Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Securing Windows
GCWN Practical Assignment
v3.1

Option 2

Securing Windows 2000
With Security Templates

Date Prepared: November 13, 2002

Prepared by: Alexander Lopyrev

Summary

This paper describes an attempt to benefit a security template approach to secure Windows 2000 systems in order to use a VPN/IPSec solution to secure wireless communication. As one of the methods to mitigate the risk related to unprotected WLAN communication, it is suggested to connect the user's system this wireless network card into the private network by using VPN server with IPSec enabled.

Based on the role of the systems that could provide a required level of protection, the National Institute of Standards and Technology (NIST) Windows Professional Gold Security Template was selected and discussed in details in the document.

The paper explains all steps involved in process of securing default installation of Windows 2000 system including a patch management, RRAS configuration, template implementation, security assessment and functionality testing.

As result of the testing of the encrypted and authenticated wireless communication, it is proved that suggested configuration will protect against passive eavesdropping, traffic capturing, bandwidth stealing, and wireless packet floods.

Table of Contents

WINDOWS 2000 WIRELESS VPN CLIENT

Introduction

Current development of IEEE 802.11 family of standards demonstrates many of the weaknesses that exist in wireless networking [1]. The approved wireless Ethernet standards use the 2.4-GHz band at data rates up to 11 Mbps (IEEE 802.11b). Some vendors offer various nonstandard implementations with 5-GHz band at data rates up to 108 Mbps (IEEE 802.11a/g). Wired Equivalent Privacy (WEP) protocol used in 802.11b and in later standard 802.11a does not represent any significant increase in security. The key management process is not defined in 802.11b, which leads to, in most implementations, a single WEP key is shared by all Access Points (AP) and clients, and rarely updated. The shared key is manually distributed to users and then input into their client devices. A newer version, 802.11g, uses the Advanced Encryption Standard and is a large improvement for security. But neither version is perfect.
One of the recommendations to improve WEP security is to implement VPN/ IPSec technology over wireless communication.
An attempt to use a VPN/IPSec solution to secure wireless communication between two Windows 2000 system by implementing the National Institute of Standards and Technology (NIST) security templates will be discussed in this assignment.

System Description

Problem definition
A mobile client (or wireless client) with a laptop that has Windows 2000 Professional OS installed requires a secure connection over a wireless network to the Internet and to the file and print shares on the private Local Area Network (LAN). The Internet connection for the private LAN is provided by a DSL modem and is protected from public Internet by a firewall. The LAN consists of numerous different computers that should all be accessible to the mobile client. Computers connected to the private LAN are out of scope for the assignment and will be used only for evaluation and testing purpose. The client either requires the ability to work as a Power User on a standalone laptop or as a regular user connected to private LAN. Selecting the level of the user's privilege as a "Power User" is conditioned by the type of work that the client conducting on regular basis: design of MS Office application on VBA, browsing the Internet and burning CD-ROMs. Due to the security concerns with the WEP protocol, a more secure solution is vital. An acceptable security level could be obtained by implementing a L2TP VPN (virtual private network). At the time of preparing this assignment many commercial wireless access points were available, even integrated with a cable modem or DSL router and firewall. However, a quick analysis has shown that vendors tend to make WAP routers that provide VPN connectivity only for the un-trusted interface. In other words, VPN is provided for clients coming from Internet into the private LAN, not for the clients behind the DSL router/firewall communicating over wireless connection.

---

[1] Intercepting Mobile Communications: The **Insecurity** of **802.11**
http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

Proposed solution

One of the solutions to meet the problem identified is to equip one of the computers connected to LAN with second wireless network card. The wireless card will provide the required wireless connection for the mobile client. This computer will play the role of the wireless access point (WAP or Wireless server) and the VPN Remote Access Server. Routing and Remote Access Service (RRAS) will enable mobile client to gain access to the LAN and the Internet. The security features of RRAS for dial-in VPN connection should supply a required level of authentication and encryption. Since RRAS is available on the Windows 2000 Server and Advanced Server, the WAP computer will be loaded with Windows 2000 Server and configured as a stand-alone server. The Wireless client will be configured to use a VPN dial-in connection and is not limited by the type of OS, it may be either Windows 2000 server or Windows 2000 Professional. However, for purpose of getting experience with the implementation of various security templates, a workstation configuration was chosen.   To simplify further reading, the mobile client's computer will be called as "wireless laptop" and the computer which offers the wireless connection to the LAN will be called as "wireless server".

System configuration

The Wireless Access Point (WAP) that routes and processes incoming traffic at 11 Mbps doesn't need much processing power. Even and old laptop might be chosen to serve this task. The laptop doesn't require a PCI- or ISA-to-PCMCIA adapter, and already has a built-in backup power supply. The laptop also can often be put at the best signal transmission place, in places a desktop might be hard to fit.
The hardware configuration of the computers is represent on the network diagram below:

Figure 1
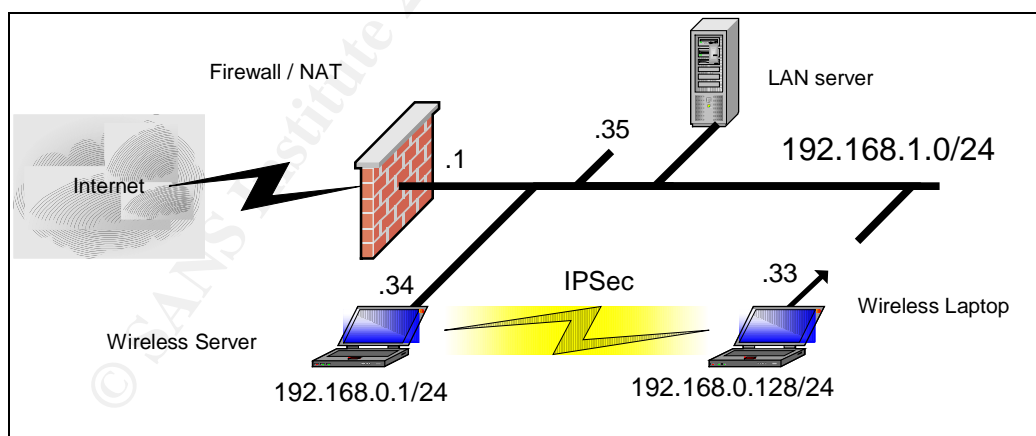
The hardware configuration of the laptops consist of the following:

Wireless server:

- IBM T21 PIII-800
- 256MB RAM
- 20 GB Hard Drive

- CDROM/Floppy
- Generic Ethernet card (IBM)
- IBM High Rate Wireless LAN PC Card with PCI adapter

Wireless laptop:

- IBM T23
- Intel PIII-1.13Ghz
- 640 MB RAM
- 48 GB Hard Drive
- CDROM/Floppy
- On-board Intel(R) PRO/100 VE Network adapter
- High Rate Wireless LAN MiniPCI Combo Card

Hard drives on both laptops are configured with two partitions. The first partition is formatted with NTFS and contains operation system and program files. The second partition is created with the aim to quickly backup/restore an image of an installed operation system. This will save a significant amount of time in case one needed to restore the whole system back to the stable software configuration. The second partition is located at the end of hard drive and has a size of 2GB and is formatted with FAT32. This size is large enough to hold a compressed image of the operation system, applications and tools to be installed on the first NTFS partition. The backup and restore operations of the system image are accomplished using Symantec Ghost v.7 utility using a special bootable floppy diskette.

Windows 2000 installation and Post installation tasks.

Windows 2000 Server and Windows 2000 Professional were installed from the corresponding CD-ROMs by following the standard installation procedure. The system was installed in the C:\WINNT folder in both systems. The Wireless laptop had been requested to also install additional the software package Microsoft Office 2000. Both systems need to be protected with antivirus software. McAfee's VirusScan v4.5.1 SP1was installed on the wireless laptop and the wireless server was loaded with McAfee NetShield Version: 4.5.0 SP1. Post installation tasks were directed to make sure that the lastest service packs were all installed and all new hot fixes were also applied. At the time of writing this paper, the last service pack available from Microsoft was Service Pack 3. After applying service pack SP3 on both laptops the Windows Update feature was used to obtain any other outstanding security updates.
To verify that all current security patches were installed the *hfnetchk* tool from Microsoft was executed. The tool can be downloaded from the Microsoft Web site [2]. The Hot Fix Checker produced a patch level status report for on the system configuration. *Hfnetchk* accomplishes this by referring to an online XML database that's constantly updated by Microsoft. The XML database contains information about patches available for the Windows NT 4.0, Windows 2000, all system services, including IIS 4.0/5.0/5.1, SQL Server 7.0 and 2000, MSDE, and Internet Explorer 5.01 and later.

---

[2] Microsoft Network Security Hotfix Checker (HFNetChk) Version 3.3
http://download.microsoft.com/download/win2000platform/Utility/3.3/NT45/EN-US/Nshc332.exe

The results of **hfnetchk** for the wireless laptop with Windows 2000 Pro are shown in the screenshot (Figure 2).

Figure 2


```
C:\WINNT\system32\CMD.EXE                                          _ □ ×

Scanning BM70001415
.....................................................
Done scanning BM70001415
------------------------------
BM70001415 (192.168.0.15)
------------------------------

        * WINDOWS 2000 SP3

        Note            MS01-022        Q296441
        Note            MS02-053        Q324096
        Note            MS02-064        Q327522

        * INTERNET EXPLORER 5.5 SP2

        Information
        All necessary hotfixes have been applied.


C:\Util\MS_hfnetchk>_
```

Three false/positive messages were generated. Record "MS01-022/Q296441" refers to the Q306460[3] article for a detailed explanation, which is saying that "NOTE" error appears when information about the file or registry setting is not available. These details cannot be stored in the XML file without generating false positives.. Specifically, several Microsoft Office programs include non-vulnerable versions of *"%CommonProgramFiles%\System\Ole DB\Msdaipp.dll"* file that are versioned newer than 8.103.4004. Hfnetchk.exe would interpret this higher version number as a fileversion and checksum mismatch and would report a WARNING message that states that the fileversion was greater than expected.

