null Session vulnerability
- Tighten up the security of the file system from the default
- Turn on System Auditing
- Set requirements for passwords, set length, rotation and lockout settings
- Set event log sizes and access restrictions

Other expected outcomes:

- The System will remain stable and reliable
- The Trend Micro applications will continue to function
- The Server to score higher with a test using the Windows Security Scoring Tool provided for free by the Center for Internet Security
- The server will have fewer "possible vulnerabilities" when tested with a web server vulnerability assessment tool.

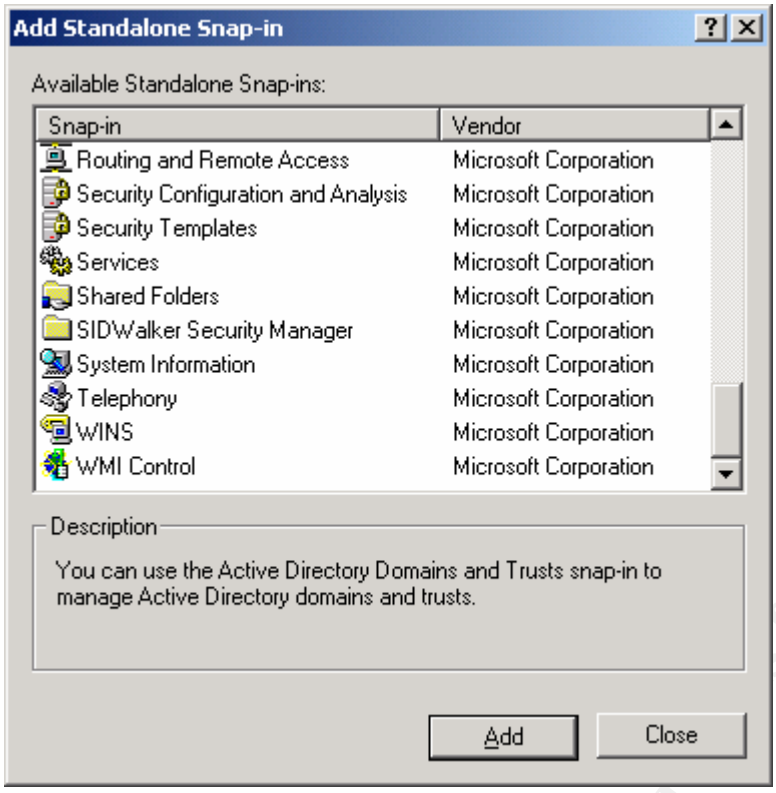
3 Template Security Settings and suggested changes

This template will update a server in a number of important security areas. The following will discuss the areas that will be modified by the template. I have included changes to the template where I feel it falls short for the security requirements of this server. The most important settings will be discussed but not every single file and registry permission setting. The Microsoft Windows 2000 Server Resource Kit [9] has a very good reference help file to understand what each setting does.

To load the Template:

- Logon on to Workstation1 using an account with Administrative privileges
- Install the Windows 2000 Server Resource Kit on the workstation (not the IIS Server as can create security holes)
- Copy the **SECUREINTRANETWEBSERVER.INF** template from the install folder of the resource kit to the C:\Winnt\Security\Templates folder on TrendServer
- Logon on to TrendServer
- Launch the MMC by selecting Start, Run, type MMC, Select OK. An empty Console will be displayed.
- Select Console, Add/Remove Snap-in
- Select Add, a list of Snap-ins will be displayed

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



- Select “Security Templates” and click on Add, then Close, then OK.
- Double click on “Security Templates” in the left pane.
- Double click on “C:\WINNT\Security\Templates” and a list of templates will be displayed.
- Select “secureintranetwebserver”.
- Go through each setting as discussed below. If changes are required, they are listed under the “Recommendation” column. Update the template to match this setting.
- When all the required changes have been made, right mouse click on “secureintranetwebserver” and select save.

One item to note: As a Workgroup has no “Server Operators” by default, you may see the user *S-1-5-32-549 in its place when reviewing the Template on a computer in a workgroup.

Area	***Template setting***	***Recommendation***

3.1 Account Policies

This section deals with account lockout timings and number of logon attempts

3.1.1 Password Policies:

Enforce password history	6	8

Sets the number of passwords that will be remembered so they cannot be reused too often.

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

Maximum password age 60 40
Sets the maximum days a password can be used

Minimum password age 14 1
Set the minimum days a password has to be used before it can be changed

Minimum password length 7 8
Set the minimum number of characters to be used in a password

Passwords must meet complexity requirements Enabled
Requires the use of three out of the four types of characters in the password: upper case letters, lower case letters, numbers and special characters.

Store password using reversible encryption for all users in the domain Enabled Disabled
Only used when for poorly written applications that need to know the users password for authentication. E.g. a low end Remote Access Server.

3.1.2 Account Lockout Policy:

Account lockout duration 30 60
Minutes account is locked if bad attempt threshold is met.

Account lockout threshold 8 5
Number of wrong attempts to lock the account.

Reset account lockout counter after 45 30
Minutes within bad password attempts are counted.

3.2 Kerberos Policy

Kerberos Policy is used to set secure communications between computers in a domain using tickets and encrypted data. This requires Active Directory and Domain Controllers to provide the service of "Key Distribution Center". This does not apply to this "Workgroup" of computers so the "Not defined" setting is okay.

Enforce user logon restrictions Not defined
Maximum lifetime for service ticket Not defined
Maximum lifetime for user ticket Not defined
Maximum lifetime for user ticket renewal Not defined
Maximum tolerance for computer clock synchronization Not defined

3.3 Local Policies

Local policies deal with setting audit settings, User Rights, other security settings.

3.3.1 Audit Policy

Audit account logon events Success, Failure
Logs user log on and log off on servers that provide authentication for other servers like domain controllers. This has not effect on the server.

Audit account management Failure Success, Failure
Logs changes to local users and groups.

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

Audit directory service access Failure
Enables the logging of access of Directory Service objects. This has no effect on servers and workstations in a workgroup.

Audit logon events Success, Failure
Logs user local and network logons and log off.

Audit object access No auditing Success, Failure
Enables tracking of objects that has auditing turned on. Handy if you need to know who is using certain files.

Audit policy change Success, Failure
Logs changes to user rights policies, audit policies, and trusts.

Audit privilege use Failure only
Logs the use of a user using certain user rights.

Audit process tracking No auditing
This setting enables the tracking of detailed program information such as start and end.

Audit system events Success, Failure
Enables the logging of system events like power down/up, restart, or security log changes.

3.3.2 User Rights Assignment

Access this computer from the network Everyone
Sets which groups/users are allowed to connect to this computer of the network. As this server is located on the secure side of a network and it uses a web server to communicate to antivirus client software, the use of "Everyone" is warranted.

Act as part of the operating system Not defined
Process or Services may require the use of a special users right. Adding additional users can make the security worse. It is recommended that services use "LocalSystem"

Add workstations to the domain Administrators
Used to control who can add computer accounts to Active Directory. Only valid for Domain Controllers and not in the this "Workgroup"

Backup files and directories Server Operators
Backup Operators
Administrators
This sets indirect permissions for these users to read and restore all files on the system even though there are no direct rights to do so.

Bypass traverse checking Everyone
This sets groups or users that can traverse folders even though they may not have direct rights in that tree.

Change the system time Administrators
Server Operators
Sets the users and groups that can change the system clock and date.

Create a Pagefile Not defined Administrators
Sets the users and groups that are able to modify the systems pagefile settings.

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

Create a token object Not defined
This sets a user that can be used to create token objects. It is best to leave this as not defined. Process can use LocalSystem if required.

Create permanent shared objects Not defined
Only required for special kernel mode items. LocalSystem already has this right.

Debug programs Administrators
Sets which users have the right to debug a program or process. Debugging, like network sniffing, can reveal sensitive information. Setting this to a high level user like Administrator is recommended.

Deny access to the computer from the network Not defined
Adding users or groups will block their access to this computer over the network even if they are included in the "Access this computer from the network" setting.

Deny logon as a batch job Not defined
Sets which users CANNOT log on as a batch job, even those listed in "Log on as a batch job".

Deny logon as a service Not defined
Used to set which users CANNOT log on as a service, even those listed in "Log on as a service"

Deny logon locally Not defined
Used to set users that CANNOT log on locally, even those listed in "Log on locally". This can be used prevent a certain user from logging on even though they are in the "Administrator" group.

Enable computer and user accounts to be trusted for delegation Not defined
This can be dangerous if this is set to a security level less than Administrator. Allowing a user to set a computer or user to be trusted may allow a process running under that user account to trusted even though it should not.

Force shutdown from a remote system Administrators
Server Operators
This allows only users in these groups to issue a shutdown of the system by using utilities that work over the network.

Generate security Audits Not defined
This allows process running a given user id to add information to the "Security" Event logs. LocalSystem has the right by default.

Increase quotes Administrators
This sets which users are allowed to change CPU quotes of a process (that allow tuning). Good to keep this at a high security level of Administrators.

Increase scheduling priority Administrators
This sets which users are allowed to change CPU priority (through Task Manager) of a process (that allow tuning). Good to keep this at a high security level of Administrators.

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

Load and unload device drivers Administrators
Sets who can load and unload device drivers on the fly. These are often required for Plug and Play drivers. This should be restricted to Administrators.

Lock pages in memory Not defined
This is an obsolete setting and has no effect in Windows 2000.

Logon as a batch job Not defined
Sets which users can be used to run jobs from the task scheduler, other than LocalSystem.

Log on as a service Not defined
Sets which users may change a process into a service.

Log on locally Account Operators, Administrators
Administrators, Backup Operators
Backup Operators, Server Operators
Print Operators,
Server Operators
Sets who can log on to the computer via the console. For this server, I have removed Account Operators and Print Operators from the template, as I do not want them logging on locally.

Manage auditing and security logs Administrators CorpSecurity
This setting has two functions. It determines who can modify a file, folder or registry keys security settings to enable access "Auditing". It also determines who can view and clean out the security event log of the computer. For this paper, I will only allow the Corporate Security group to set auditing and to manage the security event log.

Modify firmware environment values Not defined Administrators
Sets who uses (other than Administrators and LocalSystem) can modify environment variables.

Profile single process Administrators
Set which users (other than Administrators and LocalSystem) can monitor performance of non-system processes.

Profile System performance Not defined
Sets the users (other than Administrators and LocalSystem) that can monitor performance of system processes.

Remove computer from docking stations Not defined
Set which users (other than Administrators, Power users, and users for clean Windows 2000 installs) can remove the computer from the docking station. For this server, we do not care about this setting.

Replace a process level token Not defined
Used to set which users can change a token assigned to a sub process

Restore files and directories Administrators,
Backup Operators,
Server Operators
Used to set which users can a) bypass normal file security and restore files and b) change the owner of an object.

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

Shut down the system	Server Operators, Print Operators, Backup Operators, Administrators, Account Operators	Administrator Server Operator

Sets the users that can perform a shutdown of the system while logged on locally.

Synchronize directory Service data Not defined
Not used.

Take ownership of files or other objects Administrators
This powerful setting declares which users are allowed to take ownership of any object on the server or in AD.

3.3.3 Security Options

Additional restrictions for anonymous connections
Do not allow enumeration of SAM accounts and shares
Change to "No access without explicit anonymous permissions
This requires explicit anonymous permissions to be set on objects for them to be accessed (removes "Everyone" from access to objects).

Allow server operators to schedule tasks Not defined
This setting only applies to Domain Controllers and only affects the AT scheduler, not the Task scheduler.

Allow system to be shut down without having to log on	Not defined	Disabled

Setting this ensures someone that is not allowed to log on locally cannot perform a graceful shutdown of the system. They can still pull the power cord if they can get at it.

Allowed to eject removable NTFS media	Not defined	Administrators

By default, only Administrators have this right. This is fine for this server.

Amount of idle time required before disconnecting session	Not defined	15 minutes

This setting is only valid on computers that are running as servers. The length of time needs to be balanced based on the normal network traffic. Set too long will tie up systems resources.

Audit the access of global system objects Not defined
Enables additional auditing of semaphores, events, and DOS devices.

Audit use of Backup and Restore Privilege Not defined
Tracks additional information in the security event log when Backup and Restore rights are used.

Automatically log off users when logon time expires	Not defined	Enabled

This is a domain-based setting that will disconnect user sessions if time limited use is set in their user settings.

Automatically log off users when logon time expires (local)	Not defined	Enabled

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

This is a local machine based setting that will disconnect user sessions if time limited use is set in their user settings.

Clear virtual memory pagefile when system shuts down Enabled

This setting clears the pagefile so that sensitive information cannot be read if an application rights sensitive information and if someone can get physical access to the system and if someone boots the system using another operating system. I caution that enabling this adds 3 to 10 minutes to the shut down and restart time of the system.

Digitally sign client communication (always) Not defined

Digitally sign client communication (when possible) Not defined Enabled

Digitally sign server communication (always) Not defined

Digitally sign server communication (when possible) Not defined Enabled

These communication settings determine if digital signing of the SMB protocol is to be used all the time or when possible. Setting this to "always" when other computers are not set to either "always" or "when possible" will break communications.

Disable CTRL+ALT+DEL requirement for logon Not defined Disabled

Removes the requirement to press CTRL+ALT+DEL before they logon to the computer. It is more secure to force them to use CTRL+ALT+DEL.

Do not display last user name in logon screen Not defined Enabled

Clears the user name and makes it harder to guess a valid user name.

LAN Manager Authentication Level Send NTLM response only

The setting changes the challenge and response protocol used by network clients. You always want to use the strongest you can. You will be limited by Win 9x clients that may not be able to use NTLM and pre SP4 NT4 computers that cannot use NTLMv2.

Message text for users attempting to log on Not defined "System restricted to authorized users only. System monitoring is in effect."

This will set a pre logon disclaimer message. You can even consult your Corporate Security department or lawyers to fill in a complete "Acceptable Use Policy". Never use the word "Welcome".

Message Title for users attempting to log on Not defined "Warning!"

This is the title banner for the previous message text.

Number of previous logons to cache Not defined 5

This is used for situations when a Domain Controller is not available. Not defined is fine for this server in a workgroup.

Prevent system maintenance of computer account password Not defined

Normally in AD; computer password accounts a changed every 7 days. Setting this to enable will prevent the password change. Not defined is okay for this server.

