Global Information Assurance Certification Paper

Securing a Windows 2000 Datacenter Server Deploying an Enterprise Resource Planning System With Security Templates

prepared by Francois Vorster

November 2001

in partial fulfillment for the Global Information Assurance Certification (GIAC)

Securing Windows (GCNT)

GCNT Practical Assignment (v3.0) (August 2001)

Option 2 – Securing Windows 2000 With Security Templates

Table of Contents

System and Security Template Selection

Windows 2000 Based System Selection and Description

Given the dependence of organizations on the availability, validity and integrity of their data, transaction processes and associated processing resources when deploying enterprise resource planning ("ERP") systems, it is critical that these assets be protected in the most appropriate manner without compromising operational efficiency and effectiveness.

This paper addresses, at a high-level, the security configuration settings in an ERP Windows 2000 server-based environment that, if correctly implemented and applied, should provide appropriate protection transparent to operations.

The following system, which is deployed to process all relevant enterprise-wide business transactions, and associated components were selected for the study.

System Software

Windows 2000 Datacenter Server

Oracle 9*i* Release 1 (9.01)

Application Software

Oracle E-Business Suite release 11*i* – including financials, customer relationship management, human resources, & supply chain management

Hardware (Application and Database Servers)

Dell PowerEdge 6450 – 2 node cluster

The reason for selecting the Windows 2000 Datacenter Server is as a result of the volume of real-time transactions processed by the organization.

Each of the 2 (two) servers in the cluster were installed as non-domain controllers and then promoted to domain controllers ("DC") status through executing DCPROMO.EXE. Active Directory ("AD") Services were also installed as a result of this DC promotion. Standard Windows 2000 Server domain controller setup were subsequently followed. Respectively, the two servers is responsible for transactions processing (Oracle Applications Release 11*i*) and database management (Oracle 9*i* Release 1)and data storage. Enterprise users need to obtain access to the application server, where the database server need only to be accessed by selected developers and the database administrator. This study is primarily concerned with the application

of a security template to the application server, with limited replication of these security configurations to the database server.[1]

Windows 2000 Datacenter Server navigation/application guidance:

To manage the setup for the 2 (two) cluster servers the following Microsoft Management Console ("MMC") Snap-in tools were installed:

(i) Active Directory Users and Computers
(ii) Active Directory Domains and Trusts
(iii) Active Directory Sites and Services
(iv) Active Directory Schema
(v) Security Configuration and Analysis
(vi) Security Templates
(vii) Group Policy Editor
(viii) ADSI Edit
(ix) Event Viewer

The following table provides background to the selection by comparing the different Windows 2000 Server selected technical features:[2]

Feature	Windows 2000 Server	Windows 2000 Advanced Server	Windows 2000 Datacenter Server
Processor limit	4	8	32
Memory support	4 GB Intel	8 GB Intel (PAE)	64 GB Intel (PAE)
Network Load Balancing	No	Yes (maximum 32 nodes)	Yes (maximum 32 nodes)
Server clustering	No	Yes (maximum 2 nodes)	Yes (maximum 4 nodes)
Job object	Job Object API	Job Object API	Process Control tool
Winsock Direct	No	No	Yes
Hardware Compatibility List	Yes	Yes	Datacenter HCL

Level of Security Required

The level of security is classified at the entry level of HIGH on a scale of LOW / MODERATE / HIGH. The criteria for this classification is elaborated on below.

[1] It is assumed that maintenance to the Active Directory, and the associated security settings, be restricted to the application server, with replication of selected settings to the database server.

[2] Microsoft Corporation, Windows 2000 Datacenter Server White Paper (2000), p. 3 http://www.microsoft.com/windows2000/docs/datacenterserver.doc

Secure Domain Controller Security Template

Windows 2000 comes with a number of pre-defined *basic* and *incremental* templates which can be modified. Basic templates specify default security settings for all security areas with the exception of user rights and groups, and are designed to reverse changes to system security that result in unwanted system behavior. Incremental templates are used to modify default security settings for machines already running the default security setting.[3] These templates are textual .INF files and is stored in \%systemroot%\Security\Templates and can be viewed and managed through the Security Templates snap-in tool . The following are the default templates provided:

.inf Filename	Category	Description[4]
basicwk.inf	basic	Default workstation
basicsv.inf	basic	Default Windows 2000 server
basicdc.inf	basic	Default Windows 2000 domain controller
OCFiless.inf	basic	For standalone or member servers
OCFilesws.inf	basic	For computer running Windows 2000Professional
compatws.inf	incremental	Compatible workstation or server
securews.inf	incremental	Secure workstation or server
hisecws.inf	incremental	Highly secure workstation or server
securedc.inf	**incremental**	**Secure domain controller**
hisecdc.inf	incremental	Highly secure domain controller

For our environment to be secured, the bolded template (SECUREDC.INF – Secure domain controller) will be used as the basis for the study.

Security Template (SECUREDC.INF) Selection Criteria

Based on the reasons for securing the system to a certain level, and upon initial review of the secure domain controller template, the settings provided by this template is a good starting point to achieve our security settings objectives. In addition, default security settings in the SECUREDC.INF template will result in the least of changes given the other templates and their default settings.

Security in the environment under review is pivotal, in fact more so in this environment than typical ERP organizations, based on the following reasons:

1. Availability requirements for transaction processing and information on a 24x7 basis

[3] Internet Security Systems, Inc., Microsoft Windows 2000 Security Technical Reference, (Microsoft Press, 2000), pp. 308-309.

[4] SANS Institute, Windows 2000: Active Directory and Group Policy, Track 5 – Securing Windows 2000, document version 5.0

2. Although a public company, the primary shareholders' financial data are being processed through the financial application modules

3. Sensitive human resource and payroll data and private customer information

Secure Domain Controller Security Template Analysis

Explanation and Basic Analysis of the SECUREDC.INF Security Template

To explain and perform a basic analysis of the security settings of the SECUREDC.INF security template, the following tables indicate the primary security default settings. The tables include the (i) Account Polices, (ii) Local Policies, and (iii) Event Log security areas. Excluded settings from the table are the (i) Restricted Groups, (ii) System Services, (iii) System Registry, and (iv) File System Store. The latter security areas were excluded from the analysis given that users are not assigned settings individually at this stage, as well as granularity and content constraints.