In this particular case, the file version number was examined in the DLL help database[4] and compared with local file to prove that the version of the file is up to date.

Table 1

FILE INFORMATION:

Name: msdaipp.dll
Description: Microsoft Data Access Component Internet Publishing Provider
Version: 8.103.2402.0
DLLSelfRegister: Yes
TypeLib Guid: {ED222A11-E1C6-11D0-B1E1-00AA006DCDF4}
TypeLib Version: 1.0

PRODUCTS CONTAINING THIS VERSION:

PRODUCT	SIZE	MOD DATE
Access 2000 SR1	573,440	12/2/1999
Office 2000 SR1	573,440	12/2/1999
Office 2000 SR1	573,440	12/2/1999
Small Business Server 2000	573,440	12/2/1999
Windows 2000 SP1	573,440	7/21/2000
Windows 2000 SP2	573,440	5/4/2001

---

[3] Hfnetchk.exe Returns NOTE Messages for Installed Patches
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q306460

[4] DLL Help Database
http://support.microsoft.com/default.aspx?scid=/servicedesks/fileversion/dllinfo.asp&fp=1

Windows 2000 SP3   573,440   7/22/2002

Corresponding NOTE error MS02-053/Q324096 is related to fileversion and checksum mismatch for file
"%CommonProgramFiles%Microsoft Shared\web server extensions\40\bin\fp4Awel.dll".
The version of the file was examined and compared with DLL help database to make sure that the local version of the file is up to date.

The Note message for MS02-064/Q327522[5] is associated to the default permissions provide the Everyone group with Full access (Everyone:F) on the system root folder (typically, drive C). To work around this issue, the permissions for the root directory on the system drive should be reset. The default permissions for Windows XP can serve as a guide for a set of permissions that have been thoroughly designed and tested. The following are the default permissions for the root directory on the system drive for Windows XP:

- Administrators: Full (This Folder, Subfolders, and Files)

- Creators Owners: Full (Subfolders and Files)

- System: Full (This Folder, Subfolders, and Files)

- Everyone: Read and Execute (This Folder Only)

This setting will be used futher in the section Workaround MS02-064/Q327522 when the security template will be discussed.

MS Office 2000 patch level validation.

Due to the nature of work, which is mainly conducted on the wireless laptop, the security of the installed version of MS Office is very important.

To keep MS Office at the current patch level the MS Office service release SR-1a and Service Pack 3 should be installed. [6] After applying the corresponding patches, the installation can be checked using MS Office Product Updates web site[7]. This can be done only if Active Scripting is enabled. So the Internet Explorer Security Setting was modified to allow "Run ActiveX control and plug-ins" only the user's permission has been granted. Downloadable ActiveX Control verifies the contents of MS Office *msi* and *msp* files located in the C:\WINNT\Installer folder and reports any discrepancy between collected data and what is required.

When the update of the MS Office was successfully finished the corresponding web page was displayed (Figure 3)

---

[5] MS02-064: Windows 2000 Default Permissions May Permit Trojan Horse Attack
http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q327522
[6] Office 2000 Update: Service Pack 3 (SP3)
http://office.microsoft.com/downloads/2000/o2ksp3.aspx

[7] MS Office Product Updates
http://office.microsoft.com/ProductUpdates/mainCatalog.aspx

Figure 3
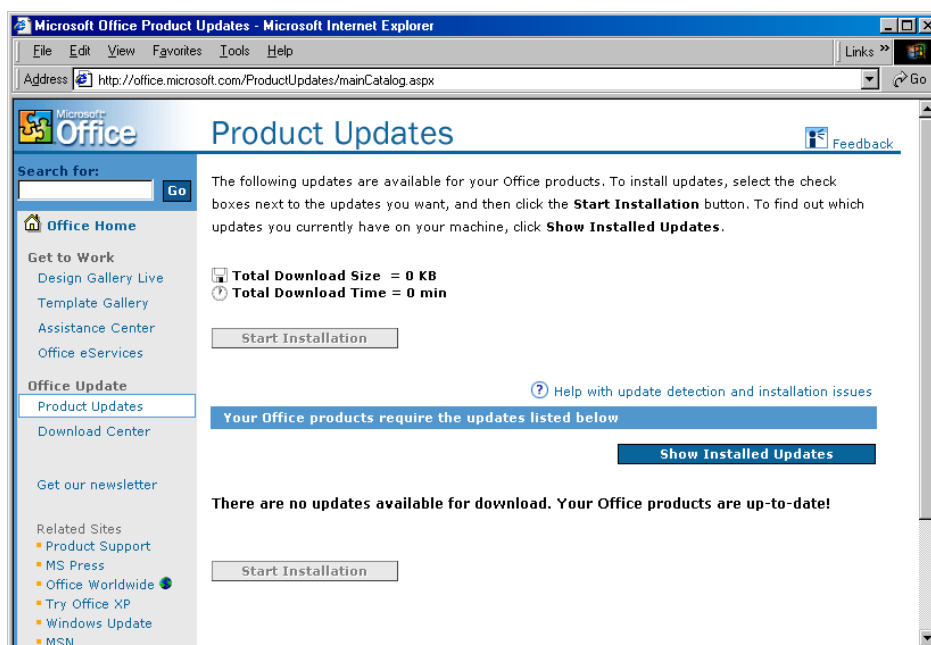
Wireless Network Card Installation.

Wireless Network Cards were installed according to the manufacturers' instructions. The SSID or network name was selected "w_net" for both stations. Also, WEP (Wired Equivalent Privacy) was disabled and both laptops were configured for peer-to-peer communication (AdHoc mode). AdHoc channel set to "10".

Figure 4. Configuration of Wireless Card.
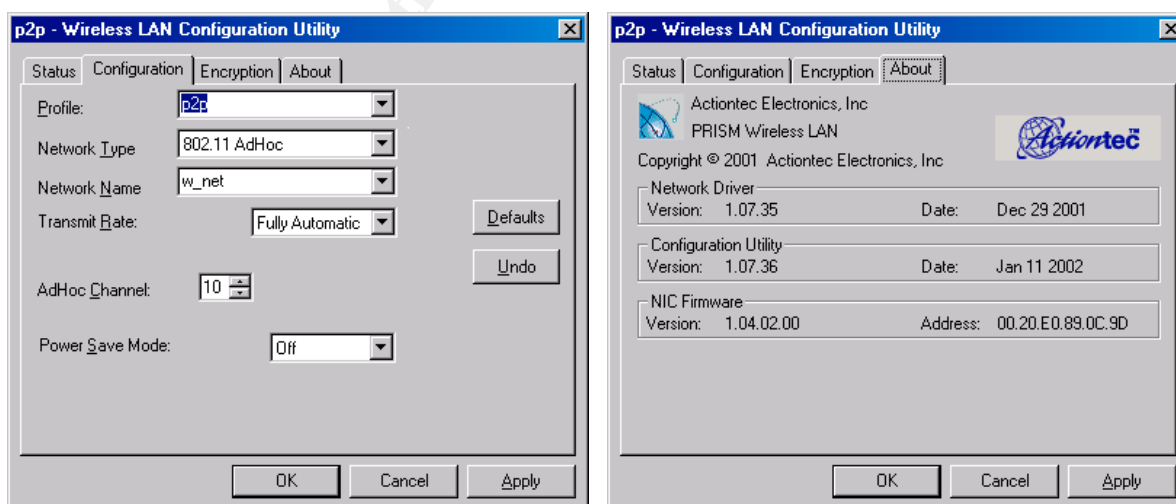
The IP address configurations for the wireless laptop were assigned according to network diagram

```
Ethernet adapter Wireless_laptop:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : High Rate Wireless LAN MiniPCI Combo Card
        Physical Address. . . . . . . . . : 00-20-E0-89-0C-9D
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.0.128
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
        DNS Servers . . . . . . . . . . . :
```

Wireless adapter of the wireless server was assigned static address:

```
Ethernet adapter Wireless_server:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : IBM High Rate Wireless LAN PC Card
        Physical Address. . . . . . . . . : 00-02-2D-3B-5C-44
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.0.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
        DNS Servers . . . . . . . . . . . : 127.0.0.1
```

Gateways were not assigned. This bound traffic between the two laptops only. Any other networks in this case will be unreachable. The second interface of the wireless server was configured for a static IP address; the gateway and DNS addresses were pointed to the firewall.

Initial Configuration of RRAS.

In order to verify initial settings and functionality of the wireless connection, the RRAS server was configured to be a VPN server. It was done by using RRAS configuration wizard "Configure and Enable Routing and Remote Access". In the configuration wizard the option "Virtual private network (VPN) server" was selected, then the protocol TCP/IP for VPN client, "wireless" network was selected as Internet connection that RRAS will use, and IP addresses to be assigned automatically for the clients. On the client side corresponding wizard "Make new connection" from "Network and Dial-up Connection" window created new VPN connection to RRAS server. The IP address of server's wireless card (192.168.0.1) was specified as address of remote VPN server. On the wireless server side, for user "administrator" and wireless_client, the remote access permissions (Dial-in or VPN) were granted to allow access to the network. After all these settings were done, the property of the created VPN connection required modification of advanced security settings to enable maximum strength encryption and MS-CHAPv2. We tested the connection, double-clicking the "Virtual Private Connection" icon, then specifying account information. The simplest way to check connectivity is to verify an ability to browse the internet. All settings were correct, and PPTP connection though wireless link was successfully established.
Configuration of RRAS to remote access server disables any port, listening on wireless interface, except 1723/tcp (PPTP), 500/udp (IPSec), and 1701/udp (L2TP). To make sure that the settings are correct, the simplest *nmap* scan of server's interface though wireless connection was conducted. The result of the scan showed that only 1723/tcp (PPTP) is opened:

```
C:\NMap254b31>nmap.exe -sSU 192.168.0.1 -P0

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap )
Interesting ports on  (192.168.0.1):
(The 3012 ports scanned but not shown below are in state: filtered)
Port       State       Service
1723/tcp   open        pptp

Nmap run completed -- 1 IP address (1 host up) scanned in 726 seconds
```

The similar scan, but targeting client's laptop from wireless server, demonstrated that wireless laptop is listening on standard Windows ports:

```
C:\NMap254b31>nmap.exe -sSU 192.168.0.128

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap )
Interesting ports on (192.168.0.128):
(The 3012 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        loc-srv
135/udp    open        loc-srv
137/udp    open        netbios-ns
138/udp    open        netbios-dgm
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
445/udp    open        microsoft-ds
500/udp    open        isakmp
520/udp    open        route
1025/udp   open        listen
1026/tcp   open        nterm
1030/udp   open        iad1


Nmap run completed -- 1 IP address (1 host up) scanned in 11 seconds
```

Hence, disabling these opened ports on wireless laptop is very important for the sake of securing the wireless communication. NetBIOS ports can be simply disabled by unbinding NetBIOS over TCP/IP. However, it will not solve the problem. Several approaches can be taken to secure wireless network adapter entirely: enabling TCP/IP filtering, installing a personal firewall, or by implementing an IPSec policy. The last solution will be discussed in the section "Configuring of RRAS for L2TP."