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

Prevent users from installing printer drivers Not defined Enabled
This setting will prevent normal users from installing printer drivers on this server. This has not effect on Power Users and Administrators. I do not expect normal users to log onto this computer, but I will enable this setting to be sure.

Prompt user to change password before expiration Not defined 5 days
This setting will prompt the user to change the password 5 days before the actual expiry date.

Recover Console: Allow automatic administrative logon Not defined Disabled
Makes using the administrative password required to gain access through the recovery console.

Recovery Console:Allow floppy copy and access to all drives and folders Not defined Disabled
When enabled, this allows use of certain SET commands that affect environment variables in the recovery console and allows use of the floppy drive for copying files.

Rename administrator account Not defined x3d4j5k2
Changes administrator account to this new identity thus making it more difficult for an attacker to break into the system.

Rename Guest account Not defined 3h4i5h6
Changes guest account to this new identity thus making it more difficult for an attacker to break into the system.

Restrict CD-Rom access to locally logged-on user only Enabled
When enabled, a locally logged on user will be the only one that can access the local CD-Rom.

Restrict floppy access to locally logged-on user only Enabled
When enabled, a locally logged on user will be the only one that can access the drive.

Secure channel: Digitally encrypt or sign secure channel data (always) Not defined
Forces secure communication between a computers by requiring either digitally signing or encrypted channels

Secure channel: Digitally encrypt secure channel data (when possible) Enabled
This setting will tell the computer to encrypt the data channel whenever possible.

Secure channel: Digitally sign secure channel data (when possible) Enabled
This setting will tell the computer to digitally sign the data in the channel whenever possible.

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

Secure channel: Require strong (Windows 2000 or later) session key Not defined
Sets the computer to use a strong session key for data encryption.

Secure system partition (for RISC) Not defined
With this set, you must have administrative rights to access the System FAT partition on a RISC computer. Not needed for this server.

Send unencrypted password to connect to third-party SMB servers Not defined Disabled
Some third party SMB interfaces allow the use of unencrypted passwords which is dangerous. This should be disabled and you should avoid using third party SMB servers that allow clear text passwords.

Shut down system immediately if unable to log security audits Not defined Enabled
This system will be monitored by a log watch utility that will clean out the logs with every check. If for some reason the log files are tampered with, or the log watch utility stops, I would rather have this server stop than to run for days without logging the security information.

Smart card removal behavior Not defined Lock Workstation
This item sets the computers action when a smart card is disconnected while a user is logged on. Lock workstation will allow the user to keep any fore ground applications running while protecting their session.

Strengthen default permissions of global system objects (e.g. Symbolic links) Not defined Enabled
This setting will change access to shared system resources so that non-admin users are able to read them but not modify them. They will be able to still modify the ones they created.

Unsigned driver installation behavior Not defined Warn, but allow
This item sets what will happen when an attempt is made to install an unqualified driver.

Unsigned non-driver installation behavior Not defined Warn, but allow
This item sets what will happen when an attempt is made to install an unqualified non-device driver on the system.

3.4 Event Log

Event log settings deal with log size, rotation and access

Maximum application log size	6144	
Maximum security log size	6144	19968
Maximum system log size	6144	
Restrict guest access to application log	Enabled	
Restrict guest access to security log	Enabled	
Restrict guest access to system log	Enabled	
Retain application log	Not defined	
Retain security log	Not defined	
Retain system log	Not defined	
Retention method for application log	As needed	

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

Retention method for security log	Manually	
Retention method for system log	As needed	
Shut down the computer when the Security audit log is full	Not defined	Enabled

(This can be used as a denial of service attack. In this case, there is monitoring and paging software that will alert within a few minutes if this server goes down.)

3.5 Restricted Groups

Restricted groups are used to control membership in groups. This is accomplished by pre-determining the membership by using "Members" and "Members of". As this section is designed for domains, OUs and sites, it is not applicable for local computer policy even though it shows in the template.

3.6 System Services

System Services are used to control services by disabling ones that are a risk and setting permission rights to them.
The template provide by Microsoft provides no changes to the services. I suggest a few be set for this server and save them in the template:

Messenger	Not defined	Disabled
MSFtpSVC (Ftp Service)	Not defined	Disabled
Internet connection sharing	Not defined	Disabled
Infrared Monitor	Not defined	Disabled
NetMeeting Remote Desktop Sharing	Not defined	Disabled
Print Spooler	Not defined	Disabled
Remote Access Auto Connection Mgr	Not defined	Disabled
Remote Access Connection Mgr	Not defined	Disabled
Remote Registry	Not defined	Disabled
Task Scheduler	Not defined	Disabled
Telnet	Not defined	Disabled
Routing and Remote Access	Not defined	Disabled
Simple Mail Transport Protocol	Not defined	Disabled

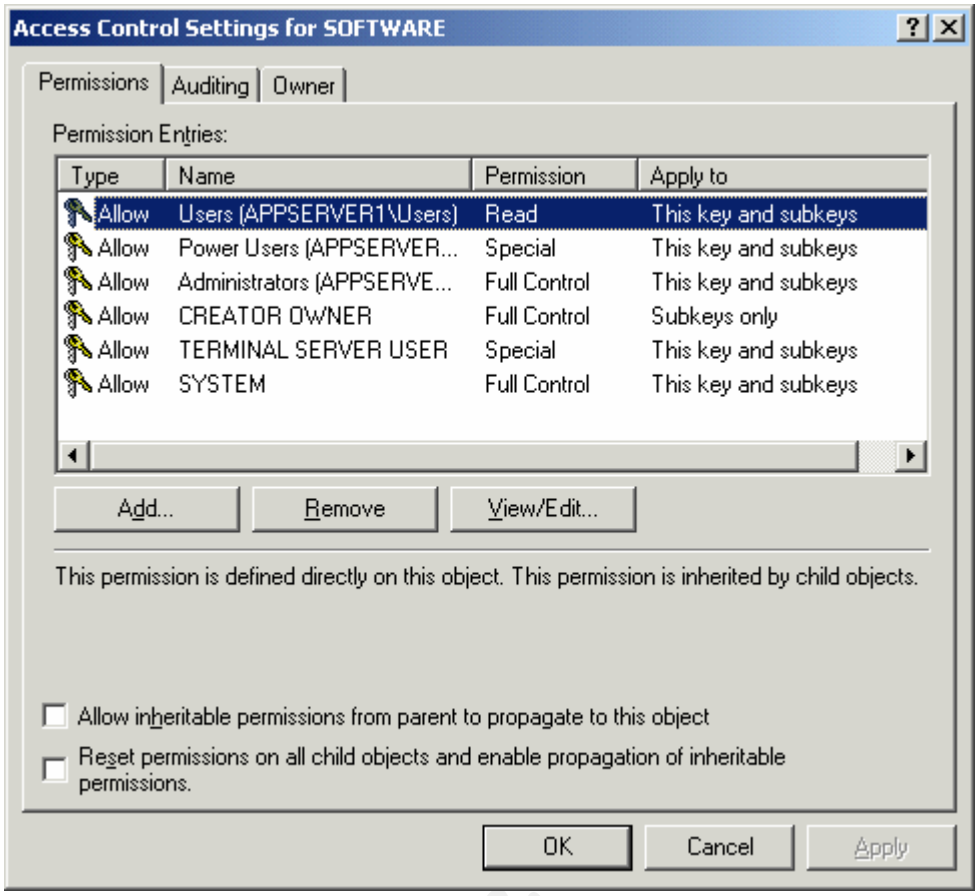
3.7 Registry

Registry settings in the template are used to set access permissions and/or access auditing for keys in the registry. The principle is to reduce the access to only those users that require the access. You can also enable auditing on registry keys and subkeys. Making changes through the template is like launching Regedt32 and modifying the "Security" permissions. To view the security of Hkey_Local_Machine, Start, Run, Regedt32. Select the Software Key, and then select Security, Permissions, and Advanced. In this case, the setup security is:

- The Users group has Read rights on this key and subkeys
- The Power Users group has Special rights on this key and subkeys
- The Administrators group has Full Control rights on this key and subkeys
- The Creator Owner group has Full Control rights on this key and subkeys

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

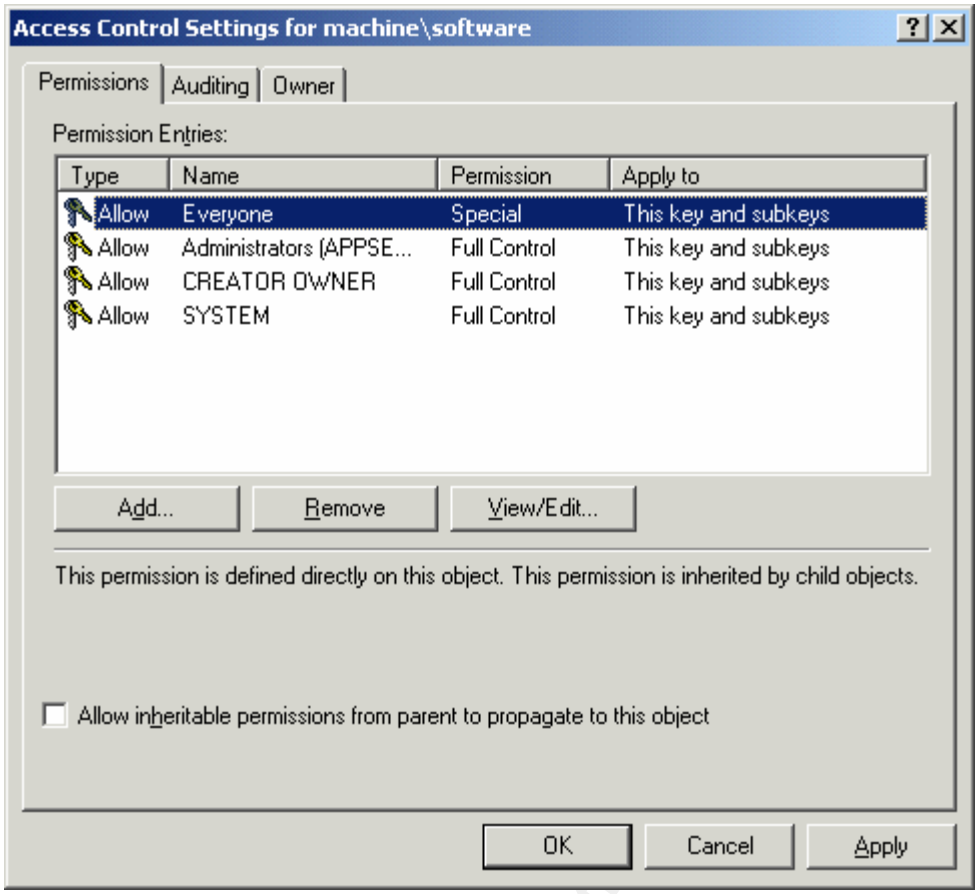
- The Terminal Server User has Special rights on this key and subkeys
- The System group has Full Control rights on this key and subkeys



Lets have a look at the template to see if this portion is usable. In the Security Templates MMC, Double click on Machine\System. You will see that options set for Configure this key then, Replace existing permissions on all subkeys with inheritable permissions. Click on Edit Security. You will now see users and groups with their access permissions. Click on Advanced. In this case, the template will set:

- The Administrators group to have Full Control rights on this key and subkeys
- The Creator Owner group to have Full Control rights on this key and subkeys
- The Everyone group to have Read, Execute, Write, and Delete rights on this key and subkeys
- The System group to have Full Control rights on this key and subkeys

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



As this template sets the Everyone group with Change rights on many registry keys, the template is worse than the original security of the computer. It is possible that this template is from an NT 4.0. For TrendServer, we will use the security, as it was setup. This is accomplished by pressing Ctrl-A to select all the registry keys in the right pane, then pressing the delete key and clicking on Yes to confirm delete.

3.8 File System

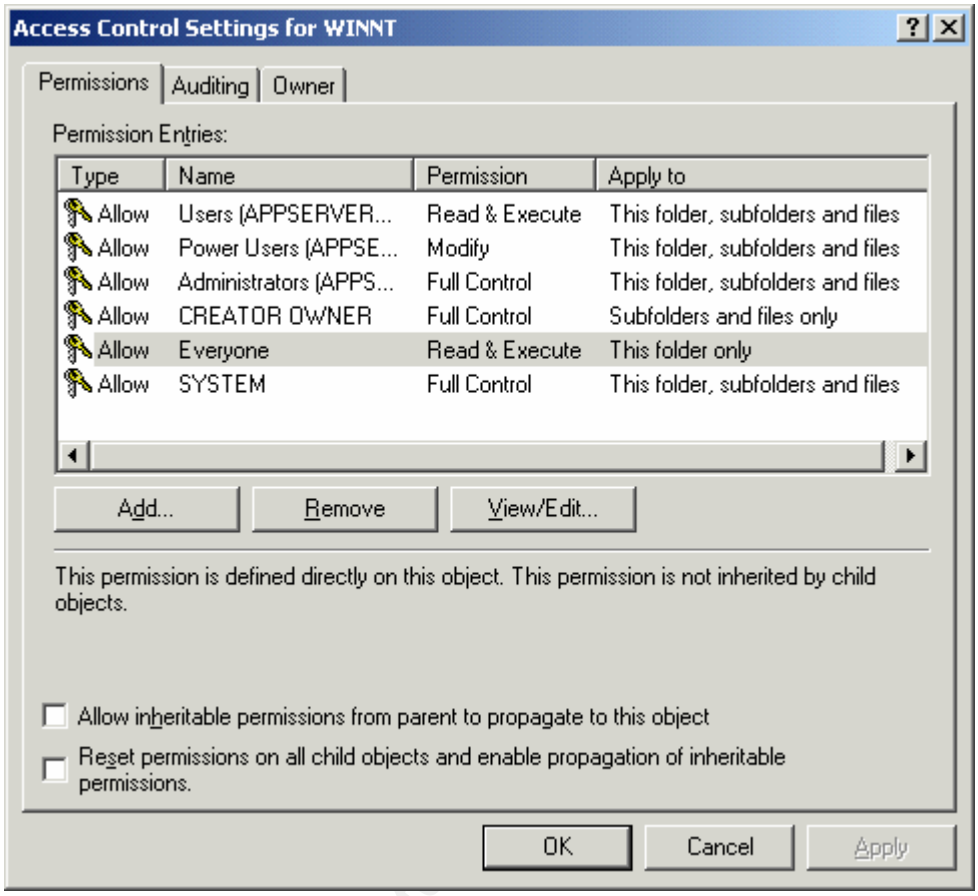
File system settings in the template are used to set access permissions and/or set access auditing of files and folders on the system. As there can be thousands of files on the system, you can get very granular with settings. We will have a look at the settings in the template to see it they would make the computer more or less secure.