Windows 2000 Datacenter Server navigation/application guidance:

1. Open Security Template tool
2. Select the SECURE.INF in the Security Templates container
3. Double-click on the required Security Setting in the list of settings
4. Configuration options available in setting will be displayed

Account Policies

Security Configuration Tool Set Title	Default Setting (Secure DC)	Explanation	Too Strong	Too Weak	Appropriate	Adjusted Setting[5]
Password Policy						
Enforce password history	24 passwords remembered	A password is not allowed to be used within the stated number of setting	X			12 passwords remembered
Maximum password age	42 days	Number of days a password is valid prior to expiration		X		30 days
Minimum password age	2 days	Age of a password before change allowed	X			1 day
Minimum password length	8 characters	Mandatory number of characters in a password	X			6 characters
Password must meet complexity requirements	Enabled	Password must contain capitals, numerals or punctuation, and cannot contain your account or full name			X	

[5] Settings indicated as adjusted for the system under review, will be changed according to the steps in the next section

Security Configuration Tool Set Title	Default Setting (Secure DC)	Explanation	Too Strong	Too Weak	Appropriate	Adjusted Setting[5]
Store password using reversible encryption for all users in the domain	Disabled	[NOT APPLICABLE]			X	
Account Lockout Policy						
Account lockout duration	30 minutes	Time that an account is locked out after maximum number of invalid logon attempts			X	
Account lockout threshold	5 invalid logon attempts	The user account is disabled/l locked out after the specified number of invalid password attempts		X		3 invalid logon attempts
Reset account lockout counter after	30 minutes	Allow user to re-logon after invalid attempt lockout			X	

Security Configuration Tool Set Title	Default Setting (Secure DC)	Explanation	Too Strong	Too Weak	Appropriate	Adjusted Setting[5]
Kerberos Policy						
Enforce user logon restrictions	Not defined	When enabled the Kerberos Key Distribution Center ("KDC") validates every request for a session ticket by examining user rights policy on the target computer to verify that the user has the right either to Log on locally or to Access this computer from network.		X		Enabled
Maximum lifetime for service tickets	Not defined	A "service ticket" is a session ticket. A ticket obtained during a logon session, those used to access other resources or services. The environment establishes the lifetime of the ticket and allows the user to maintain that session information for the entire time it is valid. The session ticket default lifetime is ten hours just as the lifetime of the Ticket Granting Ticket ("TGT") as in the setting below, but the time is set in minutes, not hours. The maximum lifetime for a session ticket can be anything above ten minutes up to and including (but never more than) the maximum lifetime for the TGT.[6]		X		600 minutes

[6] Microsoft Corporation, Windows 2000 Kerberos Authentication White Paper (1999)
http://www.microsoft.com/TechNet/prodtechnol/windows2000serv/deploy/confeat/kerberos.asp

Security Configuration Tool Set Title	Default Setting (Secure DC)	Explanation	Too Strong	Too Weak	Appropriate	Adjusted Setting[5]
Maximum lifetime for user ticket	Not defined	A "user ticket" is a Ticket Granting Ticket (“TGT”). The TGT in Kerberos is used by the client to request a ticket to access the desired network resource or service. During the time the TGT is valid for the user, their system maintains the information in a location known as the "credentials cache". This is a part of the volatile memory, which is erased when the power to the machine is interrupted. The credentials cache information is never stored on the disk in the machine or any other static memory location where it could be obtained and used without authorization. This setting specifies the maximum lifetime for such tickets.		X		10 hours
Maximum lifetime for user ticket renewal	Not defined	With the basic ticket it is only issued for a finite, one time period and cannot be reused or changed in any way. A renewable ticket is one issued with the intent of being able to change small parts of information on the ticket and reuse them for extended periods of time. Setting indicate time for ticket renewal.		X		10 days

Security Configuration Tool Set Title	Default Setting (Secure DC)	Explanation	Too Strong	Too Weak	Appropriate	Adjusted Setting[5]
Maximum tolerance for computer clock synchronization	Not defined	When the client logs onto their system and asks for a TGT, the Kerberos client will normally take the user's long-term key (derived from the hashing of the password entered) and encrypt the system time on the machine, hence the requirement for a time tolerance as indicated by this setting.		X		20 minutes

Local Policies

Security Configuration Tool Set Title	Default Setting (Secure DC)	Explanation	Too Strong	Too Weak	Appropriate	Adjusted Setting
Audit Policy						
Audit account logon events	Failure	Record account logon activities – currently only when there are failed activities, i.e. incorrect user			X	
Audit account management	Success/Failure	Record account management activities – currently during all activities			X	
Audit directory services access	Failure	Record access to directory services			X	
Audit logon events	Failure	Record logon activities – currently only when there are failed activities, i.e. incorrect passwords/authentication			X	
Audit object access	No auditing	Record activities related to specific objects. Only to be activated on an ad hoc basis when circumstances require investigation.			X	
Audit policy change	Success/Failure	Record when there is a change to the audit policies – currently under all circumstances			X	

Security Configuration Tool Set Title	Default Setting (Secure DC)	Explanation	Too Strong	Too Weak	Appropriate	Adjusted Setting
Audit privilege use	Failure	Record activities related to privilege use.			X	
Audit process tracking	No auditing	[NOT APPLICABLE]			X	
Audit system events	No auditing	[NOT APPLICABLE]			X	
User Rights Assignment	**Not defined**	Determine range of policy settings for users.	**No settings defined as this is excluded from the scope at present**			
Security Options						
Additional restrictions for anonymous connections	Do not allow enumeration of SAM accounts and shares	Setting related to Security Accounts Manager (SAM) accounts and shares. The SAM database area of the registry on domain controllers is replaced by AD.			X	
Allow server operators to schedule tasks (domain controllers only)	Disabled	[NOT APPLICABLE]			X	
Allow system to be shut down without having to log on	Disabled	[NOT APPLICABLE]			X	
Allowed to eject removable NTFS media	Administrators	Only Administrators are allowed to eject removable NT File System media			X	
Amount of idle time required before disconnecting session	15 minutes	Inactivity by user, in minutes, when a session will be disconnected.			X	
Audit the access of global system objects	Disabled	[NOT APPLICABLE]			X	
Audit use of Backup and Restore privilege	Disabled	[NOT APPLICABLE]			X	
Automatically log off users when logon time expires	Enabled				X	
Automatically log off users when logon time expires (local)	Enabled				X	
Clear virtual memory pagefile when system shuts down	Disabled	[NOT APPLICABLE]			X	
Digitally sign client communication (always)	Disabled	[NOT APPLICABLE]			X	