Making a backup image.

After the OS installation and initial software update has been completed, the binary image of the bootable NTFS partition was stored on the small second FAT32 partition using Symantec GHOST7. This method allows for a quick restore of the laptop to initial stage in case of unsuccessfully applying a security template or other "hardening" experiments. Resulting system image can then be stored on a CD for future roll back.

Checklist or Template?

Selecting a Template

Security templates are text-based files that include security settings for any or all of the security areas of Windows 2000 policies. Security templates can contain password policies, lockout policies, kerberos policies, audit policies, event log settings, registry values, service startup modes, service permissions, user rights, group membership restrictions, registry permissions and file system permissions.

Windows 2000 includes a set of standard security templates, each appropriate to the role of a computer: The templates range from security settings for "low security" domain clients to "high security" domain controllers. These templates can be used as provided, can be modified, or serve as a basis for creating custom security templates.

At the same time many reputable organization, based on best practice have developed their own security templates (e.g. National Security Agency (NSA), National Institute of Standards and Technology, Computer Security Division (NIST, CSRC), SANS, etc.). Those templates allow for securing Windows system based on various roles, starting from the basic personal workstation to the "high security" domain controller.
Laptop users may be either inside of outside of the office network. They might have unique security requirements and might require elevated privileges to accomplish the same tasks when disconnected from the corporate network.
Based on the role of the wireless laptop and the security requirements the NIST Windows Professional Gold Security Template was selected.
NIST conducted extensive analysis and testing of the NSA settings, substantially extended and refined the NSA template settings, and developed additional template settings. Subsequently, NIST led the development of a consensus baseline of Win2K security settings in collaboration with the public and private sectors; most notably NSA, Defense Information Systems Agency (DISA), the Center for Internet Security (CIS), and the SANS Institute. The consensus settings are reflected in the NISTWin2kProGold.inf security template[8]. Template and Guidance can be downloaded from: http://csrc.nist.gov/itsec/NIST_Win2KPro_R1.2.3.zip

Systems Administration Guidance for Windows 2000 Professional document and security templates, version R1.2.3.

The NIST Windows 2000 Professional Security Templates are text-based configuration files that specify values for security-relevant system settings. The security templates modify several key policy areas of a Windows 2000 Professional system. The policy areas include password policy, account lockout policy, auditing policy, user rights assignment; system security options, event log policy, system service settings, and file permissions.

As part of GIAC practical repository.

Security Template

The following sections contain descriptions of the settings provided by the
NISTWin2kProGold.inf security template[8]

Account Policies

These policies cover areas of security regarding users and their accounts. Account
Policies include the following areas:

- **Password Policy.** This policy includes restrictions on password length age
  uniqueness, requirements for users to use complex passwords and prevent the
  reuse of passwords, or variants of simple passwords.

Table 2. NIST Security Template. Password Policy

Password Policy	Template Settings	Comments
Enforce password history	24	Number of passwords remembered
Maximum password age	90 days	Reduce the maximum number of days before users must change passwords for compliance with local security policy.
Minimum password age	1 day	
Minimum password length	8 characters	Increase the minimum password length for compliance with local security policy and greater security.
Passwords must meet complexity requirements	Enabled	Enforce password complexity
Store password using reversible encryption for all users in the domain	Disabled	If enabled, the passwords are stored on the system in clear text versions; this setting should never be enabled.

- **Account Lockout Policy**. This policy gives the rules on Account Lockout, including
  duration, reset by time or administrator, users' accounts to lock out after a certain
  number of failed logon attempts, and the duration of lockout.

Table 3. NIST Security Template. Account Lockout Policy

Account Lockout Policy	Template Settings	Comments
Account lockout duration	15 minutes	Modify the account lockout settings for compliance with local security policy..
Account lockout threshold	3 invalid logon attempts	Increase this parameter to a higher value before a vulnerability scan is performed.
Reset account lockout counter after	15 minutes	

Security template .inf file in [System Access] section contains additional parameters that do not appear in the GUI interface:

Table 4. NIST Security Template. Account Lockout Policy

Account Logon Policy	Template Settings	Comments
Require logon to change the password	Enabled	This parameter required that the users be logged on a system before they can change their password.
Force Logoff When Hour Expire	Enabled	This parameters force user to logoff when permitted hours expire
Clear Text Password	Disabled	Disable saving a password as clear text.

RequireLogonToChangePassword = 1
ForceLogoffWhenHourExpire = 1
ClearTextPassword = 0

- **Kerberos Policy.** This policy governs the security settings for Kerberos authentication, such as settings for Kerberos ticket lifetimes. The NIST Windows Professional Gold Security Template does not define Kerberos policy.

Local Policies

The Local Policies area of the template defines the policies for the system auditing policy and user rights assignment:

- **Audit Policy.** Windows 2000 can record a variety of security events ranging from system-wide events to local file access. This area contains the overall audit policy settings. Specific audit settings are configured in other areas.

Table 5. NIST Security Template. Audit Policy

Audit Policy	Template Settings	Comments
Audit account logon events	Success, Failure	
Audit account management	Success, Failure	
Audit directory service access	Not defined	Not defined in NIST template. Track access to an Active Directory object.
Audit logon events	Success, Failure	
Audit object access	Failure	Determines whether to audit the event of a user accessing an object (e.g., a file, folder, registry key, or printer) that has its own system access control list (SACL) specified.
Audit policy change	Failure	Determines whether to audit every incidence of a failed attempt to change user rights assignment policies, audit policies, or trust policies. Adding success to this setting will increase not only log entries, but also the system activity tracking capability.
Audit privilege use	Failure	Note that it is likely to generate a very large number of events.
Audit process tracking	Not defined	Not defined in NIST template. May be used for an troubleshooting purpose.
Audit system events	Success, Failure	

- **User Rights Assignment.** These settings specify rights for user accounts and security groups, including the rights for users and groups to perform a variety of

security-related tasks[9]. The content in the Table 6 is a reference between Security policy setting for User Right Assignment and the actual NT user right. This table is useful if it is require to convert a legacy batch scripts that use the Resource Kit's command-line utility NTRIGHTS.EXE, for granting or revoking a Windows NT right to or from a user or group of users.

Table 6. Security Template User Rights and NT user rights

User Right Assignment	NT user rights
Access this computer from the network	SeNetworkLogonRight
Act as part oi the operating system	SeTcbPrivilege
Add workstations to domain	SeMachineAccountPrivilege
Back up files and directories	SeBackupPrivilege
Bypass traverse checking	SeChangeNotifyPrivilege
Change the system time	SeSystemtimePrivilege
Create a pagefile	SeCreatePagefilePrivilege
Create a token object	SeCreateTokenPrivilege
Create permanent shared objects	SeCreatePermanentPrivilege
Debug programs	SeDebugPrivilege
Deny access to this computer from the network	SeDenyNetworkLogonRight
Deny logon as a batch |ob	SeDenyBatchLogonRight
Deny logon as a service	SeDenyServiceLogonRight
Deny logon locally	SeDenyInteractiveLogonRight
Enable computer and user accounts to be trusted for delegation	SeEnableDelegationPrivilege
Force shutdown from a remote system	SeRemoteShutdownPrivilege
Generate security audits	SeAuditPrivilege
Increase quotas	SeIncreaseQuotaPrivilege
Increase scheduling priority	SeIncreaseBasePriorityPrivilege
Load and unload device drivers	SeLoadDriverPrivilege
Lock pages in memory	SeLockMemoryPrivilege
Log on as a batch |ob	SeBatchLogonRight
Log on as a service	SeServiceLogonRight
Log on locally	SeInteractiveLogonRight
Manage auditing and security log	SeSecurityPrivilege
Modify firmware environment values	SeSystemEnvironmentPrivilege
Profile single process	SeProfileSingleProcessPrivilege
Profile system performance	SeSystemProfilePrivilege
Remove computer from docking station	SeUndockPrivilege
Replace a process level token	SeAssignPrimaryTokenPrivilege
Restore files and directories	SeRestorePrivilege

---

[9] Windows 2000 Common Criteria Secure Configuration Guide. Appendix C - User Rights and Privileges.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCSCG/W2kSC
Gcc.asp

User Right Assignment	NT user rights
Shut down the system	SeShutdownPrivilege
Synchronize directory service data	SeSyncAgentPrivilege
Take ownership of files or other objects	SeTakeOwnershipPrivilege

Table 7. NIST Security Template. User Rights Assigment

. User Rights Assignment	Template Settings	Comments
Access this computer from the network	**User, Administrators**	Users and administrators will be removed from this setting hence the local workstations do not share files, folders, or printers and if remote administration is not desired. Administrator needs to be able access this computer from network in order to conduct Vulnerability Assessment.
Act as part of the operating system	None	
Add workstations to domain	None	
Back up files and directories	Administrators **Power Users**	Power users will be added as required by the laptop user.
Bypass traverse checking	Users	
Change the system time	Administrators **Power Users**	Power users will be added as required by the laptop user.
Create a pagefile	Administrators	
Create a token object	None	
Create permanent shared objects	None	
Debug programs	None	
Deny access to this computer from the network	Guests	
Deny logon as a batch job	None	
Deny logon as a service	None	
Deny logon locally	None	
Enable computer and user accounts to be trusted for delegation	None	
Force shutdown from a remote system	Administrators	
Generate security audits	None	
Increase quotas	Administrators	
Increase scheduling priority	Administrators	
Load and unload device drivers	Administrators	
Lock pages in memory	None	
Log on as a batch job	None	
Log on as a service	None	
Log on locally	Users, Administrators	
Manage auditing and security log	Administrators **Power Users**	Power users will be added as required by the laptop user.
Modify firmware environment values	Administrators	
Profile single process	Administrators	
Profile system performance	Administrators	

. User Rights Assignment	Template Settings	Comments
Remove computer from docking station	Users, Administrators	
Replace a process level token	None	
Restore files and directories	Administrators **Power Users**	Power users will be added as required by the laptop user.
Shut down the system	Users, Administrators	
Synchronize directory service data	None	
Take ownership of files or other objects	Administrators	

- **Security Options**. A wide range of security options are controlled via specific registry keys and govern such diverse issues as the welcome dialog message, Server Message Block signing, and the right to eject removable NTFS-formatted media.