Check the current setting of the computer by clicking on My Computer, browsing to the C: drive, right mouse clicking on the folder C:\Winnt, select Properties, Security, then Advanced. You will see:

- The Users group has Read & Execute rights on this folder, subfolders, and files
- The Power Users group has Modify rights on this folder, subfolders, and files

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

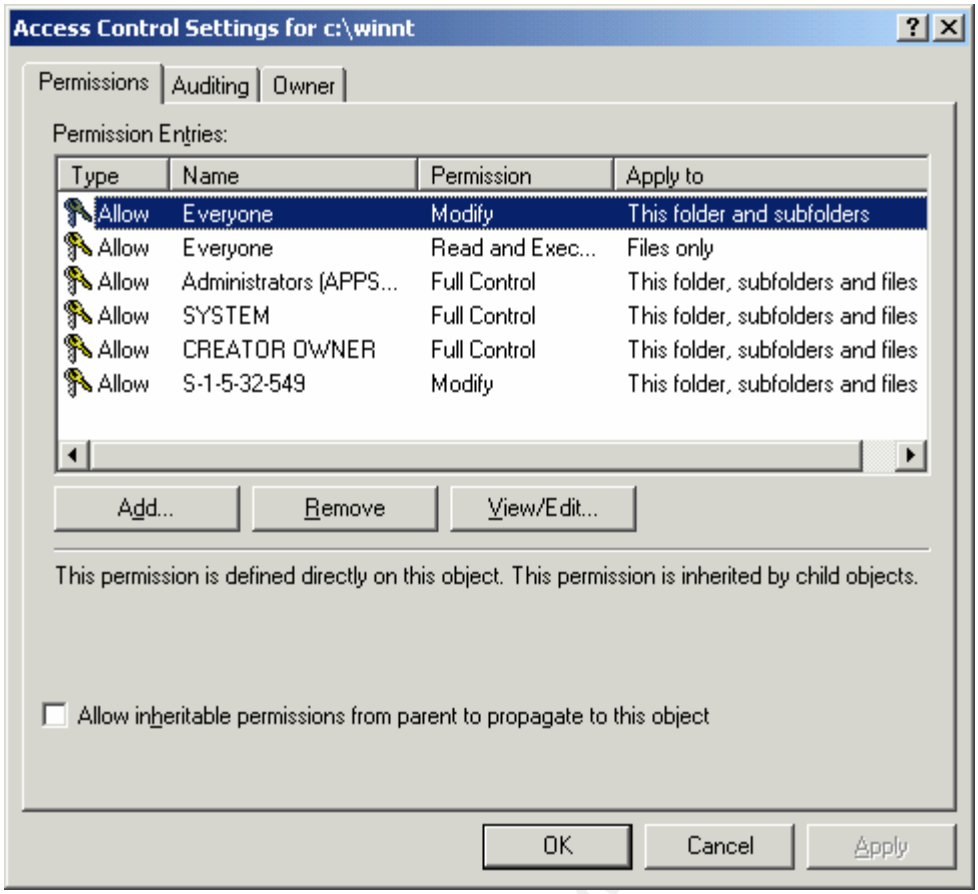
- The Administrators group has Full Control rights on this folder, subfolders, and files
- The Creator Owner has Full Control rights on subfolders and files only
- The Everyone group has Read and Execute rights on this folder only
- The System has Full Control rights on this folder, subfolders and files



Now, lets have a look at the proposed security of the same folder in the Template.

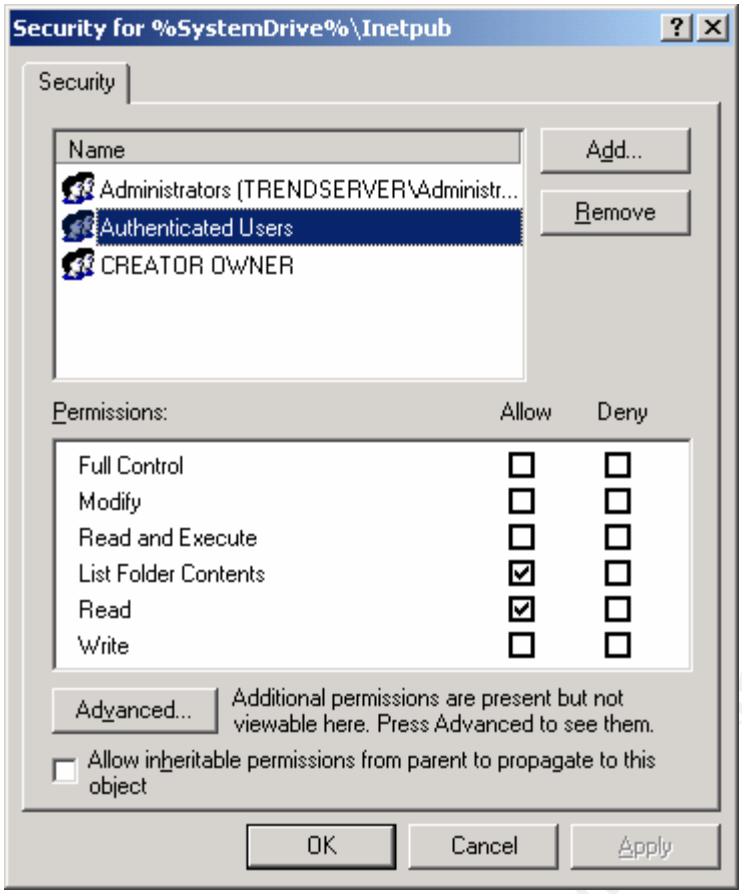
- The group Everyone to have Modify rights on this folder and subfolders
- The group Everyone to have Read and Execute rights on files only
- The Administrators group to have Full Control rights on this folder, subfolders, and files
- The System to have Full Control rights on this folder, subfolders and files
- The Creator Owner to have Full Control rights on this folder, subfolders and files
- The group S-1-5-32-549 (also known as Builtin\Server Operators) to have Modify rights on this folder, subfolders, and files.

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



Granting the Everyone Group Modify rights to this folder and subfolders is not a good idea. A check of the security settings in the template on other files and folders show a similar trend. Therefore, for TrendServer, we will modify the template, as the servers setup permissions are better than those in the template are. First, select the first file in the list so it is highlighted. Next, scroll down the bottom of the list and press the Ctrl button as you select the last file name. Press Delete and Yes to confirm. We need to add the C:\Inetpub folder by right mouse clicking on the open are of the file display area, Add File, browse to C:\Inetpub\ and click Ok. This will display a security window for %SystemDrive%Inetpub. Click on Add, select the Authenticated Users group, click Add, then select the Creator Owner group, then Add, and finally the Administrator group and Add. Click on OK. Change the Permissions so that Administrators and Creator Owner have Full Control, Authenticated Users have List Folder Contents and Read. Then select the Everyone group and click on Delete. Unselect the option for "Allow inheritable permissions from parent to propagate to this object". Click on OK. Verify the setting "Propagate inheritable permissions to all subfolders and files" is selected. Click on OK.

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



For the OfficeScan virtual web site share on D: drive, we will leave the permissions alone as they were modified by the Trend software installation.

4 Steps to perform before applying the Template

4.1 Change Management

As with any change to systems in production, a professional should follow the "Change Management" practices for your company. If your company does not have a process, it is suggested you work to implement one. A Change Management process should include the following high-level steps:

- Scheduling the change during a proper maintenance window
- Advance notice of the change to the system business owner
- Proper approval for the change by the system business owner
- Advance notice of the change to the end users of the system(s)
- Advance notice of the change to other technical support staff
- Planning and performing the proper precautions before the change
  - backing up any specific application data
  - backing up the operating system partition
  - backing up the system state
- Verifying the backup(s) to ensure backup integrity

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

- Defining and performing a series of tests to confirm the changes had the affect you planned
- A back out plan if events do not happen as planned.

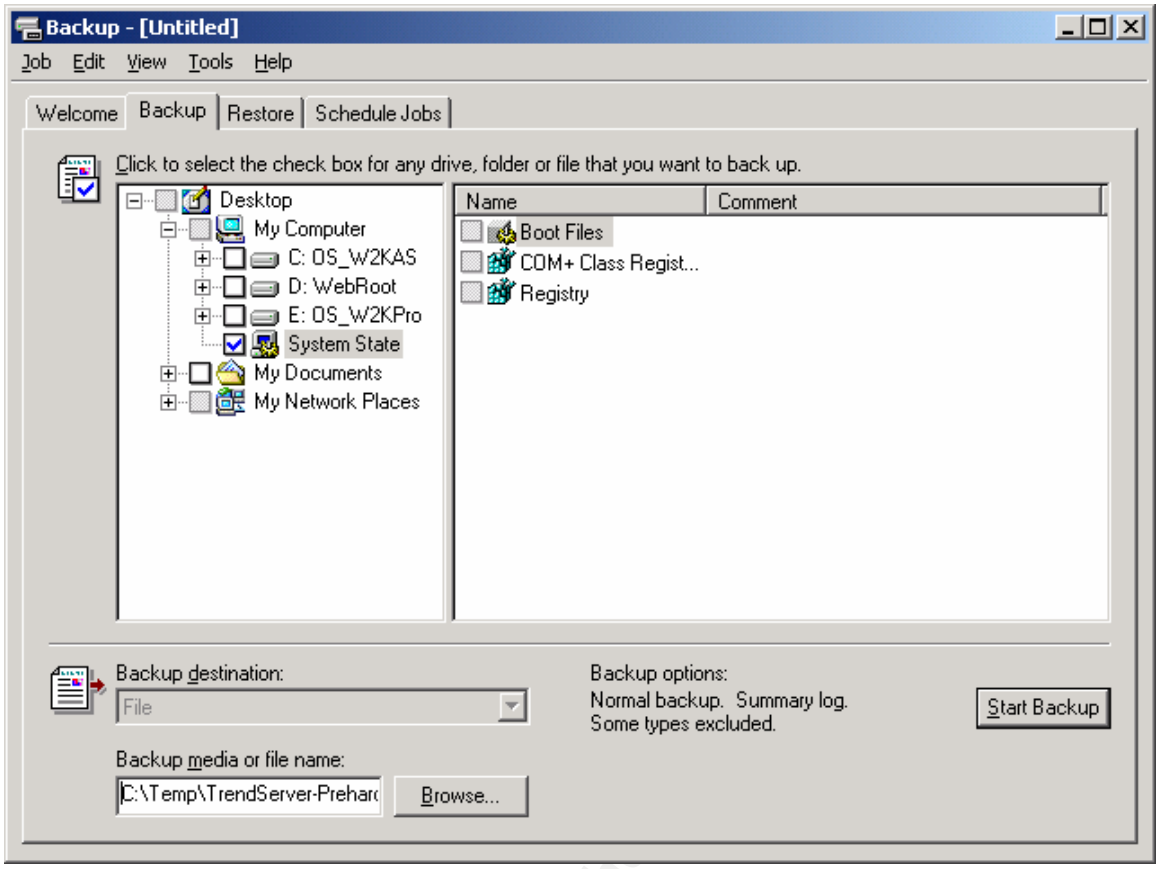
4.2 Back up before making changes

Before applying this template, we will perform three different backups. The first step is to backup the web server's metabase up by using the IIS MMC snap-in. In the MMC, select the computer name; right mouse click, select Action, Backup/Restore Configuration, and then select Create Backup. Secondly, the "System State" will be backed up by launching Programs, Accessories, System Tools, and Backup. The following dialog box will be displayed.

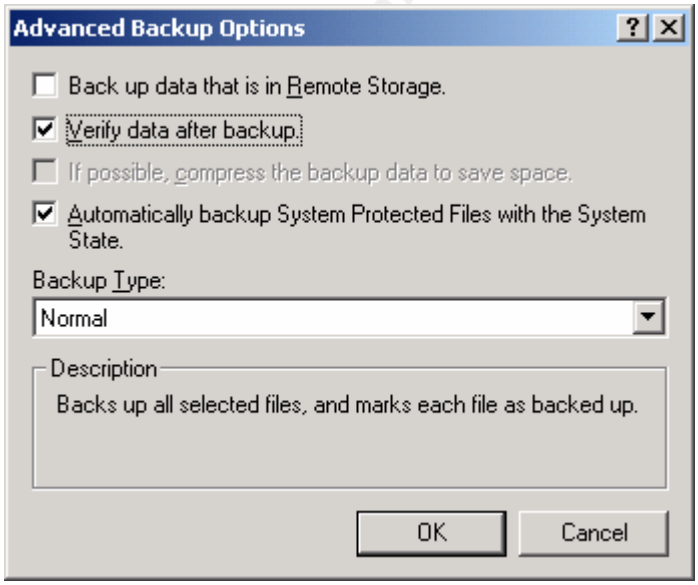


- Choose the Emergency Repair Disk.
- Confirm "System State" is selected

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



- Click on Browse. Select a file name that makes sense e.g. "TrendServer-PreHardening" and Select the C:\Temp folder (or another secure folder that will be backed up
- Click on “Start Backup”
- Another dialog box appears
- Click on Advanced



- Select "Verify the data after backup"

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

- Click on OK
- Click on Start Backup.
- The Backup will proceed with a time estimate.
- Once the backup is complete, confirm the Status shows “Completed”.
- Click on Close and then Exit Backup.
- Copy the file off the Server to another secure location.

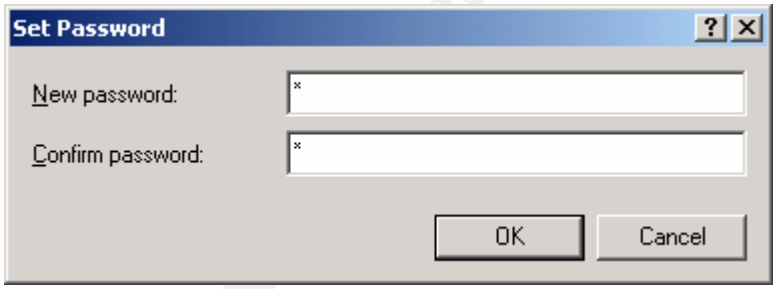
The last step for the backup will be to perform a full system backup using Arcserve 2000 from Computer Associates. This backup will pickup the files created from the previous two steps, all of the Operating system partitions as well as all the application data for OfficeScan and Server Protect. The backup is launched by using the Arcserve 2000 console (instructions are not included to save space in this document).