Security Configuration Tool Set Title	Default Setting (Secure DC)	Explanation	Too Strong	Too Weak	Appropriate	Adjusted Setting
Digitally sign client communication (when possible)	Enabled				X	
Digitally sign server communication (always)	Disabled	[NOT APPLICABLE]			X	
Digitally sign server communication (when possible)	Enabled				X	
Disable Ctrl+Alt+Del requirement for logon	Disabled	[NOT APPLICABLE]			X	
Do not display last username in logon screen	Disabled	[NOT APPLICABLE]		X		Enable
LAN Manager Authentication Level	Send NTLM response only				X	
Message text for users attempting to log on		Please contact Help Desk at 1-800-555-SANS when help is needed			X	
Message title for users attempting to logon					X	
Number of previous logons to cache (in case domain controller is not available)	10 logons				X	
Prevent system maintenance of computer account password	Disabled	[NOT APPLICABLE]			X	
Prevent users from installing printer drivers	Enabled				X	
Prompt user to change password before expiration	14 days				X	
Recovery Console: Allow automatic administrative logon	Disabled	[NOT APPLICABLE]			X	
Recovery Console: Allow floppy copy and access to all drivers and all folders	Disabled	[NOT APPLICABLE]			X	
Rename administrator account	Not defined	[NOT APPLICABLE]			X	
Rename guest account	Not defined	[NOT APPLICABLE]			X	

Security Configuration Tool Set Title	Default Setting (Secure DC)	Explanation	Too Strong	Too Weak	Appropriate	Adjusted Setting
Restrict CD-ROM access to locally logged-on user only	Enabled				X	
Restrict floppy access to locally logged on user only	Enabled				X	
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled	[NOT APPLICABLE]			X	
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled				X	
Secure channel: Digitally sign secure channel data (when possible)	Enabled				X	
Secure channel: Require strong (Windows 2000 or later) session key	Disabled	[NOT APPLICABLE]			X	
Secure system partition (for RISC platforms only)	Not defined	[NOT APPLICABLE]			X	
Send unencrypted password to reversible connect to third-party SMB servers	Disabled	[NOT APPLICABLE]			X	
Shut down system immediately if unable to log security audits	Disabled	[NOT APPLICABLE]			X	
Smart card removal behavior	Force Logoff	[NOT APPLICABLE]			X	
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled				X	
Unsigned driver installation behavior	Do not allow installation				X	
Unsigned non-driver installation behavior	Warn but allow installation				X	

Event Log

Security Configuration Tool Set Title	Default Setting (Secure DC)	Explanation	Too Strong	Too Weak	Appropriate	Adjusted Setting
Settings for Event Logs						
Maximum application log size	Not defined	Specify application event log size		X		5120 kilobytes
Maximum security log size	5120 kilobytes	Specify security event log size			X	
Maximum system log size	Not defined	Specify system event log size			X	
Restrict guest access to application log	Enabled	Guest account is not allowed to access this event log			X	
Restrict guest access to security log	Enabled	Guest account is not allowed to access this event log			X	
Restrict guest access to system log	Enabled	Guest account is not allowed to access this event log			X	
Retain application log	Not defined	[NOT APPLICABLE]			X	
Retain security log	Not defined	[NOT APPLICABLE]			X	
Retain system log	Not defined	[NOT APPLICABLE]			X	
Retention method for application log	Not defined	[NOT APPLICABLE]			X	
Retention method for security log	As needed	Indicate how the retention, e.g. deletion or archiving of the security log be handled.		X		Manually
Retention method for system log	Not defined	[NOT APPLICABLE]			X	
Shut down the computer when the security audit log is full	Not defined	[NOT APPLICABLE]		X		Disabled

Security Template Application and Testing

Applying and Maintaining the Secure Domain Controller Template

Applying SECUREDC.INF with changes to the System

Applying new security settings to the environment comprise of the following two steps:

1. Create new security template based on SECUREDC.INF
2. Customize the new security template to conform to environment requirements
3. Analyze the new template relative to the computer security settings
4. Importing the new secure template into the domain controller associated Group Policy Object ("GPO")
5. Ensure that the updated GPO has been applied

Step 1 – Create and Update Security Settings

At installation the Windows 2000 Datacenter DC already has the basic security template (BASICDC.INF) applied by default through the linked GPO, (DEFAULT DOMAIN POLICY).

Our approach is to create a new security template (GC2000_ORACLE.INF) based on the selected security template (SECUREDC.INF) for the study.

Windows 2000 Datacenter Server navigation/application guidance:

1. Open Security Templates tool
2. Right click on the SECUREDC template
3. Save As GC2000_ORACLE
4. View new template in Security Tool container (no description at this stage)
5. Right click GC2000_ORACLE template / Set Description
6. Add description / click OK