Table 8. NIST Security Template. Security Options

Security Options	Template Settings	Comments
Additional restrictions for anonymous connections	No access without explicit anonymous permissions	This settings requires that "Anonymous" should be given explicit permissions to access resources. This is the best option for standalone workstation. .
Allow server operators to schedule tasks (domain controllers only)	Not defined	N/A
Allow system to be shut down without having to log on	Disabled	Requires user to logon in order to shutdown.
Allowed to eject removable NTFS media	Administrators and Power Users	Modified to allow laptop user to eject removable NTFS hard drive
Amount of idle time required before disconnecting session	30 minutes	Reduction of this setting increases the number of times that transmission of credentials occurs across the network and increases network traffic. In some cases, users are required to manually log in after disconnection from a session.
Audit the access of global system objects	Disabled	If enabled, it causes system objects to be created with a default SACL. If the <u>Audit object access</u> audit policy is also enabled, access to these system objects is audited. Enabling this setting greatly increases log entries and cause the log file to fill rapidly.
Audit use of Backup and Restore privilege	Disabled	Enabling this option will generate many log events and cause the log file to fill rapidly.
Automatically log off users when logon time expires	Enabled	
Automatically log off users when logon time expires (local)	Enabled	
Clear virtual memory pagefile when system shuts down	Enabled	The virtual memory pagefile stores information accessed during a users session. The pagefile can contain potentially sensitive data. This setting is important for laptop users.
Digitally sign client communication (always)	Not defined	
Digitally sign client communication (when possible)	Enabled	

Security Options	Template Settings	Comments
Digitally sign server communication (always)	Not defined	
Digitally sign server communication (when possible)	Enabled	
Disable CTRL+ALT+DEL requirement for logon	Disabled	
Do not display last user name in logon screen	Enabled	Enabled to prevent unveiling of a last logged user name.
LAN Manager (LM) Authentication Level	Send NTLMv2 response only	Clients use NTLMv2 authentication only, and use NTLMv2 session security if server supports it. Using this setting will allow secure challenge/response authentication
Message text for users attempting to log on	NIST/DOJ Warning message [10]	
Message title for users attempting to log on	--- WARNING ---	
Number of previous logons to cache (in case domain controller is not available)	1 logon	One logon is cached for each user logging on to the system. This situation allows users to log into domain accounts, even if the domain controller is offline. The caching of credentials on the local workstation presents a slight risk, but adds increased availability of services. Change to a higher value for a portable system that may be disconnected from the domain for an extended period of time.
Prevent system maintenance of computer account password	Disabled	
Prevent users from installing printer drivers	Enabled	Printer drivers can be potentially Trojaned by an attacker; enabling this setting allows administrators control over the verification and installation of printer drivers.
Prompt user to change password before expiration	14 days	
Recovery Console: Allow automatic administrative logon	Disabled	
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled	
Rename administrator account	Not defined	Will leave as is.
Rename guest account	Not defined	Will leave as is.
Restrict CD-ROM access to locally logged-on user only	Enabled	If the users try to install software from a CD-ROM drive and the installation packages use the Microsoft Installer (.MSI) packages, the installation will fail because the software is actually installed by the Windows Installer service. It is recommended that the users copy the installation packages to a network or local drive for the installation procedure to

10 NIST recommended DOJ logon banner:

This system is for the use by authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.

In the course of monitoring individuals who are improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Security Options	Template Settings	Comments
		succeed.
Restrict floppy access to locally logged-on user only	Enabled	
Secure channel: Digitally encrypt or sign secure channel data (always)	Not defined	Can be omitted hence the using of IPSec is assumed.
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	Can be omitted hence the using of IPSec is assumed.
Secure channel: Digitally sign secure channel data (when possible)	Enabled	Can be omitted hence the using of IPSec is assumed.
Secure channel: Require strong (Windows 2000 or later) session key	Not defined	Can be omitted hence the using of IPSec is assumed. 2000.
Secure system partition (for reduced instruction set computer (RISC) platforms only)	Not defined	N/A
Send unencrypted password to connect to third-party SMB servers	Disabled	
Shut down system immediately if unable to log security audits	Not defined	Enable this setting in a high security risk environment.
Smart card removal behavior	Lock workstation	In case the laptop user ready to use smart card logon.
Strengthen default permissions of global system objects (e.g., symbolic links)	Enabled	If enabled, the default DACL is stronger, allowing non-admin users to read shared objects, but not modify shared objects that they did not create.
Unsigned driver installation behavior	Warn but allow installation	The system prompts administrative group members to click on the confirmation dialog box to proceed. Members of the users' group do not have the right to install the drivers.
Unsigned non-driver installation behavior	Warn but allow installation	The system prompts the administrative group members to click on the confirmation dialog box to proceed. Members of the users' group do not have the right to install the nondrivers.

Event Log Policy Settings

These settings govern the configuration of the event logs, including settings such as maximum log size and log overwriting policy.

Table 9. NIST Security Template. Event Log Policy.

Event Log Policy	Template Settings	Comments
Maximum application log size	80 MB	Increase or decrease the log size to comply with local logging policy and installed hardware limitations.
Maximum security log size	80 MB	Increase or decrease the log size to comply with local logging policy and installed hardware limitations. Be aware that if the log file is filled, a users' group member will be unable to log on and only an administrator will be able to reset the system.
Maximum system log size	80 MB	Increase or decrease the log size to comply with local logging policy and installed

Event Log Policy	Template Settings	Comments
		hardware limitations.
Restrict guest access to application log	Enabled	If this policy is enabled, guests are prevented from access to the application event log
Restrict guest access to security log	Enabled	If this policy is enabled, guests are prevented from access to the application event log
Restrict guest access to system log	Enabled	If this policy is enabled, guests are prevented from access to the application event log
Retain application log	Not defined	Determines how long the application log should be retained before will be overwritten.
Retain security log	Not defined	Determines how long the security log should be retained before will be overwritten.
Retain system log	Not defined	Determines how long the system log should be retained before will be overwritten.
Retention method for application log	Overwrite events as needed	
Retention method for security log	Overwrite events as needed	
Retention method for system log	Overwrite events as needed	
Shut down the computer when the security audit log is full	Not Defined	Enable this setting in a high security risk environment.

Restricted Groups

Restricted Groups allows administrators to control who should and should not belong to a given group. When a restricted group policy is applied to a system, only the restricted groups that are local to that machine will be configured.

Table 10. NIST Security Template. Restricted Group.

Restricted Groups. Template Settings .	Actual Settings	Comments
Power Users	Members: *wireless_client*	NIST Security template requires set the Restricted Groups to Power Users. This will remove all users from the Power Users group unless they are manually entered into the inf file.

This setting ensures that the only *wireless_client* is allowed to be a member of the Power Users group. When policy is refreshed, only *wireless_client* will remain as members of the Power Users group.

System Services

These settings control the startup mode for each service (auto, manual, or disabled), together with the level of access available to users. This feature defines whether a user can start, stop, pause, or delete a service, or is restricted to read or write access only. It is possible also increase audit levels for the services to aid in detecting intruders. The recommended NIST method of starting various System Services is listed below. The following table lists the services that need to be modified in the template. Disabling the services or modifying service permissions tend to disturb the functionality of laptop user's applications, hence any changes should be tested before deployment.

Table 11. NIST Security Templates. Modified System Services.

Service Name	Template Settings	Comments
Alerter	Disabled	
ClipBook	Disabled	
Computer Browser	Disabled	Disabling the service prevents the user from browsing the network neighborhood.
Fax Service	Disabled	
FTP Publishing Service	Disabled	
IIS Admin Service	Disabled	
Internet Connection Sharing	Disabled	
IPsec Policy Agent	Not defined/ **ENABLED/Automatic/ Administrators/Full Control**	Should be enabled in order to use IPSec
Messenger	Not defined	Disabling the service prevents the user from receiving administrative alerts.
MSSQLServer	Not defined	Disable and uninstall the MS SQL server if it is not required.
NetMeeting Remote Desktop Sharing	Disabled	
Remote Registry Service	Disabled **ENABLED/Manual/ Administrators/Full Control**	Disabling this service may break some remote administration tools, so test before full-scale deployment. The MBSA tool will not work if the service is disabled. Administrator should have permission to start service in order to run MBSA.
Routing and Remote Access	Disabled/ **ENABLED**	Should be enabled in order to use RRAS
Simple Mail Transport Protocol (SMTP)	Disabled	
SNMP Service	Disabled	
SNMP Trap	Disabled	
SQL Server Agent	Not defined	Disable and uninstall the MS SQL server agent if it is not required.
Task Scheduler	Not defined	Restrict Users and System access to the AT.EXE program.
Telnet	Disabled	
World Wide Web Publishing Services	Disabled	

Registry Permissions.