4.3 Pre Hardening Benchmarks

Before the template is applied, a few system and application checks will be run against the server. The results will be saved. The same checks will be run against the server after the template has been installed. The results of these tests will be discussed.

4.3.1 Pre System Test #1 - Account Password check

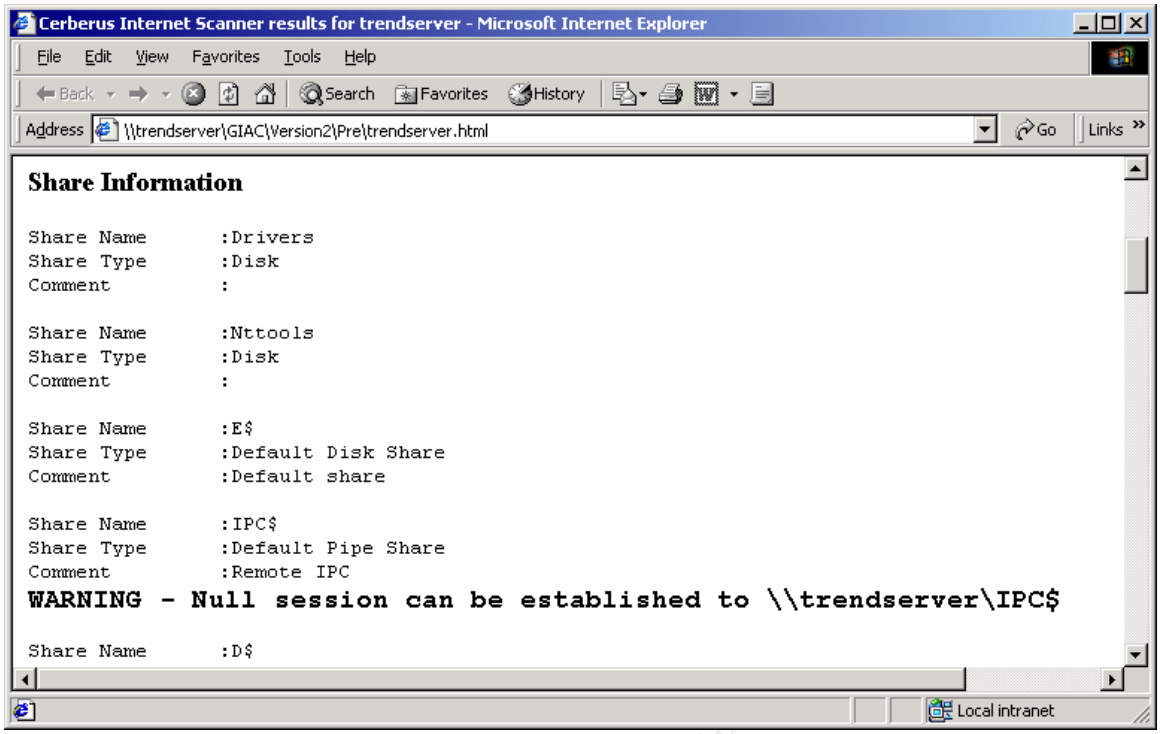
Open the Computer Management MMC and select Users under Users and Groups. Using a test user account called TestUser, right mouse click and select “Change Password”. Enter the letter “x” on the “New password” and on the “Confirm password” lines and then click OK. The one character password is accepted.



4.3.2 Pre System Test #2 - Null session check

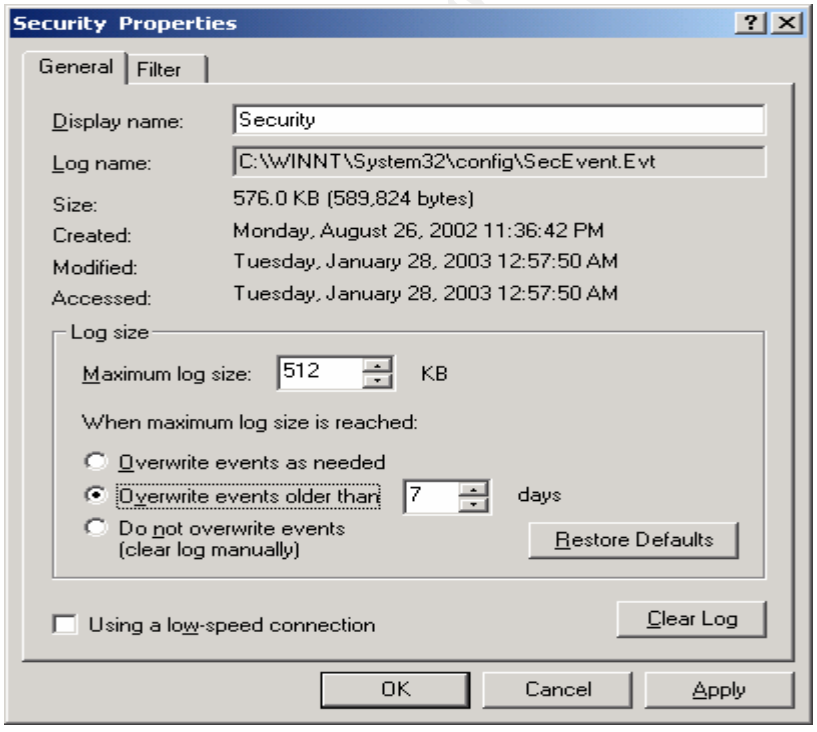
On Workstation1, download NBTDUMP.EXE [10] into C:\Temp. Open a Dos window. CD \Temp. Type in “nbtdump trendserver”. This tool attempts to connect to the server using the IPC$ channel (null session). This tool saves the results to an HTML file named the same as trendserver. Information about the server’s shared folders and users is displayed. Hackers would use this information to perform reconnaissance on a windows host.

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



4.3.3 Pre System Test #3 - Security log check

Launch the Computer Management MMC, view the event logs, right mouse click on Security log and select properties. You will see the default setting of a size of 512 KB and set to overwrite events over than 7 days. You are allowed to view records in the log file.



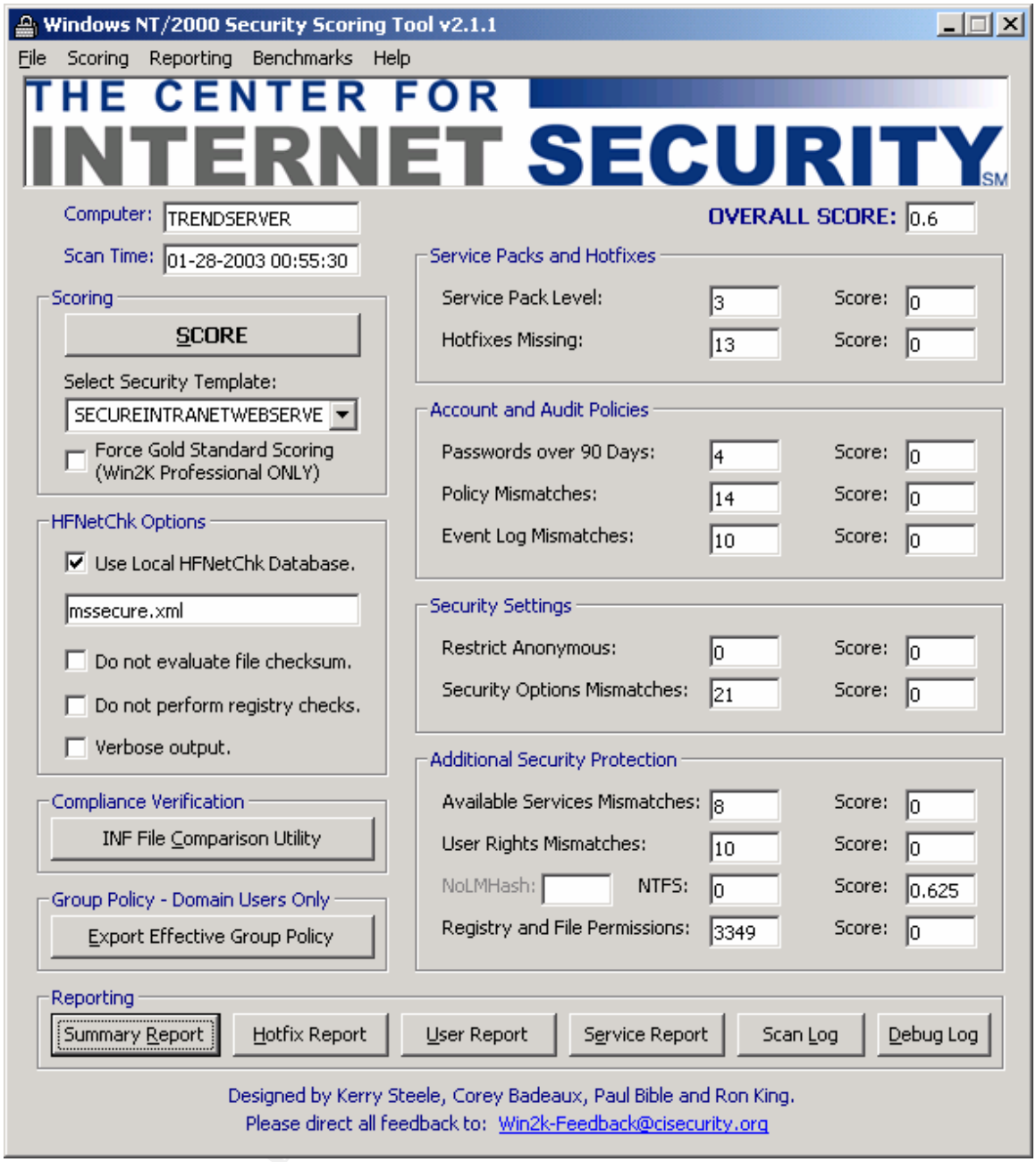
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.3.4 Pre System Test #4 - CIS Windows NT/2000 Security Scoring Tool

This test will be performed using the Windows NT/2000 Security Scoring Tool [11] from the Center for Internet Security This powerful tool is downloaded from www.CISecurity.org and installed on "TrendServer". The version of the tool is 2.1.1. The version of the mssecure.xml database used for the test was the version current as of January 11, 2003. Before launching the tool, copy the file customized SECUREINTRANETWEBSERVER.INF from the C:\Winnt\Security\Templates folder, to C:\Program Files\CIS\Templates folder. When the tool is launched, it defaults to using the "Force Gold Standard Scoring" option turn on. This option must be unchecked, then use the pull down used to select proper template for the test, SECUREINTRANETWEBSERVER.INF. The SCORE button is pressed and various checks are performed. The results are displayed as shown below. In this case, the score was a low of .6 out of 10. This low score is due to the large number of setting mismatches between the Servers actual settings and the settings in the Template. You can click on the Reporting buttons to view more information. The good news is this low score is easy to fix.

© SANS Institute 2003, Author retains full rights.

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



4.3.5 Pre System Test #5 - Web Server Vulnerability Assessment

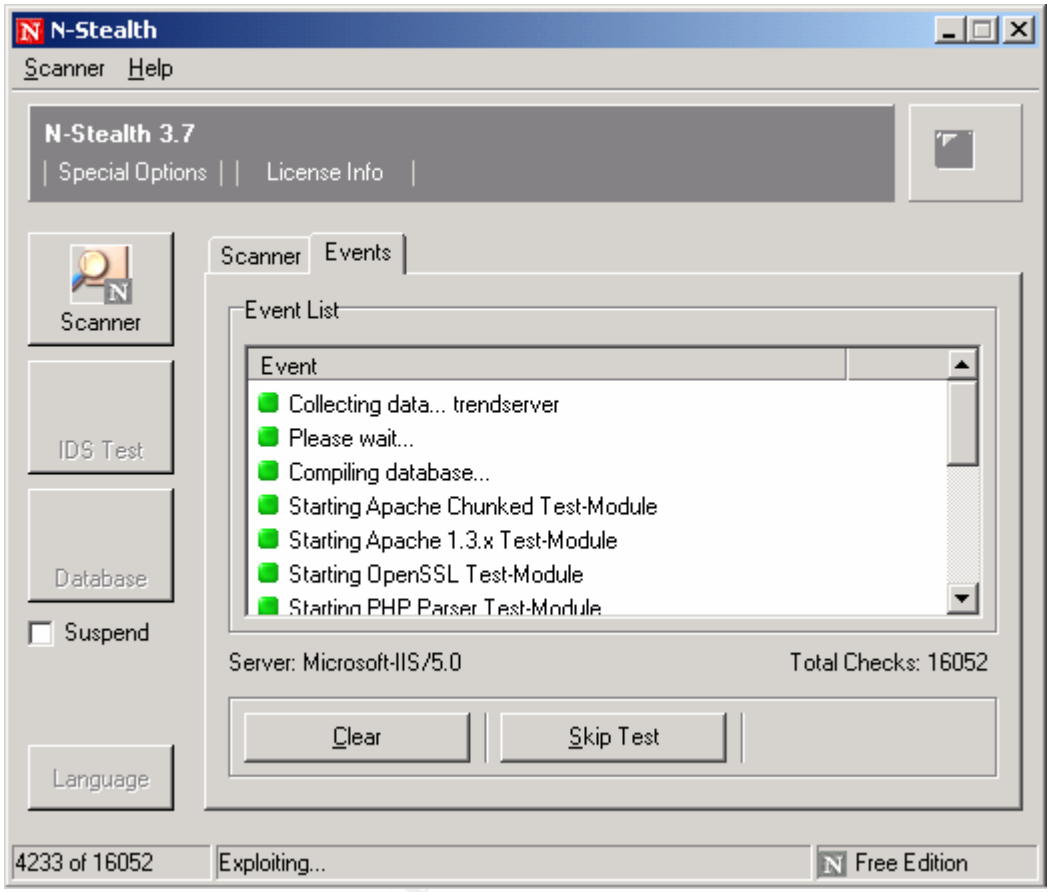
N-Stalker makes a free version of its N-Stealth [12] web server vulnerability assessment tool. This tool will perform a series of tests on a web server and report on vulnerabilities.