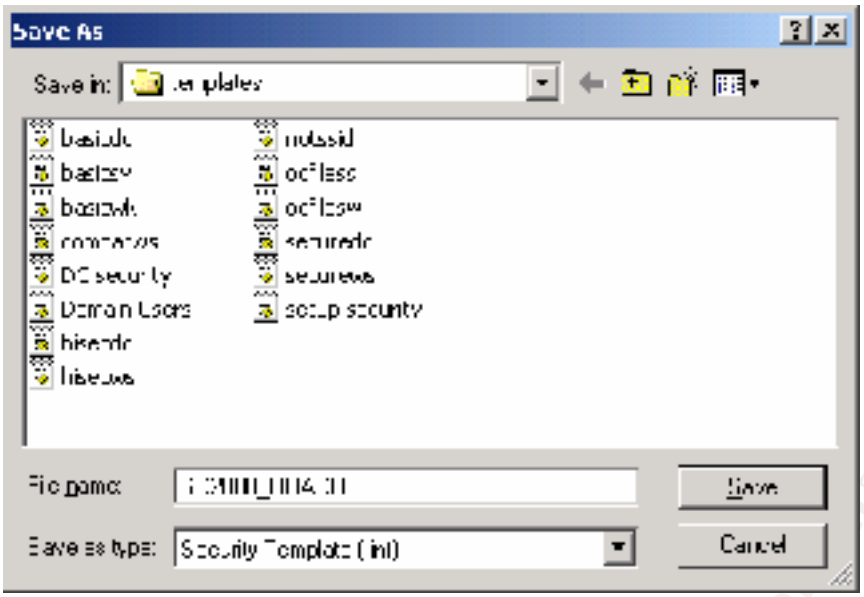

Figure 1 – Creating the new security template by saving it as GC2000_ORACLE

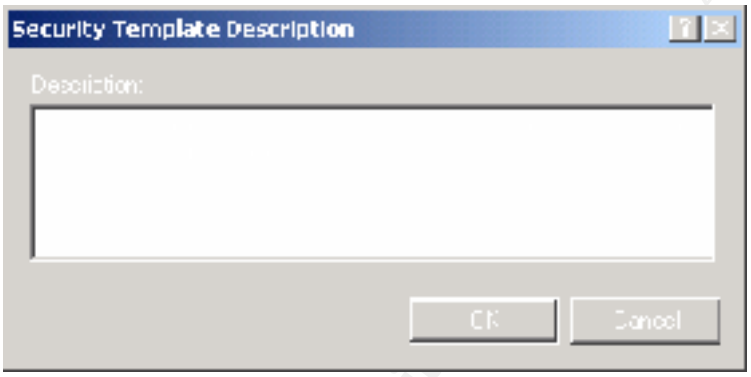

Figure 2 – Adding a subscription to the newly created security template

Step 2 – Customize the New Security Template

Changing the selected security settings, as identified in the previous section above, that are not appropriate (too strong, too weak, or need to be configured) for the environment need now be made within the GC2000_ORACLE template.

Windows 2000 Datacenter Server navigation/application guidance:

1. Open Security Template tool
2. Expand GC2000_ORACLE container
3. Click on Policy (right window) and make change, e.g. GC2000_ORACLE / Account Policies / double-click Enforce password History / change to 12 / click OK
4. Repeat changes for required policies

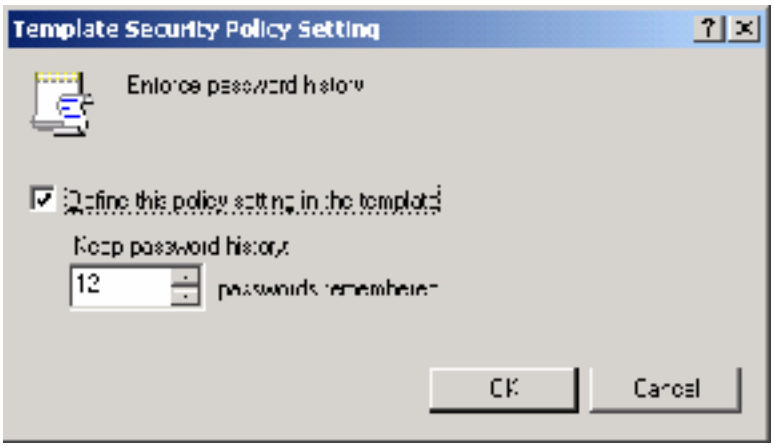

Figure 3 – Example of template security setting (Enforce password history)

Step 3 – Analyze the New Template Settings Relative to Computer Settings

An analysis of the GC2000_ORACLE template is now recommended using the Security Configuration and Analysis tool. This analysis is useful for a number of reasons:[7]

- To identify security weaknesses that might exist in the current configuration[8]
- To identify changes that a potential security policy might impart to a system before the policy is actually deployed
- To identify deviations from a policy currently imposed on the system.

Windows 2000 Datacenter Server navigation/application guidance:

1. Open Security Configuration and Analysis tool
2. Follow the steps to Create a New Database (right section of window)
3. New Security Database File created – GC2000_ORACLE.SDB
4. Follow the steps to Analyze Your Computer Security Settings (right section of window)
5. Right click Security Configuration and Analysis and select View Log File
6. Log file appears in right section of window

The analysis can be performed in two ways:

1. Review the analysis log file itself (example attached as **Appendix A**)

[7] Internet Security Systems (2000), op. cit., p. 321.

[8] It should be noted that this analysis only applies to the Local Computer policy. However, for the purposes of consistency in our policies, we would want the Domain Controller, Domain, and Local security policies to be the same.

2. Navigate to the individual policy in the Security Configuration and Analysis tool, where both the Database Setting and Computer Setting will be reflected, with discrepancies indicated by a red cross on the policy icon

Step 4 – Importing the New Template Into the GPOs

The system security settings can be configured through (i) the analysis tool (Local Computer), (ii) the GPO itself, or (iii) by importing the created and modified template into the GPO. For future consistency in management of the template and its settings, the latter approach is followed.