This feature allows configuring the permissions granted to registry keys. It can also specify the types of accesses for which auditing is desired. These values are designed to enhance the security of the operating system.

Comments inside of NIST Security Template are saying that the Registry section is inherited from the Microsoft template *hisecws.inf.* However, some permission to the registry keys was modified to enhance security. It also includes the Netscape Communicator specific registry settings. Template revokes the full control permission from those registry records for build-in users (BU).

File System.

This feature allows configuration of the permissions granted to file system objects (folders, subfolders, and files); it can also specify the types of accesses for which auditing is desired.

NIST Security Template modifies permissions and the way in which permissions propagate. These changes are summarized in the following tables:

Table 12. NIST Template. File Permissions.

File/Folder	Permissions	Access/Inheritance	
	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Admin	System
		Full Control (this folder only)	Full Control (this folder only)
%SystemDrive%\MSDOS.SYS	X	X	X
%SystemDrive%\IO.SYS	X	X	X
c:\config.sys	X	X	X
c:\autoexec.bat	X	X	X
c:\ntbootdd.sys	X	X	X
c:\ntdetect.com	X	X	X
c:\boot.ini	X	X	X
c:\ntldr	X	X	X
%SystemDrive%\autoexec.bat	X	X	X
%SystemDrive%\config.sys	X	X	X

Special permissions assigned to the tack scheduler executable file.

Table 13. NIST Template. File Permissions

File/Folder	Permissions	Access/Inheritance
	Do not allow permissions on this file or folder to be replaced	Local Administrator
%SystemRoot%\system32\at.exe	X	Full Control (this folder, subfolders, and files)

Table 14. NIST Template. File Permissions

File/Folder	Permissions	Access/Inheritance	
	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Admin	System
		Full Control (this folder, subfolders, and files)	Full Control (this folder, subfolders, and files)
%SystemRoot%\system32\secedit.exe	X	X	X
%SystemRoot%\system32\regedt32.exe	X	X	X
%SystemRoot%\system32\rsh.exe	X	X	X

File/Folder	Permissions	Access/Inheritance	
	Configure this file or folder; then, replace existing permissions on all subfolders and files with inheritable permissions	Admin Full Control (this folder, subfolders, and files)	System Full Control (this folder, subfolders, and files)
%SystemRoot%\system32\rexec.exe	X	X	X
%SystemRoot%\system32\Ntbackup.exe	X	X	X
%SystemRoot%\system32\rcp.exe	X	X	X
%SystemRoot%\regedit.exe	X	X	X
%SystemDrive%\boot.ini	X	X	X
%SystemDrive%\ntdetect.com	X	X	X
%SystemDrive%\ntbootdd.sys	X	X	X
%SystemRoot%\system32\arp.exe	X	X	X
%SystemRoot%\system32\cacls.exe	X	X	X
%SystemRoot%\system32\debug.exe	X	X	X
%SystemRoot%\system32\edit.com	X	X	X
%SystemRoot%\system32\edlin.exe	X	X	X
%SystemRoot%\system32\finger.exe	X	X	X
%SystemRoot%\system32\ftp.exe	X	X	X
%SystemRoot%\system32\irftp.exe	X	X	X
%SystemRoot%\system32\tftp.exe	X	X	X
%SystemRoot%\system32\xcopy.exe	X	X	X
%SystemRoot%\system32\net.exe	X	X	X
%SystemRoot%\system32\ipconfig.exe	X	X	X
%SystemRoot%\system32\nslookup.exe	X	X	X
%SystemRoot%\system32\telnet.exe	X	X	X
%SystemRoot%\system32\nbtstat.exe	X	X	X
%SystemRoot%\system32\ping.exe	X	X	X
%SystemRoot%\system32\pathping.exe	X	X	X
%SystemRoot%\system32\route.exe	X	X	X
%SystemRoot%\system32\runonce.exe	X	X	X
%SystemRoot%\system32\ipxroute.exe	X	X	X
%SystemRoot%\system32\syskey.exe	X	X	X
%SystemRoot%\system32\tracert.exe	X	X	X
%SystemRoot%\system32\cmd.exe	X	X	X
%SystemRoot%\system32\cscript.exe	X	X	X
%SystemRoot%\system32\regsvr32.exe	X	X	X
%SystemRoot%\system32\runas.exe	X	X	X
%SystemRoot%\system32\netsh.exe	X	X	X
%SystemRoot%\system32\wscript.exe	X	X	X
%SystemRoot%\system32\nwscript.exe	X	X	X
%SystemRoot%\system32\appmgmts.dll	X	X	X

Besides the modification of the executable files, many changes were done on sensitive Windows 2000 NTFS folders. Modifications in the NIST template for folders were very complicated to list here. I have included to put in a table for information related to the affected security groups only. Those groups were: Build-Administrators (BA), System (SY), Build-Users (BU), Creator-Owner (CO), Authenticated Users (AU), and Everyone (WD).

Table 15. NIST Security Template. Folder Permissions.

Folder	BA	SY	BU	CO	AU	WD
%SystemRoot%\system32\GroupPolicy	X	X			X	
%SystemRoot%\system32\NTMSData	X	X				
%SystemRoot%\Debug\UserMode	X	X	X			
%SystemDrive%\Documents and Settings	X	X	X			
%SystemRoot%\system32\Setup	X	X	X			
%SystemRoot%\system32\appmgmt	X	X	X			
%SystemDrive%\Documents and Settings\All Users	X	X	X			
%SystemRoot%\Registration	X	X	X			
%SystemRoot%\debug	X	X	X	X		
%SystemDrive%\	X	X	X	X		X
%SystemRoot%\ReinstallBackups	X	X	X	X		
%SystemRoot%\Offline Web Pages						X
%SystemRoot%\Tasks						
%SystemDrive%\Program Files\Netscape\Users			X			
%SystemRoot%\system32\ias	X	X		X		
%SystemRoot%\system32\dllcache	X	X		X		
%SystemDrive%\Documents and Settings\Administrator	X	X				
%SystemRoot%\config	X	X				
%SystemRoot%\repair	X	X				
%SystemRoot%\CSC	X	X				
%SystemRoot%\$NtServicePackUninstall$	X	X				
%SystemDrive%\ntldr	X	X				
%SystemDrive%\Program Files\Resource Kit	X	X				
%SystemRoot%\ServicePackFiles	X	X				
%SystemDrive%\Documents and Settings\Default User	X	X	X			
%SystemRoot%\security	X	X		X		
%SystemRoot%\Temp	X	X	X	X		
%SystemRoot%\system32\spool\printers	X	X	X	X		
%SystemDrive%\Temp	X	X	X	X		
%SystemRoot%\system32\DTCLog	X	X	X	X		
%SystemRoot%	X	X	X	X		
%ProgramFiles%	X	X	X	X		
%SystemRoot%\system32	X	X	X	X		
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson	X	X	X	X		

NIST Security Template also includes the Netscape Communicator specific files and folders settings:

%SystemDrive%\Program Files\Netscape\Users",2,"D:AR(A;OICI;0x1301bf;;;BU)
%SystemRoot%\nsreg.dat",2,"D:AR(A;OICI;0x1301bf;;;BU)

Registry values

These settings allow you to configure the permissions granted to registry keys. It can also specify the types of accesses for which auditing is desired. The table below explains which additional registry setting will need to be modified when the NIST Security template is applied.

Table 16

Registry Path	Value	Comment
HKLM \SOFTWARE \Microsoft \Command Processor \PathCompletionChar	<TAB>	
HKLM \SOFTWARE \Microsoft \DrWatson \CreateCrashDump	0/Disabled	Enable Crash dump file after an application crash has occurred.
HKLM \SOFTWARE \Microsoft \Windows NT \CurrentVersion \AeDebug \Auto	0/Disabled	Execute the debugger on system crash.
HKLM \Software \Microsoft \Windows NT \CurrentVersion \Winlogon \AutoAdminLogon	0/Disabled	Administrator Auto Logon
HKLM \Software \Microsoft \Windows \CurrentVersion \Policies \Explorer \NoDriveTypeAutoRun	255	Disables Autoplay on all types of drives
HKLM \Software \Microsoft \Windows \CurrentVersion \Policies \Network \HideSharePwds	1/Enable	Hide the password typed when accessing a file share.
HKLM \Software \Microsoft \Windows \CurrentVersion \Policies \Network \NoDialIn	1/Enable	Disable Dial-In Access
HKLM \system \CurrentControlSet \Control \CrashControl \AutoReboot	0/Disabled	If "Blue Screen" occurs, write a crash log file and reboot
HKLM \system \CurrentControlSet \Services \Cdrom \Autorun	0/Disabled	CDROM Autorun
HKLM \system \CurrentControlSet \Services \IPSEC \NoDefaultExempt	1/Enable	Secure Kerberos or RSVP traffic. RSVP and Kerberos are not exempted (only IKE, Multicast, and Broadcast are exempted)
HKLM \system \currentcontrolset \services \lanmanserver \parameters \autodisconnect	30 min	LAN Autodisconnect timeout
HKLM \System \CurrentControlSet \Services \LanmanServer \Parameters \AutoShareWks	0/Disabled	Displaying the administrative shares (c$, d$, admin$, etc.)
HKLM \system \currentcontrolset \services \lanmanserver \parameters \hidden	1/Enable	Determines whether the server's computer name and comment can be viewed by other computers on the domain.
HKLM \system \CurrentControlSet \Services \MrxSmb \Parameters \RefuseReset	1/Enable	Ignore ResetBrowser frames that can shut down Computer Browser Service
HKLM \system \CurrentControlSet \Services \NetBT \Parameters \NoNameReleaseOnDemand1	1/True	Determines whether the computer releases its NetBIOS name when it receives a name-release request.
HKLM \System \CurrentControlSet \Services \Rasman \Parameters	1/Enable	Do not allow modify RAS parameters
HKLM \system \CurrentControlSet \Services \Tcpip \Parameters \DisableIPSourceRouting	2	Disable source routing completely
HKLM \system \CurrentControlSet \Services \Tcpip \Parameters \EnableDeadGWDetect	0/Disable	Allows to perform dead-gateway detection and switch to backup gateway
HKLM \system \CurrentControlSet \Services \Tcpip \Parameters \EnableICMPRedirect	0/False	Determine whether Windows will alter its route table in response to an ICMP redirect message.
HKLM \system \CurrentControlSet \Services \Tcpip	1/Enable	Enable discovering the Maximum