- Download and install N-Stealth
- Launch N-Stealth
- Select language and click on OK
- Click on “Scan Rule”
- Select complete scan
- A warning dialog box appears

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

- Click on OK
- Type in the server name in the host address field. In this case, Trendserver
- Click on “Perform Scan”

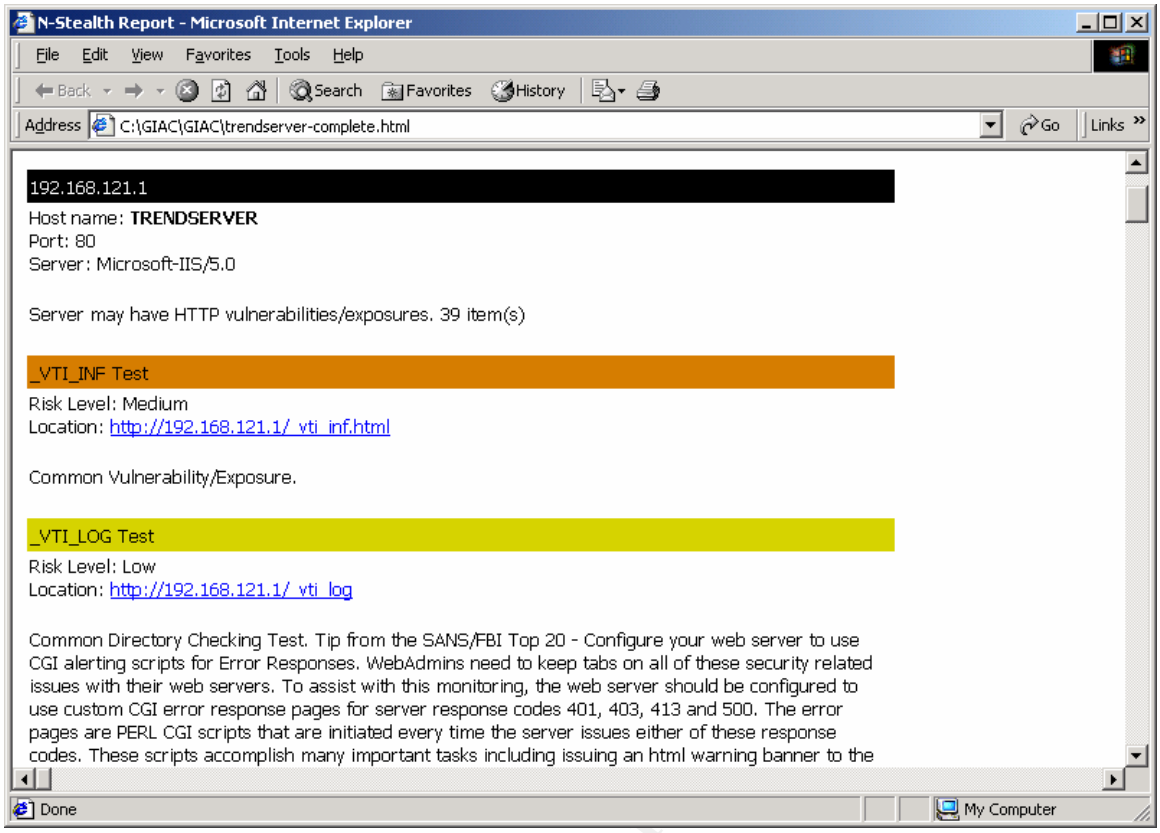
Vulnerability checks will be performed



- When the scan is complete, you will be prompted for a file name e.g. Trendserver
- Click on “Location” to view the possible vulnerabilities
- You can also open the saved file to review the possible vulnerabilities

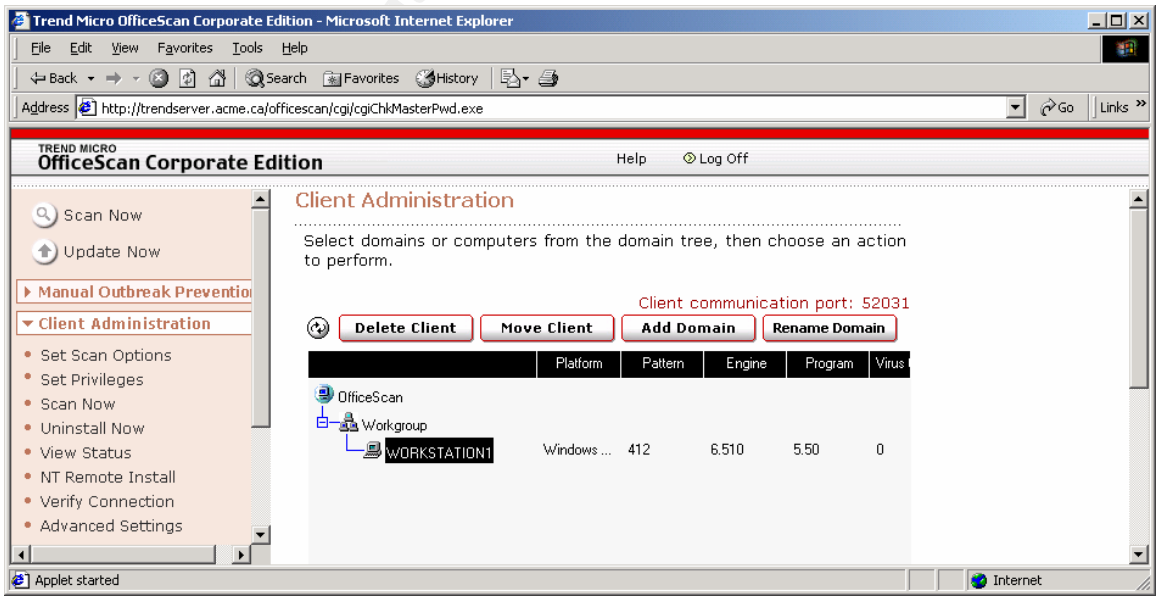
In this case, there were 39 possible vulnerabilities found. These are exposures based on responses to certain probes. The Server is reporting information that a hacker can use to find an exploit. The two shown in the screen shot are vulnerabilities from Front Page Server Extensions.

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



4.3.6 Pre Application Test #1 – OfficeScan – Manage the Console

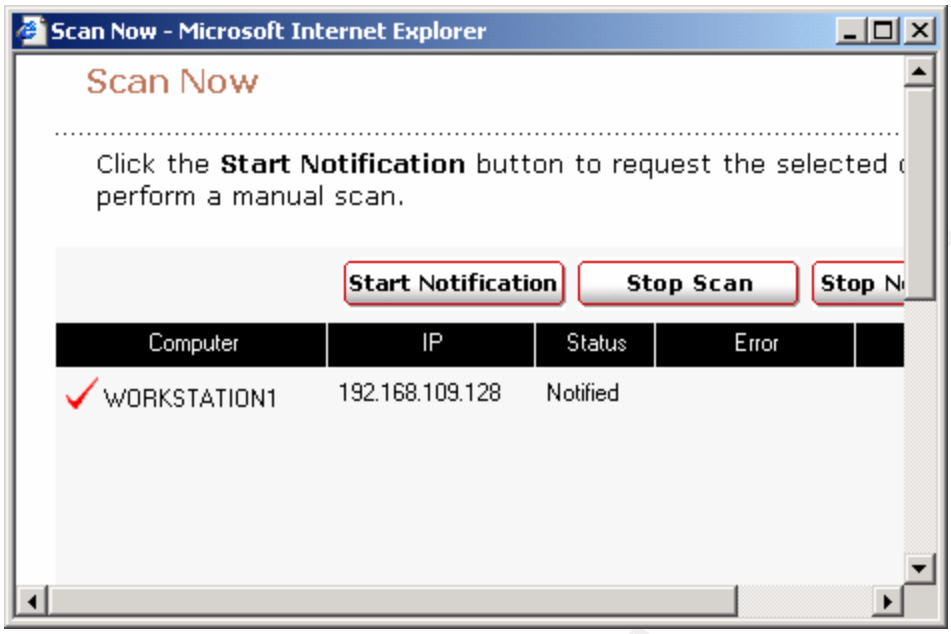
From Workstation1, IE is started and the URL for the management console on Trendserver is loaded http://trendserver.acme.ca/officescan. The logon screen is presented. Once the password is entered, Client Administration is selected and "Workgroup" is seen with "Workstation1" in it. If the console cannot communication with a client, the icon is changed to one that has the word OFF in it. This test passes as the active client is shown active and connected.



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

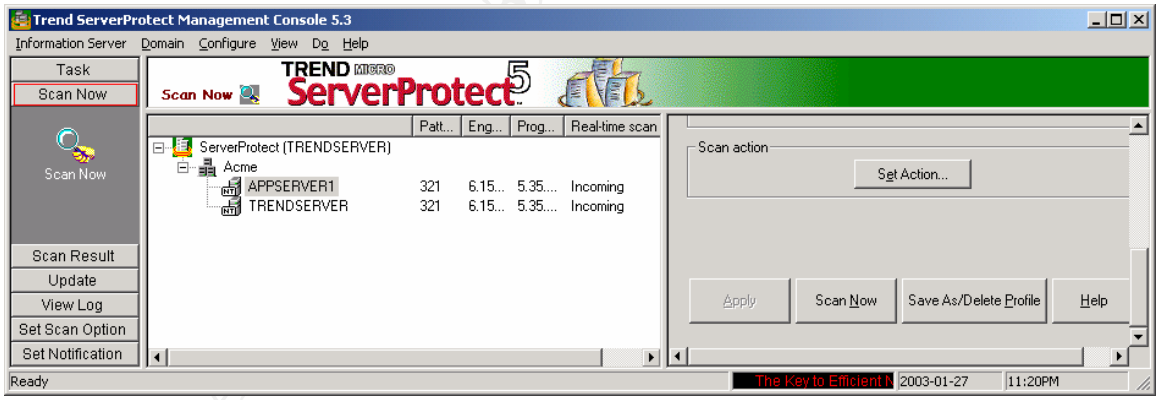
4.3.7 Pre Application Test #2 – OfficeScan – Force Client manual scan

This test is accomplished by clicking on “Scan Now”. Worksation1 is selected and then click on “Start Notification”



4.3.8 Pre Application Test #3 – Server Protect – Manage the Console

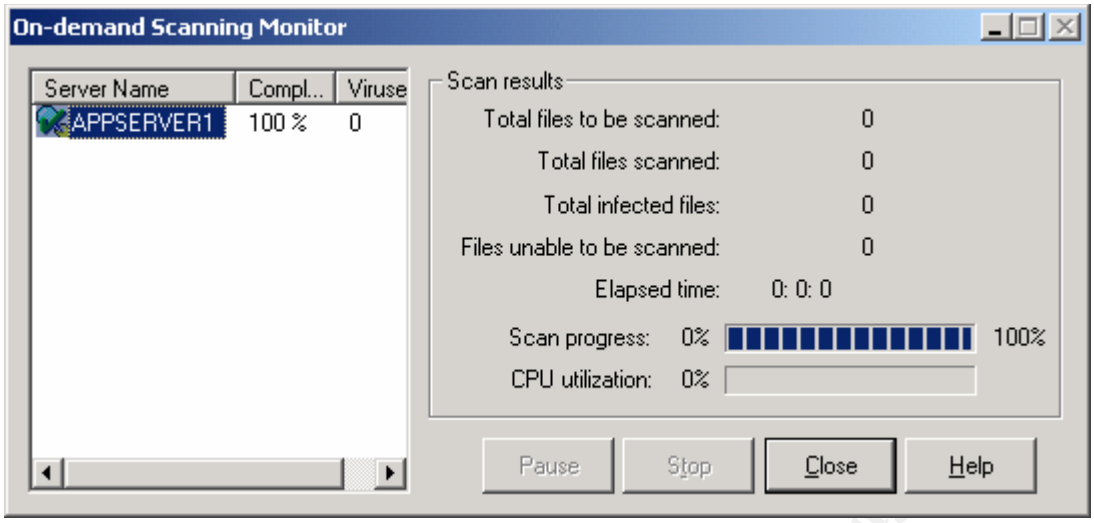
The console is started on Workstation1 by Start/Program Files/Trend Server Protect, ServerProtect Management Console. The console password is entered.



4.3.9 Pre Application Test #4 – Server Protect – Force Client manual scan

This is tested by selecting the server AppServer1, clicking on Scan Now on the left side of the console, then clicking on Scan Now on the right side of the console. This launches a scan of the server. The status is seen in the “On-demand Scanning Monitor”.

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



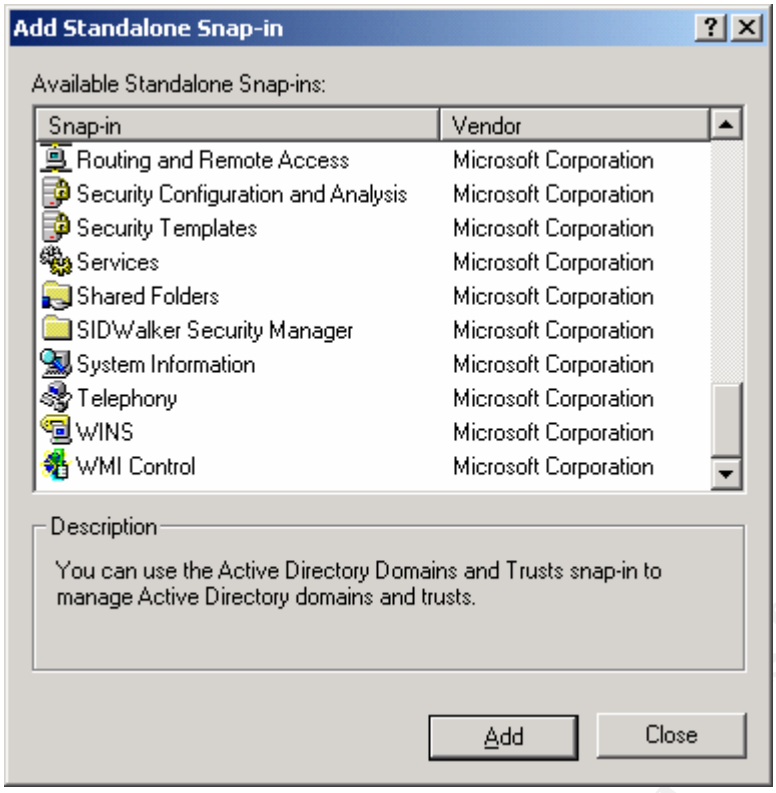
5 Steps to install the template

They're a few ways to apply hardening security templates on Windows servers. With Windows NT 4.0 Systems, either the Security Configuration Manager for the MMC or the command line tool SECEDIT.EXE can be used. These are available from the Microsoft web site. With Windows 2000 Server systems, you have a few more choices. For standalone servers, the command line tool SECEDIT.EXE, or the Security Configuration and Analysis snap in for the MMC can be used. For Domain Controllers and Member Servers in an Active Directory Forest, SECEDIT.EXE, the Security Configuration and Analysis snap in for the MMC, or GPO – Group Policy Objects can be used.