Windows 2000 Datacenter Server navigation/application guidance:

1. Open the Group Policy tool and expand the container – Local Computer Policy
2. Right click on the Security Settings in the Windows Settings container / select Import Policy
3. Select GC2000_ORACLE template in the Import Policy From window / click OK
4. Repeat 1 – 3 for the Domain Controller and the Domain GPOs via the respective Group Policy tools

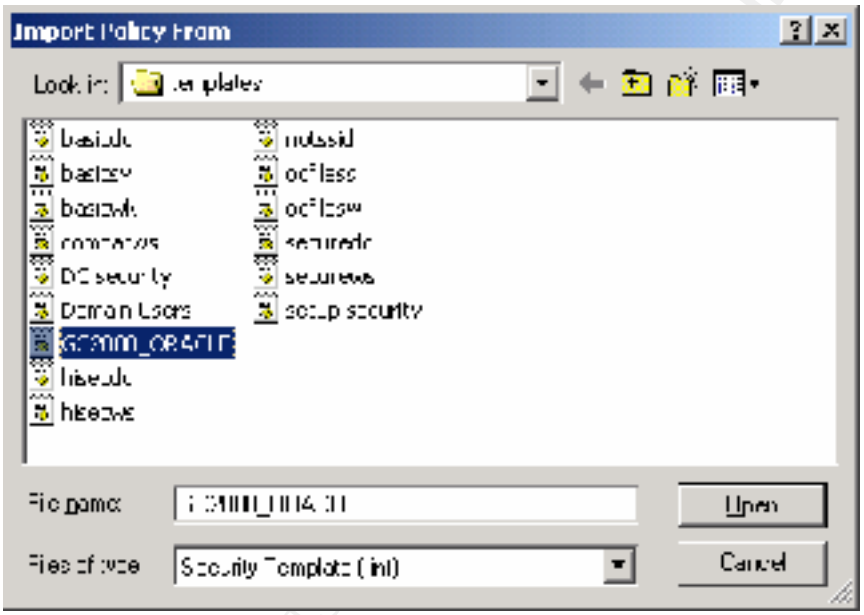

Figure 4 – Importing the GC2000_ORACLE security template/policy into the GPO

Step 5 – Ensure the Updated GPO is Applied

It should be taken into account that within Active Directory, computers refresh GPO settings at established intervals. The default Group Policy refresh intervals are:[9]

[9] Julie M. Haney, Guide to Securing Microsoft Windows 2000 Group Policy, National Security Evaluations and Tools Division of the System and Network Attack Center (SNAC), National Security Agency, January 2001, Version 1.0

- 90 minutes for computer running Windows 2000 Professional and for member servers running Windows 2000 Server;
- 5 minutes for domain controllers

Refreshing of the policy can also be done manually by typing the following at the command line: secedit/refreshpolicy MACHINE_POLICY

Another method of determining whether a security policy was applied, the Event Viewer Snap-in tool was installed. The following event was specifically noted as a result of the Kerberos policy change:

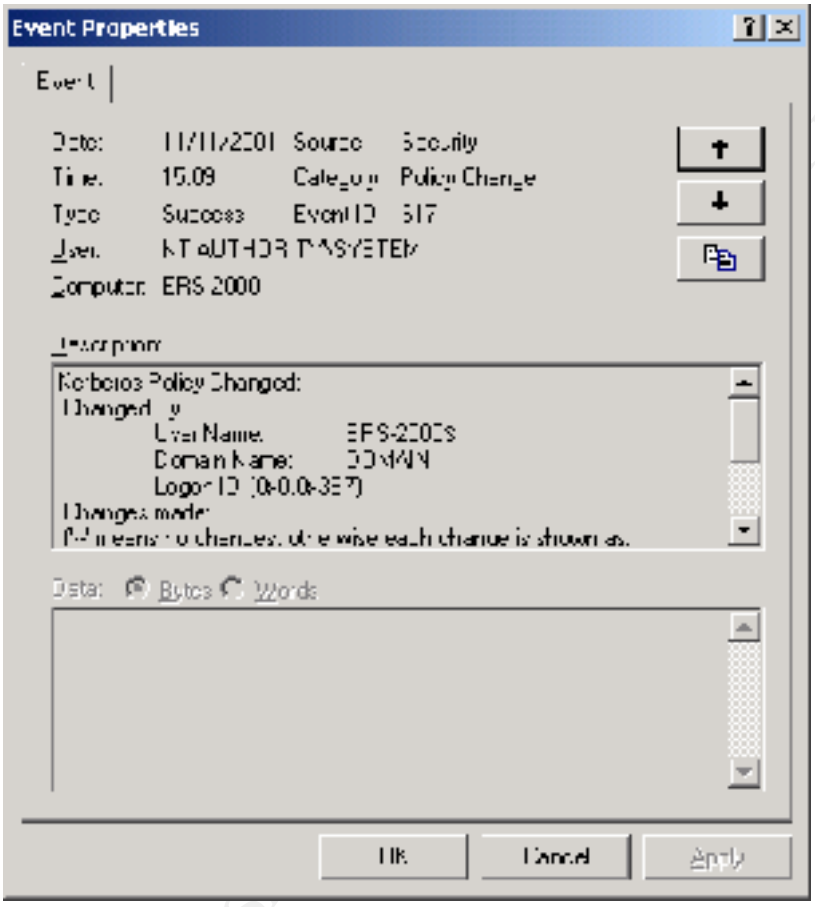

Figure 5 – Event log entry properties indicating the security policy change

Maintaining and Refreshing the Security Settings and Template Over Time

It is imperative that the security settings of the system be kept in accordance with requirements as the environment dictates, whether based on internal or external threats, or operating efficiencies.

To ensure the validity, consistency, accuracy and integrity of security changes applied, a formal written policy and associated procedures should be developed and implemented. This will limit discrepancies in the event of security breaches and possible associated system problems.

From the Windows 2000 Server perspective, the following maintenance and refreshing steps should be implemented and followed:

1. Review event logs on a regular basis and determine whether security settings are appropriate based on analytic review.
2. Through the formal change control procedure, refine security settings within the template in a test environment. Test the changes and obtain approval for migration to production.[10]
3. Apply the changes to the security template in the production environment.
4. Re-associate the security template with the applied policy.
5. Ensure that the replication between the physical domain controllers occur as intended.[11]
6. Monitor implemented changes on an ongoing basis through reviews and event logging.

Security Template Acceptance Testing

Three security settings are now tested to ensure that the applied template and configuration changes are working as expected. The testing is presented in a table as follows:

Security Setting	Test Steps	Expected Result	Test Result	Ref. #
Maximum password age	1. Change password with initial sign-on 2. Advance system date 10 days. 3. Sign-on normally 4. Record results 5. Advance system date more than 30 days 6. Attempt to change password 7. Record results	Force password change at 30 days	The password was forced to be changed only after the 30th day and not after the 10th day. Expected result.	Fig. 6

[10] It is assumed that the environment contains a test system (at least one domain controller) that mirrors the production environment to perform the necessary tests. This test environment would be subject to the same level of security to provide the appropriate level of integrity for security changes tested prior to migration to production.