Registry Path	Value	Comment
\Parameters \EnablePMTUDiscovery=4,1		Transmission Unit (MTU or largest packet size) over the path to a remote host. By discovering the Path MTU and limiting TCP segments to this size, TCP can eliminate fragmentation at routers along the path that connect networks with different MTUs.
HKLM \system \CurrentControlSet \Services \Tcpip \Parameters \KeepAliveTime=4,300000	300000 (5 min)	Controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet.
HKLM \system \CurrentControlSet \Services \Tcpip \Parameters \PerformRouterDiscovery=4,0	0/False	Controls whether Windows will try to perform router discovery.
HKLM \system \CurrentControlSet \Services \Tcpip \Parameters \SynAttackProtect=4,2	2/ reduces transmission retries and delays route cache entry, and delay indication to winsock.	Reduce the amount of time the system will wait for SYN-ACKs
HKLM \system \CurrentControlSet \Services \Tcpip \Parameters \TcpMaxHalfOpen=4,100	100	Determines the number of connections in the SYN-RCVD state is allowed before SYN-ATTACK protection begins to operate
HKLM \system \CurrentControlSet \Services \Tcpip \Parameters \TcpMaxHalfOpenRetried=4,80	80	Determines the number of connections in the SYN-RCVD state for which there has been at least one retransmission of the SYN sent before SYN-ATTACK protection begins to operate.
USERS \.DEFAULT \Software \Microsoft \Windows \CurrentVersion \Policies \Explorer \NoDriveTypeAutoRun=4,255	255	Disables Autoplay on all types of drives and propagate this settings for all users.

Using the Security Configuration Manager to customize NIST template. [11]

The Security Configuration Manager (SCM) is a set of tools allows security administrators to define security templates that can be applied to individual machines or any number of machines via group policy.

The set of security settings available via user-friendly GUI interface of the SCM snap-in and corresponding set of registry values can be extended by modifying and then registering the information in the *Sceregvl.inf* file located in the *%windir%\inf* folder. The security relevant registry values, configurable by SCM, appear under *Local Policies\Security Options* when using SCM tools such as the security templates snap-in, the security configuration and analysis snap-in, or the security settings extension to Group Policy.

---

[11] How to Add Custom Registry Settings to Security Configuration Editor
http://support.microsoft.com/default.aspx?scid=kb;en-us;214752

The **Sceregvl.inf** is a text-based configuration file and can be modified by hand. Once the custom modifications to the file has been done, the changes should be registered by issuing the following command:
regsvr32 scecli.dll

Settings for disabling automatic IPSec Policy Injection for L2TP.

The way of customizing SCM UI, described above, can be also used for disabling automatic IPSec policy injection for L2TP. In order to do this, the following modifications should be done in the **Sceregvl.inf** to allow for customization of the RRAS settings in the registry[12]

[Register Registry Values]
; Automatic L2TP policy injection
MACHINE\System\CurrentControlSet\Services\Rasman\Parameters\ProhibitIpSec,4,%Cre
ateDymamicL2TPpolicy%,0|,%DisableDymamicL2TPpolicy%,1

[Strings]
CreateDymamicL2TPpolicy= Enable automatic injection of a dynamic IPSec policy
DisableDymamicL2TPpolicy= Disable automatic injection of a dynamic IPSec policy

These modifications need to be applied on each Windows 2000-based endpoint computers: wireless server and wireless laptop. Then new IPSec policy will be assigned to precisely control the protocols, key length, authentication, and for debugging purpose of VPN L2TP connection.

The results of the modification to the **Sceregvl.inf** file are presented on the Appendix 1.

After disabling the automatic injection of the dynamic IPSec policy the new static IPSec policy should be created instead. The simplest way to automatically assign the L2TP IPSec static policy is to use the batch script where a corresponding policy setting will be specified as parameters for the **ipsecpol** command line tool. The IPSec static policy for wireless communication will be discussed in section "Configuring of RRAS for L2TP."

---

[12] Disabling IPSEC Policy Used with L2TP
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q258261

Figure 5
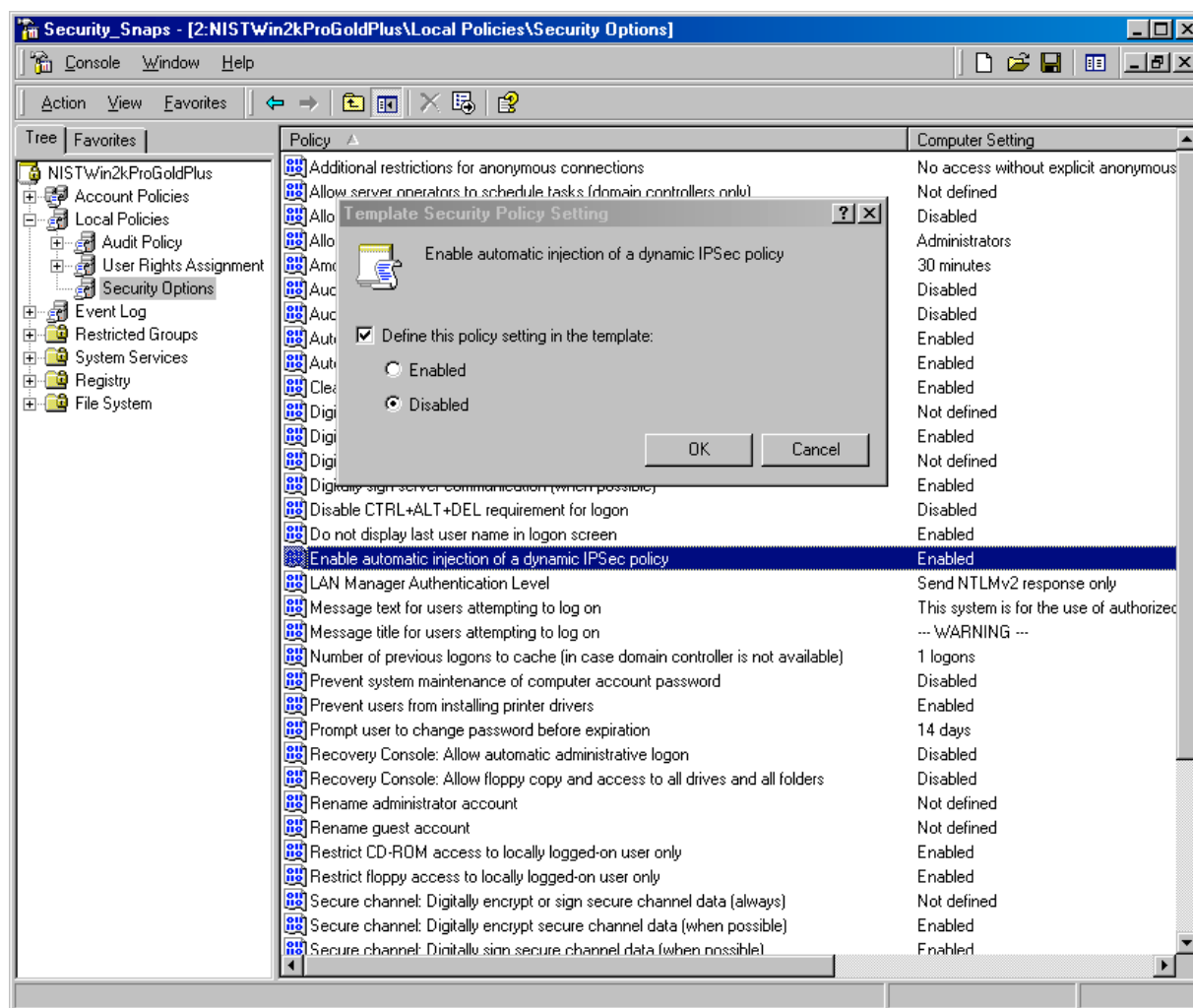
Workaround MS02-064/Q327522

To work around the issue of the insecure default permissions being provide to the Everyone group with Full access (Everyone:F) on the system root folder the following permissions were applied to the %systemdrive% to make the permissions the same as those for Windows XP.

It's recommended in Q327522 to add the following to the [File Security] section of the security template:

[File Security]
"%SystemDrive%\",0,"D:AR(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICIIO;GA;;;CO)
(A;CIOI;GRGX;;;BU)(A;CI;0x00000004;;;BU)(A;CIIO;0x00000002;;;BU)(A;;GRGX;;;WD)"

This string set the permission for the root directory object by modifying **discretionary access control list** (*DACL*)[13]. If an object has a DACL, the system allows only the access that is explicitly allowed by the **access control entries** (*ACEs*) . If there are no ACEs in the DACL, the system does not allow access to anyone. Similarly, if a DACL has ACEs that allow access to a limited set of users or groups, the system implicitly denies access to all trustees not included in the ACEs.

Security templates use the **security descriptor definition language** (*SDDL*)[14] to control access to the various objects. Each record SDDL in the template defines the names of the object, the policy settings parameter, and the object's permission string.
The policy settings parameter defines the way in which the policy will affect security settings for the object

Figure 6

---
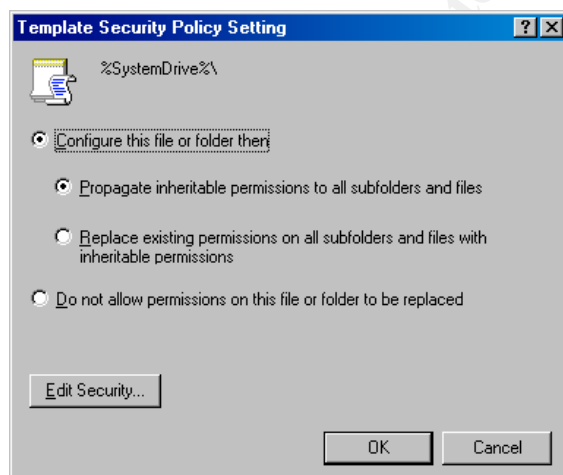
[13] Platform SDK: Security. Security Glossary. DACL
   http://msdn.microsoft.com/library/en-us/security/security/d_gly.asp?FRAME=true
[14] Platform SDK: Security: Security Descriptor Definition Language.
http://msdn.microsoft.com/library/en-us/security/Security/security_descriptor_definition_language.asp

The parameter values are summarized in the Table 17.