For this paper, the Security Configuration and Analysis snap in for the MMC will be used to apply the Security Template on the Server. This is loaded by performing the following steps:

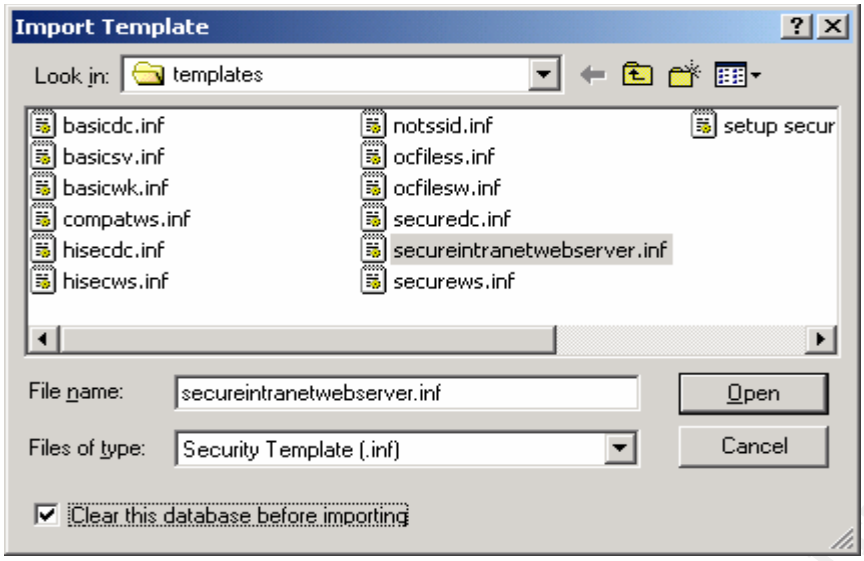
- Logon on the server using an account with Administrative privileges
- Launch the MMC by selecting Start, Run, type MMC, Select OK. An empty Console will be displayed.
- Select Console, Add/Remove Snap-in
- Select Add, a list of Snap-ins will be displayed

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



- Select “Security Configuration and Analysis” and click on Add, then Close, then OK.
- Select “Security Configuration on the left pane.
- Right mouse click and select “Open Database”
- Select a name for the database that makes sense. In this case, we will use SecureIntranetWeb, and then click Open.
- The next screen that pops up is to “Import Template”. Select the “SecureIntranetWebServer.INF” file
- Select “Clear this database before importing”
- Click Open.

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



5.1 Apply the template to the server

To apply the settings, right mouse click on Security Configuration and Analysis and select “Configure Computer Now”. You will be prompted for a log file location. Click OK. The security settings in the template will be applied to the server. This may take a few minutes. Close the console when it is finished.

5.2 Harden the IIS Server

As this Web server is not on the Internet, we will not go crazy in locking it down. We will perform a few steps to make it more secure. Note: It is usually best to use the IIS Lockdown tool to harden an IIS Server. According to Trend, it may work [13]. My experience to date with OfficeScan Management servers is that OfficeScan does not always work properly after using the Lockdown tool. I have provided a list of steps that hardens the IIS Server to a reasonable degree but does not break OfficeScan.

5.2.1 Remove unneeded Web components

In the Add/Remove Programs console, under Internet Information Services (IIS) uncheck all the subcomponents except World Wide Web Server, Common Files, and Internet Information Services Snap-In.

5.2.2 Delete unneeded virtual directories

Microsoft includes a number of help and script sample files for web server developers. These files can be used to gain information about the server. Delete these virtual mappings (if they exist) using the Internet Information Services MMC:
Scripts
IISHelp
IISSamples
_vti_bin
_private
_vti_cnf
_vti_log

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

_vti_pvt
_vti_script
_vti_txt
postinfo.html
_vti_inf.html

5.2.3 Delete unneeded and sample files

Microsoft includes a number of help and script sample files for web server developers. These files can be used to gain information about the server. Files in these folders should be deleted from the hard drive (if they exist):
\inetpub\AdminScripts
\inetpub\iissamples\
\Program Files\Common Files\msadc\Samples\
%SystemRoot%\help\iishelp\
%SystemRoot%\System32\Inetsrv\iisadmpwd\

Also, remove these Front Page files and folders if they exist
\inetpub\wwwroot_vti_inf.html
\inetpub\wwwroot\postinfo.html
\inetpub\wwwroot_private
\inetpub\wwwroot_vti_bin
\inetpub\wwwroot_vti_pvt
\inetpub\wwwroot_vti_log
\inetpub\wwwroot_vti_txt
\inetpub\wwwroot_vti_cnf
\inetpub\wwwroot_vti_script

5.2.4 Disable Internet printing

Internet printing is available on IIS 5.0. As this server will not be sharing any printers. We will disable this feature.

1. Use Regedit to edit the registry key:
   HKLM\Software\Policies\Microsoft\Windows NT\Printers\DisableWebPrinting
   Value name: DiableWebPrinting
   Value type REG_DWORD
   Change the value to 0x1

2. Remove the /printers virtual from the web server site(s)

3. Delete the files in %SystemRoot%\web\printers\

4. Un-register the web printer dll by opening a Command Prompt, CD to C:\Winnt\System32. Enter the command REGSVR32 MSW3PRT.DLL /U.

5.2.5 Disable Parent paths

This is done by using the launching the IIS Management MMC Snap in. Select each web site, right mouse click to select properties, select the Home Directory

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

Tab, select the Configuration button, select the App Options tab, un-check "Enable Parent Paths". Ok

5.2.6 Enable Web logging

As a number of hack attempts come from the inside of the network, be sure to turn on web logging so we can monitor what the web server is seeing. This is accomplished by viewing the properties of the Default web site, select the Web Site tab, and verify "Enable Logging" is enabled, set Active Log format to W3C Extended Log file Format. Click on Properties; enable "Use Local Time for file naming and rollover. Then the select the Extended Properties tab. Enable the following:

Date, Time, Client IP Address, User Name, Server IP Address, Server Port, Method, URI Stem, URI Query, Protocol Status, Win32 Status, User Agent

Click on Apply and OK, OK. The log files are stored by default in the %Windir%\System32\Logfiles folder. This is fine for this server.

5.2.7 Install URLSCAN.DLL ISAPI Filter

Microsoft provides a free ISAPI filter that can be configured to prevent bad network traffic from getting to the web server. When you install this filter, you modify the URLSCAN.INI file in the C:\Winnt\System32\inetsrv\urlscan folder. A few changes are required to allow the OfficeScan Management Console to continue to work [14] . A working version of URLSCAN.INI has been added to the end of this document. The filter is added to the default web site by selecting its properties in the Internet Information Services MMC, selecting the ISAPI Filters tab, clicking on ADD, adding a descriptive Filter Name, e.g. OfficeScan, browsing for URLSCAN.DLL in the C:\Winnt\System32\Inetsrv\urlscan folder. An added benefit of this filter is that any web requests rejected by the filter are logged to the same log as the Web site with the entry of <Rejected-By-UrlScan>. This will allow you to setup a log monitoring system that will also be able to report on suspect traffic.

5.2.8 Lock down Console file permissions

This step is required to modify the file permissions on certain management file. There was a vulnerability in earlier version of OfficeScan were a user could put in a full path to certain CGI files and can limited access without having to use the console password. This vulnerability has been fixed as the console now tracks sessions better. This step will improve security one step better by removing the user IUSR_TRENDSERVER read access to certain files in the CGI folder. See the Trend Knowledge base article 13353 [15] for more information.

1. On the server, open Windows Explorer, and go to the `\PCCSRV\Admin\Utility\CGI_NTFS` folder of OfficeScan.

2. Copy `CGI_NTFS.exe`, `CGI_NTFS.txt`, and `CGI_NTFS.ini` to the `\PCCSRV\Web\CGI` folder.

3. Open a command prompt, and then go to the `\PCCSRV\Web\CGI` folder of OfficeScan.

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

4. Type `cgi_ntfs.exe`, and then press ENTER. A confirmation message appears.

5. Type "Y", and then press ENTER. `CGI_NTFS` modifies the CGI permissions.

6. The next time you try to open the Web console, you will be prompted for your user name and password. Use an account that has administrator privileges to the server. Users with IUSR_XXX privileges only will not be able to open the Web console.

Note: Delete `CGI_NTFS.exe`, `CGI_NTFS.txt`, and `CGI_NTFS.ini` from the `\PCCSRV\Web\CGI` folder of OfficeScan when you finish running `CGI_NTFS`.

Reboot the server for all the changes to take affect.

6 Test the Systems Functionality

Power up the Server and confirm you are able to log in. The first thing you will notice that the logon account name has been cleared. Check the event logs for system and application for errors (services that no longer work).

6.1 Post System Test #1 - Account Password check

As before, open the Computer Management Console and select “TestUser”. Right mouse click on the user and select Change Password. Enter the letter “x” on the “New password” and the “Confirm password” lines and then click OK. The password will not be accepted, as it does not contain enough characters. Try again with a password of abcdefg1. This password will again be rejected, as it does not contain all the required elements of upper case, lower case, numeric, and special characters. While this console is open, look for the Administrator and the guest account. They have both been renamed as per the template.



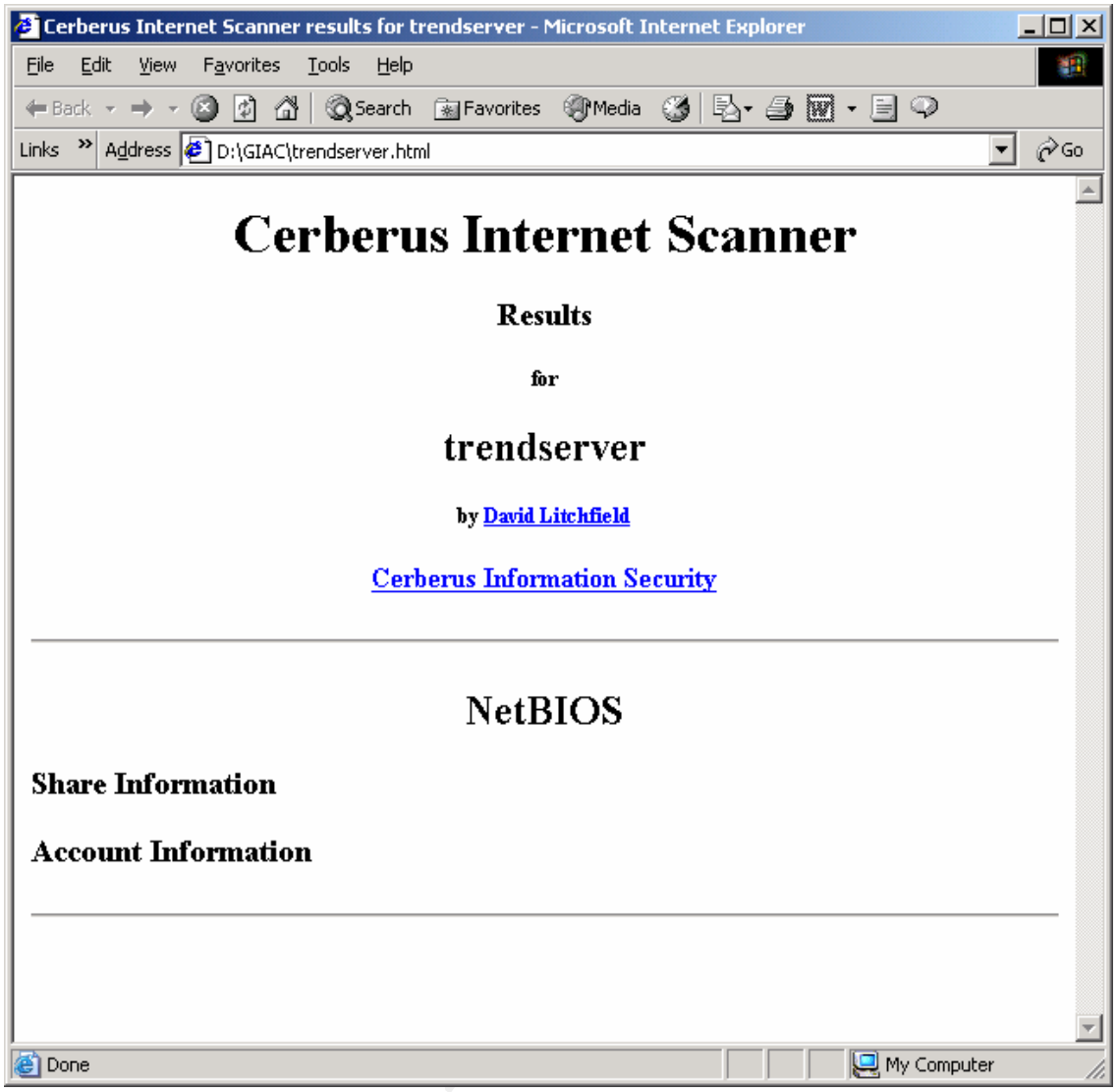
6.2 Post System Test #2 - Null Session check

As before, on Workstation1, open a Dos window, change directory to where NBTDUMP.EXE is located, type in “NBTDUMP trendserver”. An html file will be created showing the Server has the IPC$ (null session) port closed (as no user or file share information was extracted by the tool).

```
C:\Temp>nbtdump trendserver

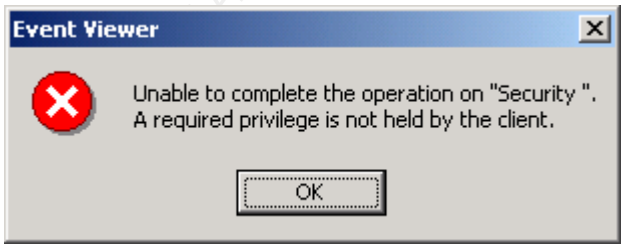
Results are written to trendserver.html.
Connecting to \\trendserver...Couldn't connect via nbsession.
```