[11] Refer section at end of study related to domains, domain controllers, and AD replication.

Audit logon events	Attempt to logon 3 times with incorrect password	User account to be lockout after 3rd attempt	User account locked out after 3rd attempt	Fig. 7 Fig. 8
Audit policy change	Indicate that policy changed during this study has been recorded in the log (e.g. Kerberos policy changes)	Policy change recorded in Event Log	Event Log indicate relevant changes to Kerberos policy	Fig. 9

```
12/29/2001  3:35:04 PM  Security    Failure Audit     Logon/Logoff      535
      NT AUTHORITY\SYSTEM     ERS-2000    "Logon Failure:
      Reason:           The specified account's password has expired
      User Name:  fvorst
      Domain:           DOMAIN
      Logon Type: 2
      Logon Process:    User32
      Authentication Package: Negotiate
      Workstation Name: ERS-2000 "
12/29/2001  3:35:04 PM  Security    Failure Audit     Account Logon     676
      NT AUTHORITY\SYSTEM     ERS-2000    "Authentication Ticket Request
Failed:
      User Name:  fvorst
      Supplied Realm Name:    DOMAIN
      Service Name:     krbtgt/DOMAIN
      Ticket Options:   0x40810010
      Failure Code:     23
      Client Address:   192.168.0.71
 "
```

Figure 6 – Event log entry indicating that account's password has expired and that Kerberos authentication ticket request failed

```
11/11/2001  3:46:58 PM  Security    Failure Audit     Logon/Logoff      529
      NT AUTHORITY\SYSTEM     ERS-2000    "Logon Failure:
      Reason:           Unknown user name or bad password
      User Name:  fvorst
      Domain:           DOMAIN
      Logon Type: 2
      Logon Process:    User32
      Authentication Package: Negotiate
      Workstation Name: ERS-2000 "
11/11/2001  3:46:58 PM  Security    Success Audit     Account Management
      642   Everyone    ERS-2000    "User Account Changed:
       Account Locked.
      Target Account Name:    fvorst
      Target Domain:    DOMAIN
      Target Account ID:      DOMAIN\fvorst
      Caller User Name: ERS-2000$
      Caller Domain:    DOMAIN
      Caller Logon ID:  (0x0,0x3E7)
      Privileges: -
 "
11/11/2001  3:46:58 PM  Security    Success Audit     Account Management
```

```
      644   Everyone    ERS-2000    "User Account Locked Out:
      Target Account Name:    fvorst
      Target Account ID:      DOMAIN\fvorst
      Caller Machine Name:    ERS-2000
      Caller User Name: ERS-2000$
      Caller Domain:    DOMAIN
      Caller Logon ID:  (0x0,0x3E7)
 "
```

Figure 7 – Event log entry indicating that user account locked out after maximum number of invalid password attempts

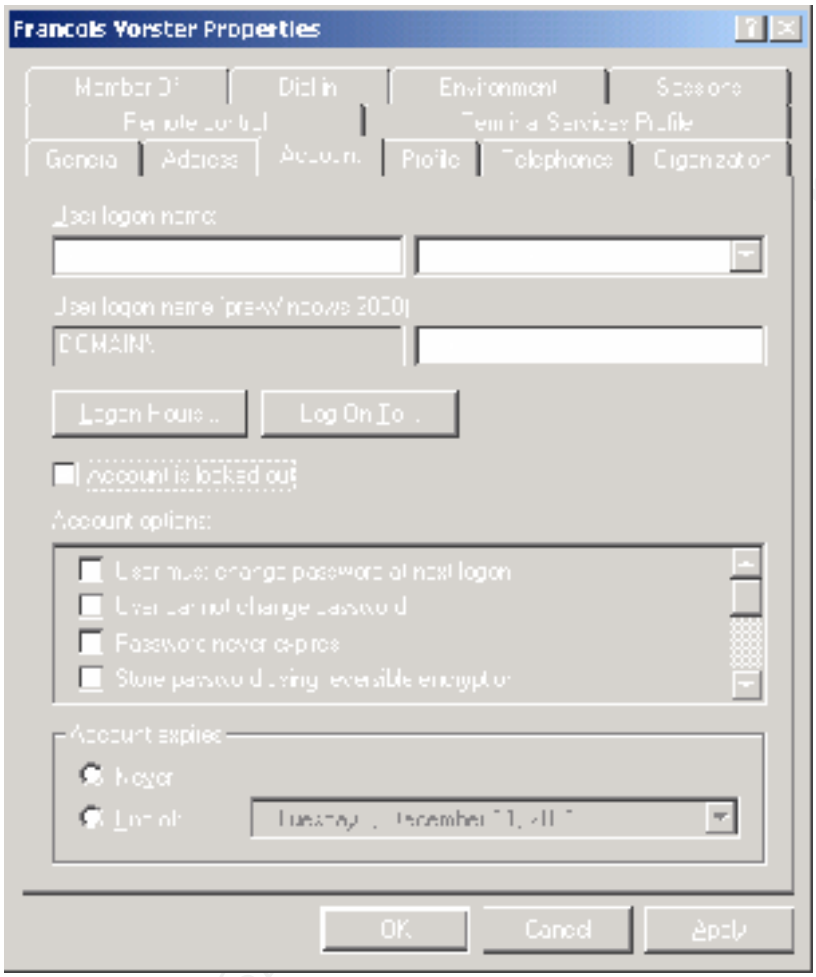

Figure 8 – Indicate in user account properties that account was placed in locked out mode after invalid attempts

```
11/21/2001  3:34:31 PM  Security    Success Audit     Account Management
      643   NT AUTHORITY\SYSTEM     ERS-2000    "Domain Policy Changed:
Password Policy  modified
      Domain:           DOMAIN
      Domain ID:  DOMAIN\
      Caller User Name: ERS-2000$
      Caller Domain:    DOMAIN
      Caller Logon ID:  (0x0,0x3E7)
```

```
      Privileges: -
"
```

Figure 9 – Event log entry indicating that security policy changes are recorded in the event log

System Intact Analysis

To widen our tests of the implementation of the new security policies into the system, additional intact analysis test were performed. These are described in the table below.