Table 17

Policy settings parameter	Template Security Policy Setting
0	Configure this file or folder then Propagate inheritable permissions to all subfolders and files
2	Configure this file or folder then Replace existing permissions on all subfolders and files with inheritable permissions
1	Do not allow permissions on this file or folder to be replaced

The permission string is formatted using DACL **Security Descriptor String Format**[15]**.** The format is a null-terminated string with tokens to indicate each of the four main components of a security descriptor: owner (**O:**), primary group (**G:**), DACL (**D:**), and SACL (**S:**).

```
O:owner_sid
G:group_sid
D:dacl_flags(string_ace1)(string_ace2)... (string_acen)
S:sacl_flags(string_ace1)(string_ace2)... (string_acen)
```

The security descriptor string is enclosed in parentheses. The fields of the ACE are in the following order and are separated by semicolons (;).
```
ace_type;ace_flags;rights;object_guid;inherit_object_guid;account_sid
```
Based on the information provided from Platform SDK, the permission configuration string for the system root folder in the case of the "NOTE MS02-064/Q327522" can be "decrypted" as follows (Table 18):

Table 18

ACE field	ace_type	ace_flags	rights	account_sid (alias)
D:AR	SE_DACL_PRESENT . The SE_DACL_AUTO_INHERIT_REQ flag is set			
(A;OICI;GA;;;BA)	SDDL_ ACCESS_ALLOWED;	OBJECT_ INHERIT_ACE, CONTAINER_ INHERIT_ACE;	GENERIC_ALL;	Built-in administrators
(A;OICI;GA;;;SY)	SDDL_ ACCESS_ALLOWED;	OBJECT_ INHERIT_ACE, CONTAINER_ INHERIT_ACE;	GENERIC_ALL;	Local system

---

[15] Platform SDK: Security: Security Descriptor String Format
 http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/Security/security_descriptor_string_format.asp

ACE field	ace_type	ace_flags	rights	account_sid (alias)
(A;OICIIO;GA;;;CO)	SDDL_ ACCESS_ALLOWED;	OBJECT_ INHERIT_ACE, CONTAINER_ INHERIT_ACE; INHERIT_ONLY_ACE	GENERIC_ALL;	Creator owner
(A;CIOI;GRGX;;;BU)	SDDL_ ACCESS_ALLOWED;	OBJECT_ INHERIT_ACE, CONTAINER_ INHERIT_ACE;	GENERIC_READ, GENERIC_EXECUT E	Built-in users
(A;CI;0x00000004;;;BU)	SDDL_ ACCESS_ALLOWED;	CONTAINER_ INHERIT_ACE;	0x00000004	Built-in users
(A;CIIO;0x00000002;;;BU)	SDDL_ ACCESS_ALLOWED;	CONTAINER_ INHERIT_ACE; OBJECT_ INHERIT_ACE,	0x00000002	Built-in users
(A;;GRGX;;;WD)"	SDDL_ ACCESS_ALLOWED;	-	GENERIC_READ, GENERIC_EXECUT E	Everyone

The substring, that expressed the access rights controlled by the ACE, can be a
hexadecimal string representation of the access rights, such as "0x00000004", or it can be
a concatenation of the different strings. I didn't manage to find a "bit-meaning" of the
hex rights in the table above due to the fact that the SDK documentation doesn't have a
C++ example of the header file **sddl.h** where all bit's definitions should be listed.
Decrypting the meaning of the SDDL to the human language is very a complicated task
and is prone to human mistake. Fortunately, one does not need to know this level of
detail in normal conditions. I've found that manually editing these SDDL access string
templates is the most effective way to manipulate them, especially if it is required for
scripting automation. Advanced administrators should write scripts or code that can
correctly construct SDDL strings.

Security Template for Wireless RAS Server

Configuration of the Wireless Server, intended to play a role of the RRAS VPN server,
has been done by implementing MS predefined security template for the High Secure
Server. All customization discussed above is included in the resulting template. This
section aims to summarize the template settings for the Wireless server.

Predefined Security Templates[16]

Windows 2000 includes several predefined security templates. These are split into two
categories: basic and incremental templates.
- **Basic Templates** specify default Windows 2000 security settings for all security
  areas with the exception of user rights and groups, and are designed to undo
  changes to system security that may result in unwanted system behavior.
    - Basicwk.inf (for computers running Windows 2000 Professional)
    - Basicsv.inf (for computers running Windows 2000 Server)
    - Basicdc.inf (for domain controllers running Windows 2000 Server)
    - OCFiless.inf (for standalone or member servers—not domain control)

---

[16] Microsoft Windows® 2000 Security. Technical Reference / Internet Security System, Inc.
Microsoft Press, 2000, p.299-342

■   OCFilesw.Inf (for computers running Windows 2000 Professional)

User rights and group modifications are not affected, as these are often modified by applications to allow successful execution of the applications by different levels. It is not the intent of the basic templates to undo such changes.

- **Incremental Templates.** Windows 2000 also includes incremental templates to modify default security settings. This means that these templates are intended for machines already running the default security settings. They do not include the default settings plus the modifications.
    - *Compatws.Inf* (for workstations or servers)
    - *Securews.inf* (for workstations and servers)
    - *Securedc.inf* (for domain controllers)
    - *Hisecws.inf* (for workstations and servers)
    - *Hisecdc.inf* (for domain controllers)

For the task of securing the wireless server the template *Hisecws.inf* was selected. The Hisecws.inf template provides increased security over the secure configuration, primarily for parameters that affect network communication protocols. The high-security template also changes the access permissions for the Power User group to be equivalent to that of the Users group. This essentially makes any end users either Users or Administrators.

- **Default Templates.** For sake of the consistency I have included an additional security template's configuration files located in the *%windir%\inf* folder.

Table 19

Template	Comments
%windir%\inf\defltsv.inf	Default Template For Windows 2000 Server. This template should NOT be used on Domain Controllers.
%windir%\inf\defltwk.inf	Default Security Settings. (Windows 2000 Professional)
%windir%\inf\dsup.inf	Security applied to upgraded servers
%windir%\inf\dsupt.inf	Security applied to upgraded terminal servers
%windir%\inf\dwup.inf	Security applied to upgraded workstations
%windir%\repair\secsetup.inf	Installation default security settings

Apply, test and evaluate the template

To configure the Windows 2000 security settings for a standalone system (not connected to the domain structure) , it is possible to use one of these options:

- Security Configuration and Analysis Snap-in (SCA);
- Secedit Command-line Tool.

Both tools allow for achieving the same results but by a using different approach. The GUI based SCA snap-in uses an intuitive user-friendly interface to modify security settings in the database and then uses this database to apply the setting to the system. Command-line Secedit.exe allows one to conduct configuration and analysis without a GUI. All modifications and analysis tasks can be accomplished by using a simple batch file or a script and can be scheduled or initiated remotely with other tools such as remote scripting (WSH starting from version 5.6), WMI, or remote console (rsh, rcmd , rconsole from Resource Kit).

For the task of this assignment, I use a both of these tools. All modifications to the original NIST template *NISTWin2kProGold.inf* and *Securews.inf* have been done by using Security Configuration and Analysis Snap-in. Then the updated templates have been stored as *wireless_wks.inf* and *wireless_srv.inf.* As a finale step, all discussed above adjustments has been applied via batch script from command-line.

Security Configuration Database.

The Security Configuration Engine (SCE) is **database-driven.** Hence, the security template should be imported into a database before the Security Configuration Engine can perform configuration or analysis of a system. The local security policy settings are maintained in the database *%windir%\security\database\ secedit.sdb)* on each Windows 2000 machine. To import and apply the custom security template a new database should be created. This database is used to import initial or basic security template when applying incremental and custom templates. Any modification on the security setting will update the database. These updated settings can then be exported back to the text-based template.

Resetting Security Settings back to default.

After applying security templates that modify the security settings of Discretionary Access Control List (DACL) of various windows objects, is very hard to restore security settings back to their original state for troubleshooting purposes. To reset the operating system back to the original installation default security settings *secsetup.inf* setup security template may be used. This template is located in folder *%windir%\repair*[17]. Article Q313222 recommended using *secedit* command tool to apply this template

secedit /configure /cfg %windir%\repair\secsetup.inf /db secsetup.sdb /verbose

This method to roll back to the initial state has been used during troubleshooting of the security templates together with the backup Ghost image of the initial state of the evaluated system.

---

[17] HOW TO: Reset Security Settings Back to the Defaults
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q313222

Applying Templates.