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



6.3 Post System Test #3 - Security Event Log check

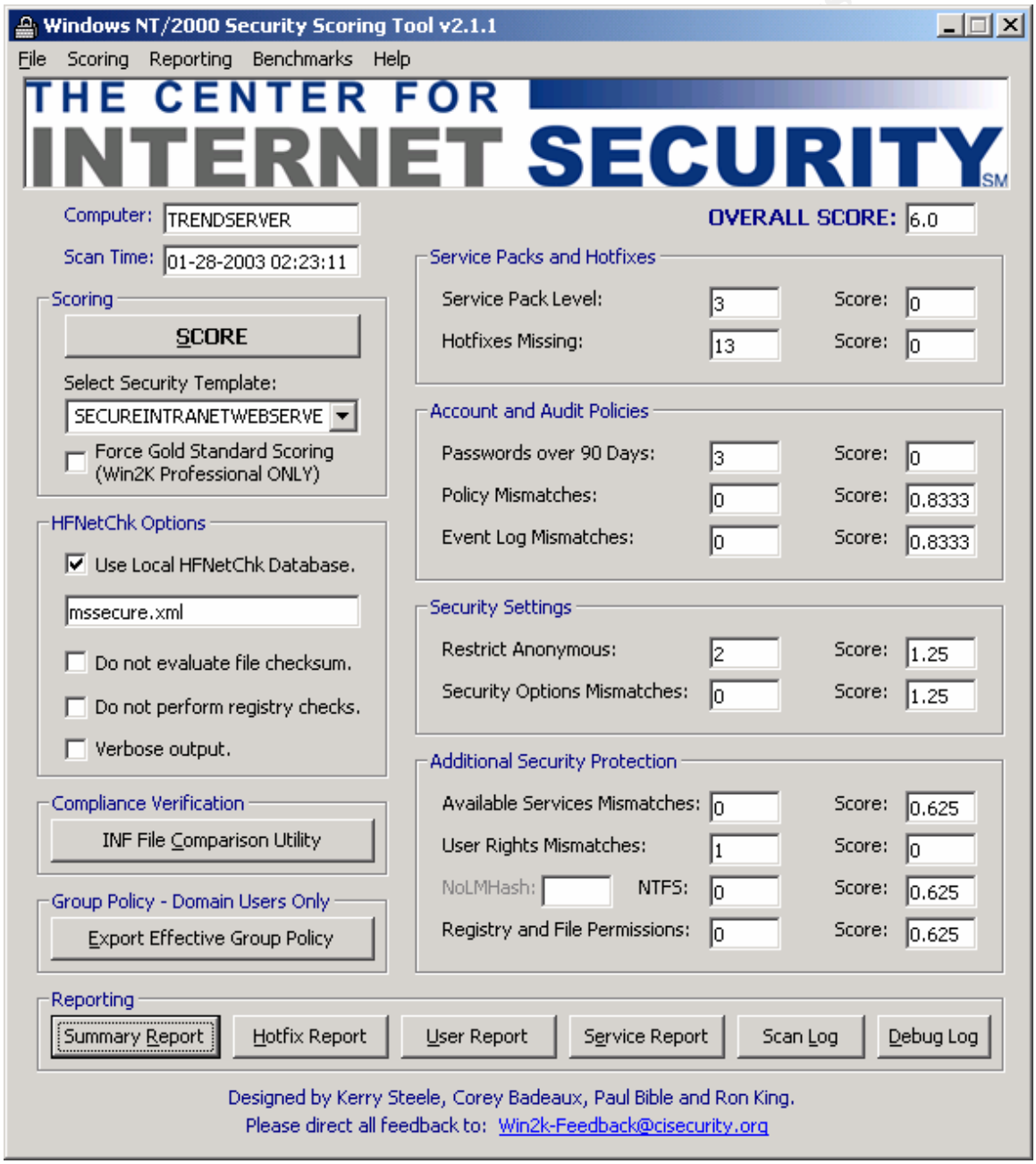
Log onto TrendServer using an account with Administrative privileges. Use the Computer Management console to view the properties of the Security Event Log. You will not be able to see any entries or settings, as you no longer have the rights to do so. Only the CorpSecurity group will be able to view and clear the Security event logs.



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

6.4 Post System Test #4 – Windows NT/2000 Security Scoring Tool

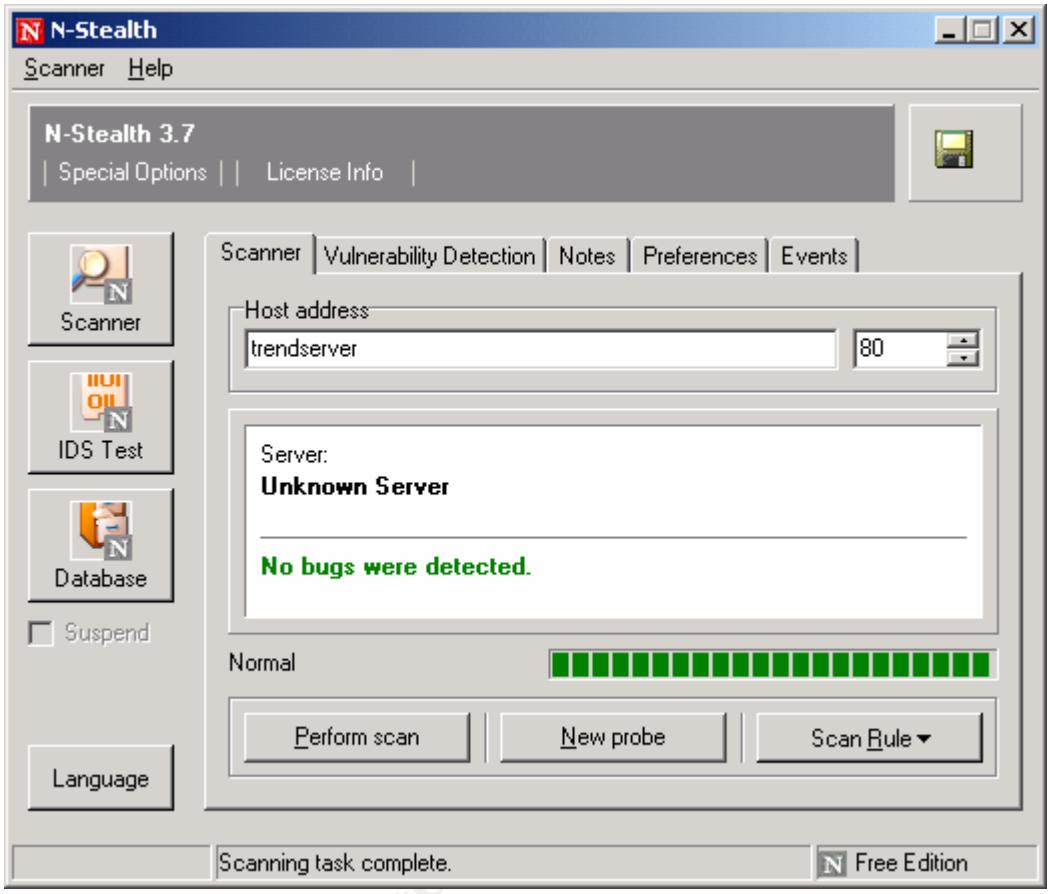
Using the CIS Windows Scoring tool as before, the system now tests with a score of 6.0. The jump in the score is based upon setting the restrictions for anonymous, turning on strong password requirements, disabling unneeded services, and setting other security options as per the template. The system would get a higher rating if the new OS patches and hot fixes were installed. Adding to the low score were accounts that have not yet had a recent password change. Now that we have password aging turned on, these accounts will require a password change in the near future.



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

6.5 Post System Test #5 - Web Server Vulnerability Assessment check

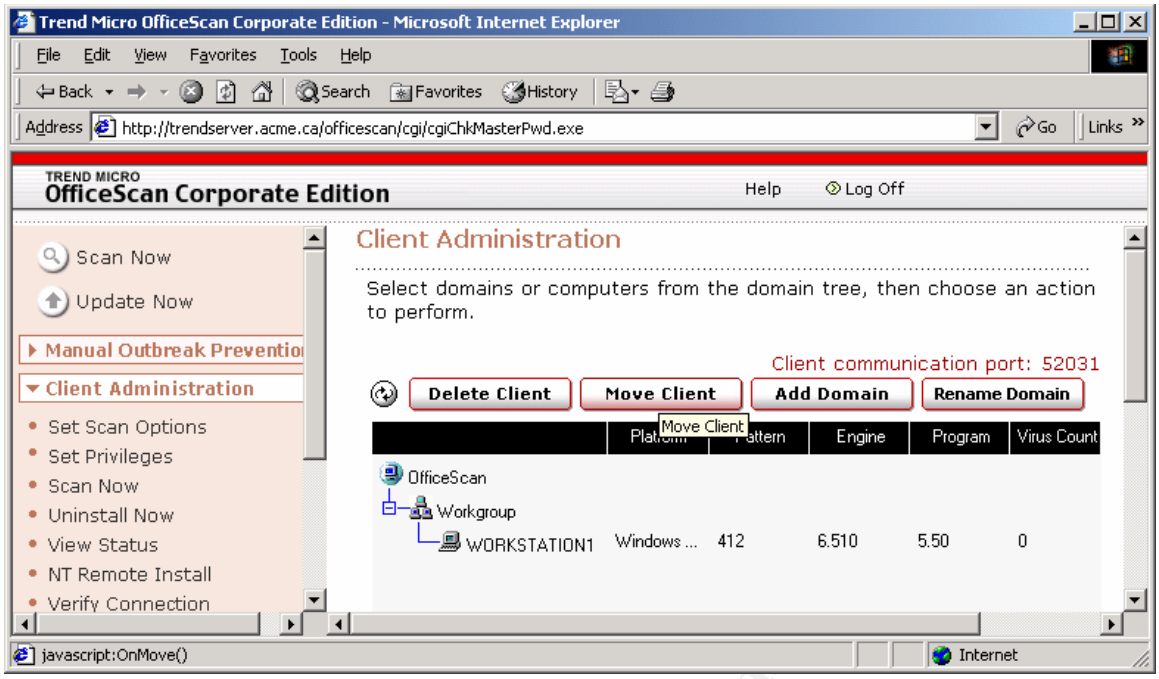
N-Stealth is launched again, Trendserver is scanned for vulnerabilities. This time, the scanner cannot tell which type of web server this system is, and there are no vulnerabilities reported. This test passes.



6.6 Post Application Test #1 – OfficeScan – Manage the Console

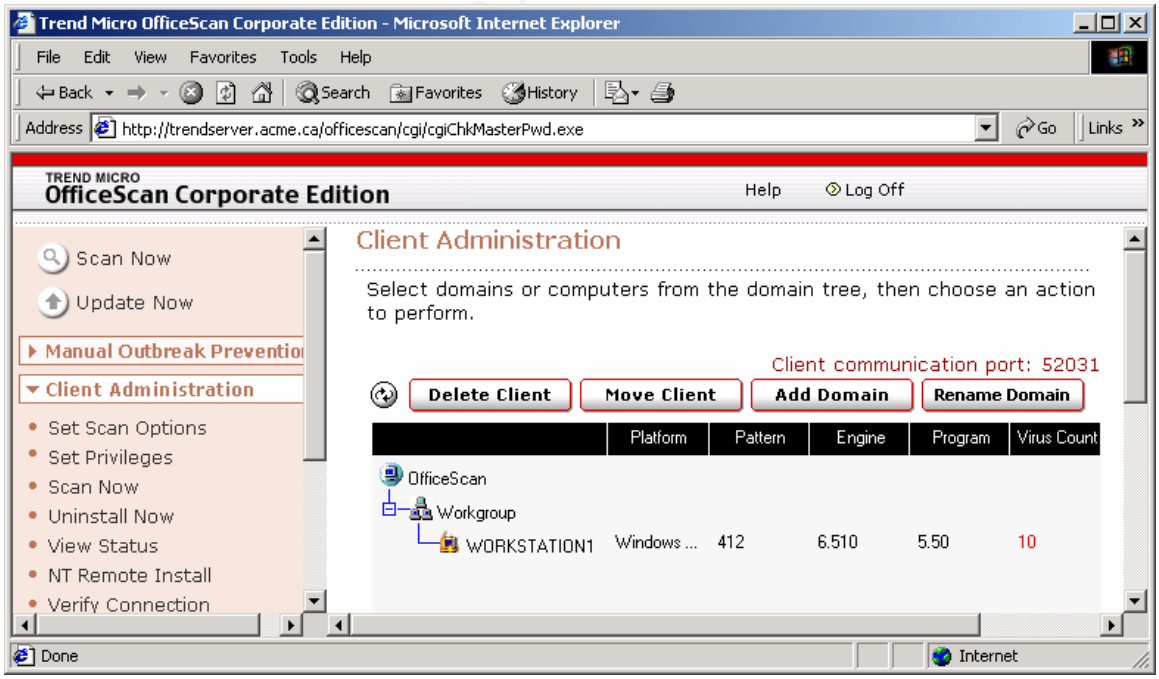
To confirm the Trend Micro OfficeScan Server console continues to functions properly, the console web page is accessed from “Workstation1”. For this test, I logged onto Workstation1 using account “Test”. This account was only in the “Users” group of Workstation1. There is no user “Test” on TrendServer. The user is able to log on to the OfficeScan console using the console password. The console shows Workstation1 as being active. The test passes as the console opens and displays properly.

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



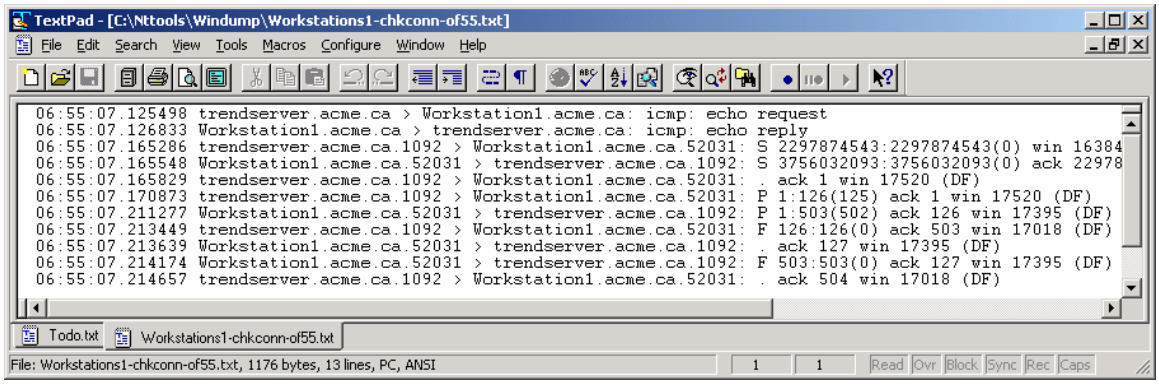
6.7 Post Application Test #2 – OfficeScan – Force a manual scan of an OfficeScan client

For this test, a manual scan is started on the client, Workstation1, by using the console. The SANS CD was put into the drive of Workstation1. Virus' were found on the CD and were reported back to the console (as seen by the computer icon with flames). This test passes as the Console to client communication is working properly in both directions.