Test Performed	Problems Noted	Results
Requested assistance from three system users to perform both normal and inconsistent logons onto the Windows 2000 systems and record the results. Typical tests performed included, but were not limited to (i) invalid logon attempts; (ii) accessing objects not generally authorized to access; (iii) changing passwords; (iv) easy password settings.	In terms of problems, it was noted that the security template still needed a lot of work related to user rights and object privileges – this was however expected given the initial installation. The security event log capture an extremely large number of events, with specific reference to the Kerberos authentication and tickets. These are not valuable for current analysis in such large number of event recordings.	The application of a security template is only a portion, however critical, in the overall scheme of security and access to system resources. In addition, although event logs may be useful, too much information captured may results in critical entries being over looked due to the volume of data.
Selected proficient hacking users were asked to see if they could break into the system.	Access to the system was obtained fairly easily based on the following: the naming convention of user accounts were well known, i.e. first letter of first name, followed by first five (5) letters of last name. Initial passwords were set the same as the user name.	A new policy was introduced for setting initial and reset passwords, i.e. intelligent derived password communicated personally to user. The password would expire should the user not log on within 2 days. In addition, the password must be changed at first logon.
Oracle application users were requested to perform their assignment as they would normally do, but notify where security settings were affecting there work either positive or negative.	Not problems were noted during this test. However, users did especially appreciate the automatic session disconnections. Initially, negative responses were received regarding the fact that work was not saved on a timely basis.	Awareness notifications were issued regarding the possible effect of security settings on applications.

For more specific testing a closer look at the *Microsoft Windows 2000 Server Resource Kit* CD-ROM[12] is recommended. The following are a few helpful tools included:

Tool	Description
Appsec.exe (Application Security)	Restrict access of users to predefined applications on the network
Dumpel.exe (Dump Event Log)	Dump event log for a local or remote system into a tab-delimited text file
Gpotool.exe (Group Policy Verification Tool)	Consistency, replication, etc. checking
Auditpol.exe (Audit Policy)	Enables user to modify the audit policy of the local computer or any remote computer
Gpresult.exe (Group Policy Result)	Displays information about the result that Group Policy had on the current computer and logged-on user
Klist.exe (Kerberos List)	Enable viewing and deleting of Kerberos tickets granted to the current logon session

[12] Microsoft Corporation, Microsoft Windows 2000 Server Resource Kit, Microsoft Corporation, 2000.

Security Template Effectiveness Evaluation

Strengths and Weaknesses

The following table is a summary of the strengths and weaknesses relative to enterprise resource system server security under review. An explanation of the reasoning behind the change to the default setting is given.

Security Configuration Tool Set Title	Default Setting (Secure DC)	Too Strong	Too Weak	Custom Environment Setting	Strength/ Weakness Explanation
Account Policies - Password Policy					
Enforce password history	24 passwords remembered	X		12 passwords remembered	The initial setting may be too extensive for some user who would like to standardize passwords on their various systems. This would not indicate a weakness in the default template, but only a convenience adjustment for the system under review.
Maximum password age	42 days		X	30 days	This may indicate somewhat of a weakness n the default template, in that 30 days may lean more to an acceptable industry standard.
Minimum password age	2 days	X		1 day	Would like users to change there passwords sooner, should they expect a breach/disclosure of their password.
Minimum password length	8 characters	X		6 characters	Given the type and level of users in the ERP system environment, 8 characters may seem fairly strict, that may result in passwords being forgotten, resulting in additional administration.
Account Policies - Account Lockout Policy					
Account lockout threshold	5 invalid logon attempts		X	3 invalid logon attempts	

Security Configuration Tool Set Title	Default Setting (Secure DC)	Too Strong	Too Weak	Custom Environment Setting	Strength/ Weakness Explanation
Account Policies - Kerberos Policy					
Enforce user logon restrictions	Not defined		X	Enabled	One of the design goals of Windows 2000 is to enable administrators to turn off NTLM authentication once all network clients are capable of Kerberos authentication. The Kerberos protocol is more flexible and efficient than NTLM, and more secure. The benefits gained by using Kerberos authentication are:[13] 1. Faster connections 2. Mutual Authentication 3. Delegated Authentication 4. Simplified trust management 5. Interoperability
Maximum lifetime for service tickets	Not defined		X	600 minutes	
Maximum lifetime for user ticket	Not defined		X	10 hours	
Maximum lifetime for user ticket renewal	Not defined		X	10 days	
Maximum tolerance for computer clock synchronization	Not defined		X	20 minutes	
Local Policies - Security Options					
Do not display last username in logon screen	Disabled		X	Enable	In that multiple users would share a terminal in an ERP environment, e.g. in a manufacturing plant during different shifts, it was decided to not display the last username in the logon screen.

Impact on Applications and System Operations

Based on the tests performed by the users above as well as with reference to technical documentation, it is concluded that the template does not adversely affect the Oracle Applications as well as other local workstation installed application software.

It should however be noted that a few users did report that their productivity may be impaired as a result of the changes, given that the security policies are now more strict. This issue was resolved through awareness of the criticality and confidentiality of data being manipulated and stored.

[13] Microsoft Corporation, Windows 2000 Kerberos Authentication (1999), op. cit.

Opportunities for Improvement

Managing Multiple Systems in the Enterprise Environment

Since we are working with a multi-domain environment, the concept of Windows 2000 Domains and AD Replication need further elaboration. A domain is a Windows 2000 directory partition and a domain have at least one domain controller. In turn, AD consists of at least one domain. Each domain defines a security boundary, i.e. security policies and settings do not cross domains[14]. However, all of a domain's domain controllers can receive changes made to objects and can replicate those changes to all other domain controllers in the domain.

In the system selected for the study, there are two domains associated with one domain controller, taking into account that each of the domains stores only the information about the objects located in that domain.