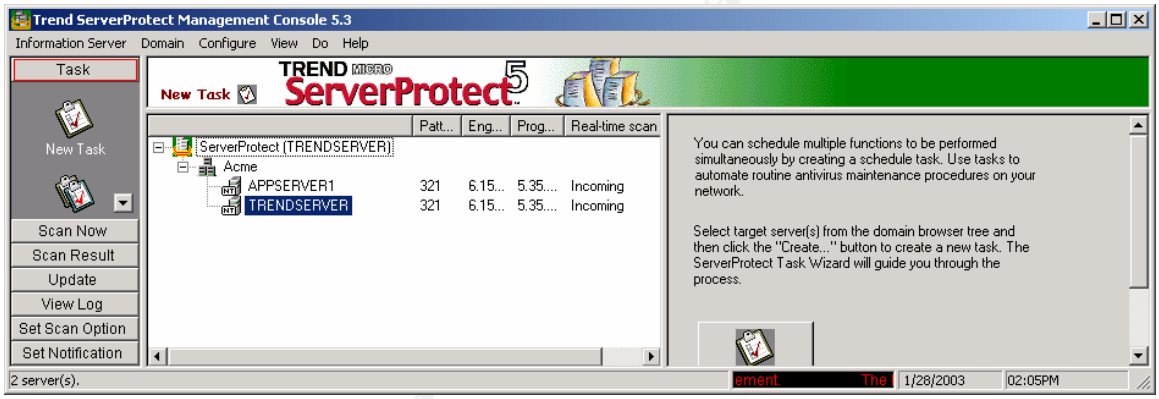
Another check was performed by using Windump [16]. One can see the successful network traffic between the Console and the workstation.

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



6.8 Post Application Test #3 – Server Protect – Manage the Console

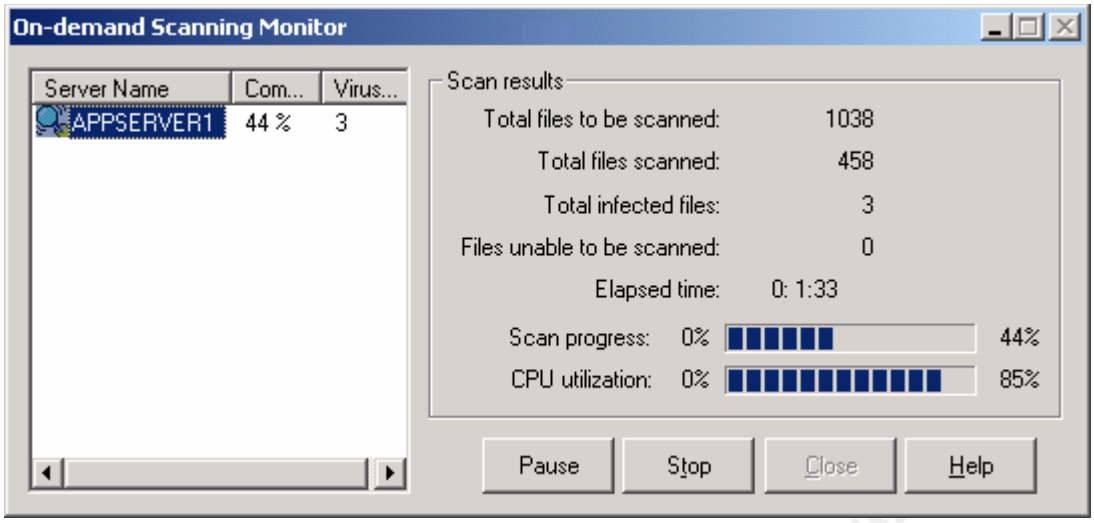
The Server Protect application is checked by launching the Server Protect console software installed locally on Workstation1. If the Information Server cannot communicate to a Normal Server client, it shows with a stop sign in the Console. This test passes as the console started okay and the Normal Servers, Appserver1 and Trendserver, show in the console as alive and connected.

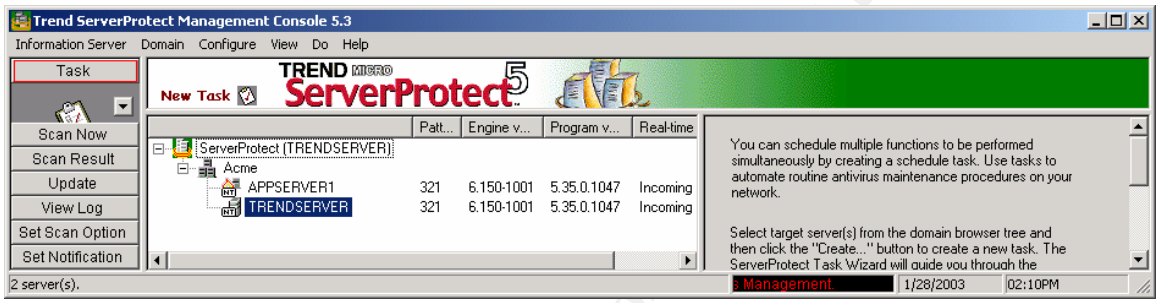


6.9 Post Application Test #4 – Server Protect – Force a manual scan of Server Protect client

A manual scan of a Normal Server client, AppServer1 was launched using the Server Protect Management Console. The SANS CD-Rom was left in the drive of AppServer1. The system passed the test as the scan started as expected and the files containing virus' were found on the CD-Rom and reported back to the console. This proves that the communication between the Information Server and the Normal server is working properly.

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





7 Evaluate the Template

The template did change several areas of the system. These changes reduced the risk from numerous vulnerabilities. The Password Policy areas have been improved by requiring complex passwords with a minimum length and minimum and maximum age. Account lockout settings were enabled to reduce the risk of someone trying to guess passwords. Auditing was enabled for the system so entries will show in the event logs. User Rights and Security options were modified to be more secure than the defaults. System Event Logs were modified to increase the size of the logs, restrict "guest" access, and the Security log was set for Manual clearing and access only by the Corporate Security group. The file system access security was modified for C:\Inetpub to restrict "Everyone" access to ftp and mail folders. The rest of the file and registry settings in the template were found to make the security worse than the initial install so they were not used. The Web server was made more secure as many unneeded and sample files were removed.

8 Undoing the Template – if required

When the server no longer functions as it should, or when an application no longer works properly, you may need to roll back your changes. This can be performed by using MS-Backup/Restore of the "System State". This requires a reboot. If that does not fix the problem, you can try the procedure outlined in the Microsoft Knowledge Base Article 313222 [17] http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b313222. This Article describes the following:

To reset your operating system back to original installation default security settings:

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

1. Click **Start**, click **Run**, type `cmd`, and then press ENTER.
2. Type `secedit /configure /cfg %windir%\repair\secsetup.inf /db secsetup.sdb /verbose`, and then press ENTER. You receive a "Task is completed" message, and a warning message that something could not be done. You can safely ignore this message. For more information about this message, view the %windir%\Security\Logs\Scesrv.log file.

9 Conclusion

While hardening the system by using a single template will reduce exposure to a number of vulnerabilities, IIS servers require additional steps to further reduce existing and future vulnerabilities. It is not likely that you will find a template that will meet all your needs. Look for an existing template and modify it to meet your needs in your environment. Lock it down as far as you can without breaking applications.. Even with all this work completed, you are not done as you must evaluate and install Service Packs and Hot Fixes shortly after they are released. Service Packs often contain fixes to unpublished vulnerabilities. If you manage more than a few systems of the same type, try using scripts to reduce the repetitive work. With Windows systems, a combination of templates, checklists and sound practical knowledge is required to harden systems effectively.

© SANS Institute 2003, Author retains full rights.

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

10 Appendix A - URLSCAN.INI

```
[options]
UseAllowVerbs=1                ; if 1, use [AllowVerbs] section, else use [DenyVerbs]
section
UseAllowExtensions=0           ; if 1, use [AllowExtensions] section, else use
[DenyExtensions] section
NormalizeUrlBeforeScan=1       ; if 1, canonicalize URL before processing
VerifyNormalization=1          ; if 1, canonicalize URL twice and reject request if a
change occurs
AllowHighBitCharacters=0       ; if 1, allow high bit (ie. UTF8 or MBCS) characters in
URL
AllowDotInPath=1               ; if 1, allow dots that are not file extensions
RemoveServerHeader=1           ; if 1, remove "Server" header from response
EnableLogging=1                ; if 1, log UrlScan activity
PerProcessLogging=0            ; if 1, the UrlScan.log filename will contain a PID (ie.
UrlScan.123.log)
AllowLateScanning=0            ; if 1, then UrlScan will load as a low priority filter.
PerDayLogging=1                ; if 1, UrlScan will produce a new log each day with
activity in the form UrlScan.010101.log
RejectResponseUrl=             ; UrlScan will send rejected requests to the URL specified
here. Default is /<Rejected-by-UrlScan>
UseFastPathReject=0            ; If 1, then UrlScan will not use the RejectResponseUrl or
allow IIS to log the request

; If RemoveServerHeader is 0, then AlternateServerName can be
; used to specify a replacement for IIS's built in 'Server' header
AlternateServerName=

[AllowVerbs]

;
; The verbs (aka HTTP methods) listed here are those commonly
; processed by a typical IIS server.
;
; Note that these entries are effective if "UseAllowVerbs=1"
; is set in the [Options] section above.
;

GET
HEAD
POST

[DenyVerbs]

;
; The verbs (aka HTTP methods) listed here are used for publishing
; content to an IIS server via WebDAV.
;
; Note that these entries are effective if "UseAllowVerbs=0"
; is set in the [Options] section above.
;

PROPFIND
PROPPATCH
MKCOL
DELETE
PUT
COPY
MOVE
LOCK
UNLOCK
OPTIONS
SEARCH

[DenyHeaders]

;
; The following request headers alter processing of a
; request by causing the server to process the request
; as if it were intended to be a WebDAV request, instead
; of a request to retrieve a resource.
;

Translate:
```

© SANS Institute 2003, Author retains full rights.

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

```
If:
Lock-Token:

[AllowExtensions]

;
; Extensions listed here are commonly used on a typical IIS server.
;
; Note that these entries are effective if "UseAllowExtensions=1"
; is set in the [Options] section above.
;

.htm
.html
.txt
.jpg
.jpeg
.gif

;.idq
;.htw
;.ida
;.idc
;.shtm
;.shtml
;.stm
;.htr
;.asp
;.cer
;.cdx
;.asa
;.printer
[DenyExtensions]

;
; Extensions listed here either run code directly on the server,
; are processed as scripts, or are static files that are
; generally not intended to be served out.
;
; Note that these entries are effective if "UseAllowExtensions=0"
; is set in the [Options] section above.
;
; Also note that ASP scripts are denied with the below
; settings.  If you wish to enable ASP, remove the
; following extensions from this list:
;    .asp
;    .cer
;    .cdx
;    .asa
;

; Deny ASP requests
.asp
.cer
.cdx
.asa

; Deny executables that could run on the server
;.exe
.bat
.cmd
.com
;.dll

; Deny infrequently used scripts
.htw     ; Maps to webhits.dll, part of Index Server
.ida     ; Maps to idq.dll, part of Index Server
.idq     ; Maps to idq.dll, part of Index Server
.htr     ; Maps to ism.dll, a legacy administrative tool
.idc     ; Maps to httpodbc.dll, a legacy database access tool
.shtm    ; Maps to ssinc.dll, for Server Side Includes
.shtml   ; Maps to ssinc.dll, for Server Side Includes
.stm     ; Maps to ssinc.dll, for Server Side Includes
.printer ; Maps to msw3prt.dll, for Internet Printing Services
```

© SANS Institute 2003, Author retains full rights.

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

```
; Deny various static files
;.ini     ; Configuration files
;.log     ; Log files
.pol     ; Policy files
.dat     ; Configuration files

[DenyUrlSequences]
..  ; Don't allow directory traversals
./  ; Don't allow trailing dot on a directory name
\   ; Don't allow backslashes in URL
;:   ; Don't allow alternate stream access
%   ; Don't allow escaping after normalization
;&   ; Don't allow multiple CGI processes to run on a single request
```

© SANS Institute 2003, Author retains full rights.

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

11 References

[1] Trend Micro
http://www.trendmicro.com/en/home/us/enterprise.htm

[2] Information on ports used by Trend Micro Server Protect
http://kb.trendmicro.com/solutions/solutionDetail.asp?solutionID=11669

[3] Fport.exe from Foundstone Inc.
http://www.foundstone.com/

[4] DumpSec from Somarsoft. Found in the utilities page.
http://www.somarsoft.com/

[5] SANS
www.sans.org

[6] Microsoft Knowledge article about Hisecweb.inf
http://www.microsoft.com/downloads/details.aspx?FamilyID=564a8b50-17d7-46f1-9a22-d9637bae9547&DisplayLang=en

[7] Centre for Internet Security
www.cisecurity.org

[8] National Security Agency
http://www.nsa.gov/snac/index.html

[9] Microsoft Windows 2000 Server Resource Kit

[10] NBTDUMP null session checker
http://www.atstake.com/research/tools/nbtdump.exe

[11] CIS Scoring Tool
www.cisecurity.org

[12] N-Stealth Security Scanner, free version
http://www.nstalker.com/nstealth/

[13] Article discussing using the Microsoft Lock Down Tool in a Trend Micro OfficeScan Server.
http://kb.trendmicro.com/solutions/solutionDetail.asp?solutionID=12286

[14] Article on URLScan settings for OfficeScan
http://kb.trendmicro.com/solutions/solutionDetail.asp?solutionID=11636

[15] Trend Micro article on CGI vulnerability
http://kb.trendmicro.com/solutions/solutionDetail.asp?solutionID=13353

[16] Windump packet sniffer (also requires WinPcap) available from
http://windump.polito.it/install/default.htm

[17] Microsoft Knowledge Base Article – Reset Security Settings
http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b313222

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