How does this affect the security policy changes and the way we manage the enterprise security?

1. If consistency is required in the security policy settings between domains, consideration should be given to having one domain with two computers

2. Pinpoint delegation of administrative authority over the domains.

In Windows 2000 delegation of administrative authority can be defined granularly for both operating units ("OU") and domains.

These concepts is a starting point in designing and appropriate management policy for multiple systems in the enterprise environment.

Further Research and Template Improvements

It is important not to understand that the selection, updating and application of a security template is only one component in the overall Windows 2000 security model and subsystems. Active Directory is fundamental in that it stores all the security policy information. The primary security principles of Windows 2000 servers are:[15]

- Authenticating users and computers
- Administering security principles
- Allowing or denying access to domain resources
- Auditing actions performed with user accounts and computer accounts.

[14] Internet Security Systems (2000), op. cit., p. 106-107

[15] Ibid., p. 62.

However, the security policy, that is based on a security template in this study, contains granular detail that need to be revised and updated as the environment changes. The following are best practices in improving the template on an ongoing basis:

- Monitor events to determine whether trends exist. This could indicate problems that may be resolved by revising a security setting in the template and policy.
- Always test changes the GPO in a test environment prior to promoting into production.
- Be diligent in applying Service Pack and hotfix updates on a regular and consistent basis
- Obtain an objective opinion of the security settings
- Ensure that there is a balance between security and performance

In conclusion therefore, do not accept a setting as a given, but obtain the knowledge and skills to understand the impact of each setting.

References

Brag, Roberta, Windows 2000 Security, New Riders Publishing, 2000

Internet Security Systems, Inc., Microsoft Windows 2000 Security Technical Reference, Microsoft Press, 2000

Julie M. Haney, Guide to Securing Microsoft Windows 2000 Group Policy, National Security Evaluations and Tools Division of the System and Network Attack Center (SNAC), National Security Agency, 2001

Microsoft Corporation, Microsoft Windows 2000 Server Resource Kit, Microsoft Corporation, 2000.

Microsoft Corporation, Windows 2000 Datacenter Server White Paper, Microsoft Corporation, 2000, http://www.microsoft.com/windows2000/docs/datacenterserver.doc

Microsoft Corporation, Windows 2000 Kerberos Authentication White Paper, Microsoft Corporation 999, http://www.microsoft.com/TechNet/prodtechnol/windows2000serv/deploy/confeat/kerberos.asp

SANS Institute, Windows 2000: Active Directory and Group Policy, Track 5 – Securing Windows 2000, document version 5.0, 2001

Scambray, Joel, and McClure, Stuart, Hacking Exposed Windows 2000, McGraw-Hill Publishing, 2001

Appendix A – Security Configuration and Analysis Log File *(extracted samples)*

View Log File

11/11/2001 14:41:30
----Analysis engine is initialized successfully.----

----Reading Configuration info...

DELETED FROM APPENDIX – not configured

User Rights analysis completed successfully.

----Reading Configuration info...

----Analyze Group Membership...
DELETED FROM APPENDIX – not configured

Group Membership analysis completed successfully.

----Reading Configuration info...

----Analyze Registry Keys...
DELETED FROM APPENDIX – not configured

Registry keys analysis completed successfully.

----Reading Configuration info...

----Analyze File Security...
Not Configured - C:.

File security analysis completed successfully.

----Analyze General Service Settings...
DELETED FROM APPENDIX – not configured

General Service analysis completed successfully.

----Analyze available attachment engines...
Load attachment LanManServer.
LanManServer: Query configuration information

Attachment engines analysis completed successfully.

----Reading Configuration info...

----Analyze Security Policy...
Mismatch - MinimumPasswordLength.
Mismatch - PasswordHistorySize.
Mismatch - MaximumPasswordAge.
Mismatch - MinimumPasswordAge.
Analyze password information.
Mismatch - LockoutBadCount.
Analyze account lockout information.
Analyze account force logoff information.
Not Configured - NewAdministratorName.
Warning 5: Access is denied.
Error analyzing guest account.
Not Available - SecureSystemPartition.

System Access analysis completed with error.

Not Configured - MaximumLogSize.
Not Configured - AuditLogRetentionPeriod.
Not Configured - RetentionDays.
Not Configured - AuditLogRetentionPeriod.
Not Configured - RetentionDays.
Analyze log settings.
Analyze event audit settings.

Audit/Log analysis completed successfully.
Mismatch - MaxRenewAge.
Mismatch - MaxClockSkew.
Analyze kerberos policy.

Kerberos policy analysis completed successfully.
Analyze machine\software\microsoft\driver signing\policy.
Analyze machine\software\microsoft\non-driver signing\policy.
Analyze machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel.
Analyze machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning.
Analyze machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption.
Analyze machine\software\microsoft\windows\currentversion\policies\system\disablecad.
Analyze machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername.
Analyze machine\software\microsoft\windows\currentversion\policies\system\legalnoticecaption.
Analyze machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext.
Analyze machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon.
Analyze machine\system\currentcontrolset\control\lsa\auditbaseobjects.
Analyze machine\system\currentcontrolset\control\lsa\crashonauditfail.
Analyze machine\system\currentcontrolset\control\lsa\fullprivilegeauditing.
Analyze machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel.
Analyze machine\system\currentcontrolset\control\lsa\restrictanonymous.
Analyze machine\system\currentcontrolset\control\lsa\submitcontrol.
Analyze machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers.
Analyze machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown.
Analyze machine\system\currentcontrolset\control\session manager\protectionmode.
Analyze machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect.
Analyze machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff.
Analyze machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature.
Analyze machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature.
Analyze machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword.
Analyze machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature.
Analyze machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignature.
Analyze machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange.
Analyze machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal.
Analyze machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey.
Analyze machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel.
Analyze machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel.

Registry values analysis completed successfully.

---Analyze available attachment engines...

Attachment engines analysis completed successfully.

---Un-initialize analysis engine...
Warning 5: Access is denied.
Error occurs.

Last Updated: May 23rd, 2017

Upcoming Training

SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 06, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**