The steps, which have been taken to create and modify security template, are summarized below:

- Modify Sceregvl.inf template to allow control under L2TP injection registry settings via GUI Security Configuration and Analysis Snap-in and then re-register the new registry values.
- Using text editor modify [File Security] section of the NIST Security template to add permission for the root folder (MS02-064/Q327522)
- Modify the NIST Security template via Security Templates Snap-in and store updated templates as *nist_wireless_wks.inf* and *nist_wireless_srv.inf.*
- Create a new security database *wireless_wks.sdb* and sequently import *Basicwk.inf, Securews.inf* and then *nist_wireless_wks.inf* templates.
- Export resulting template from database as file *wireless_wks.inf .*
- Create new security database *wireless_srv.sdb* and sequently import *Basicsv.inf, Securews.inf* and then *nist_wireless_srv.inf* templates.
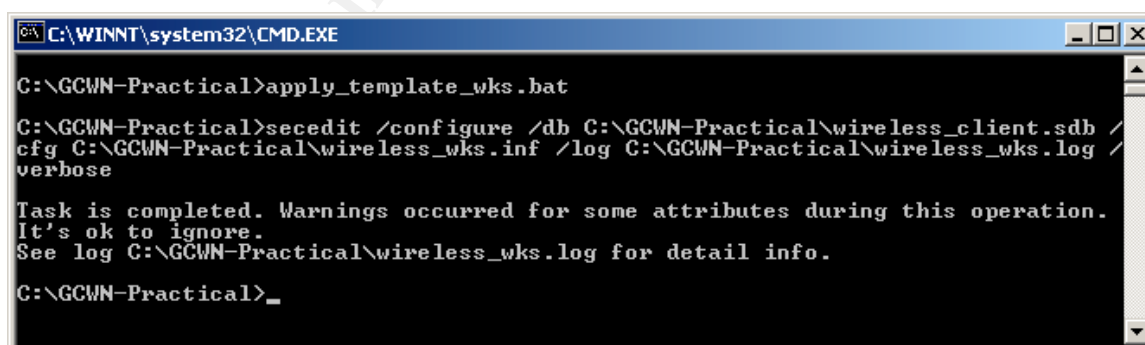- Export resulting template from database as file *wireless_srv.inf .*

After the resulting security templates for both wireless client and wireless server have been created and stored, the Secedit command-line tool was used to configure the system.

The batch command file intended to do this contains the following line:

Secedit /configure /db c:\GCWN-Practilcal\ wireless_wks.sdb
/cfg c:\GCWN-Practilcal\ wireless_wks.inf /log c:\GCWN-Practilcal
wireless_wks.log /verbose

Then the batch file was executed. As result of the successful configuration of the system, the message "Task is complete" appeared on the screen. In order to verify results, the log file has been examined. Errors, discovered in the log file, appeared because some files and registry setting did not exist in the current configuration and they can be ignored. A screenshot of the applying resulting template is presented below:
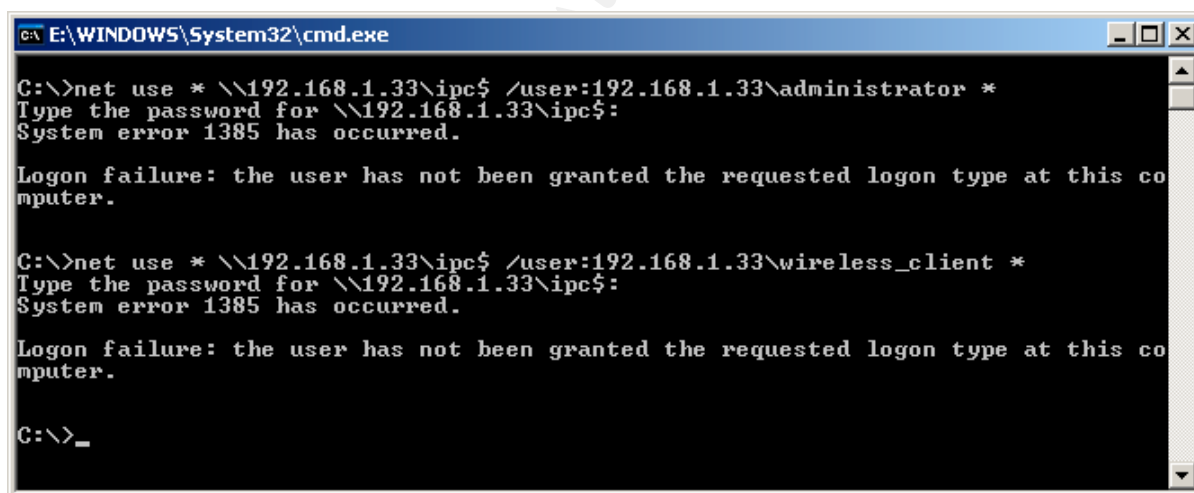
Figure 7

As usual, to ensure that all modified permissions and security setting are applied, it is strictly recommended to reboot the system after applying changes.

Test the template's security settings.

To test the security settings of the system after all discussed above templates have been applied a Vulnerability Assessment (VA) approach has been used. Comprehensive vulnerability assessment tool exists to conduct this kind of testing, investigate possible violations of security policy, and compare the results of the VA before and after the hardening procedures have been applied. Almost all network-based vulnerability assessment tools require authorized administrative access to the "system share" through the Remote Procedure Call (RPC) channel to collect as much information as possible Attempting to connect to the system share remotely is one of the ways to test a template's security settings.

In order to conduct an analysis of the security settings the Ethernet interface was enabled to DHCP mode and the wireless laptop was temporary attached to network. To establish the RPC channel to the wireless laptop the "net use" command was issued on the remote system. The first attempt used the local administrator account and password to connect to IPC$ share. Due to the local policy settings on the wireless laptop, "Access this computer from the network" is disabled (see Table 7) and this attempt failed. On the second attempt the local wireless_client account also failed. The screenshot of these attempts and corresponding messages from the security log file are presented below:

Figure 8

Figure 9
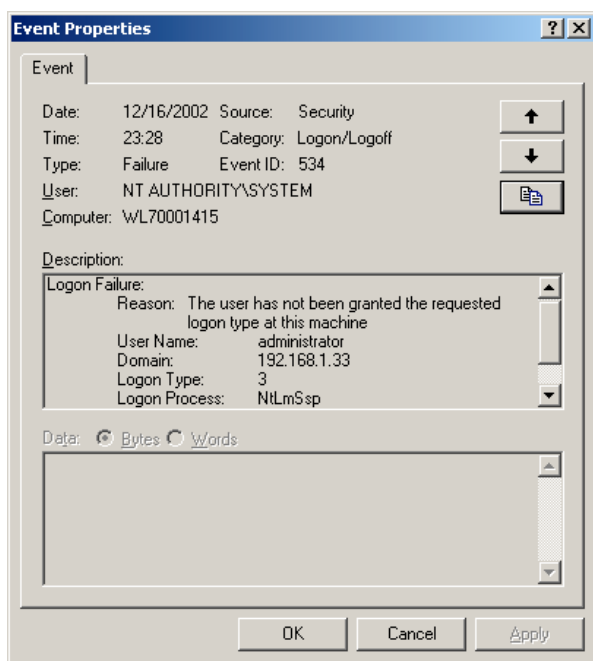
To test how the security permissions, specified in the custom template, affected the access to the system root folder and files, an attempt to open *c:\boot.ini* was conducted. The screenshot below is showing that the attempt to rename the *boot.ini* file failed for the wireless_client.

Figure 10
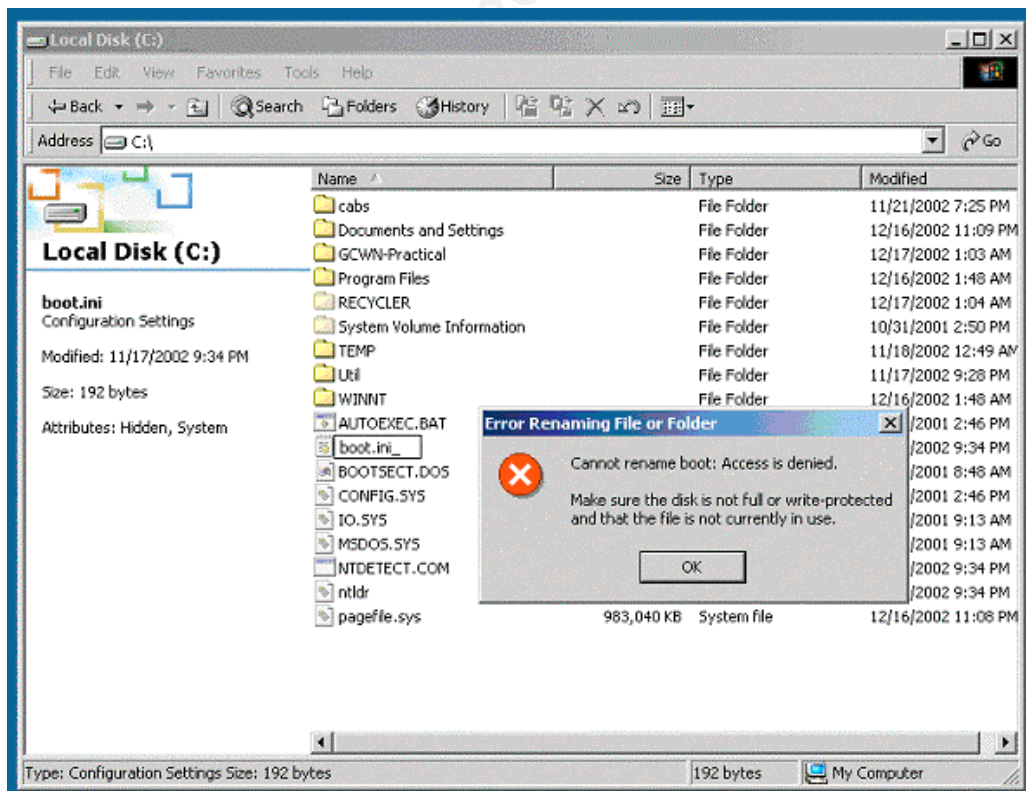
Vulnerability Assessment Scan.

As part of the evaluation of the template the Internet Security Systems ISS scanner v6.2.1 was used. The scan was supposed to detect a vulnerability remaining unfixed after applying the template. From the networking prospective, due to the fact that no specific settings were applied to the wireless and Ethernet network interface, the scan results should be the same for whatever interface we select to scan from. So, proceeding with this assumption, the first scan attempt was initiated from the Ethernet interface. However, the results of the first assessment were not comprehensive enough. As expected, the scanner managed to detect only the open ports. From one point of view it is a positive result of implementing the template. However, it is not what was expected. In order to get more results by comparing ISS' High Secure Policy with laptop's setting a second attempt was conducted. It is possible only in case where the "Access this computer from the network " permission is assigned to administrator. This permission modification was done by changing "User Rights Assignment" in Security Configuration and Analysis Snap-in and re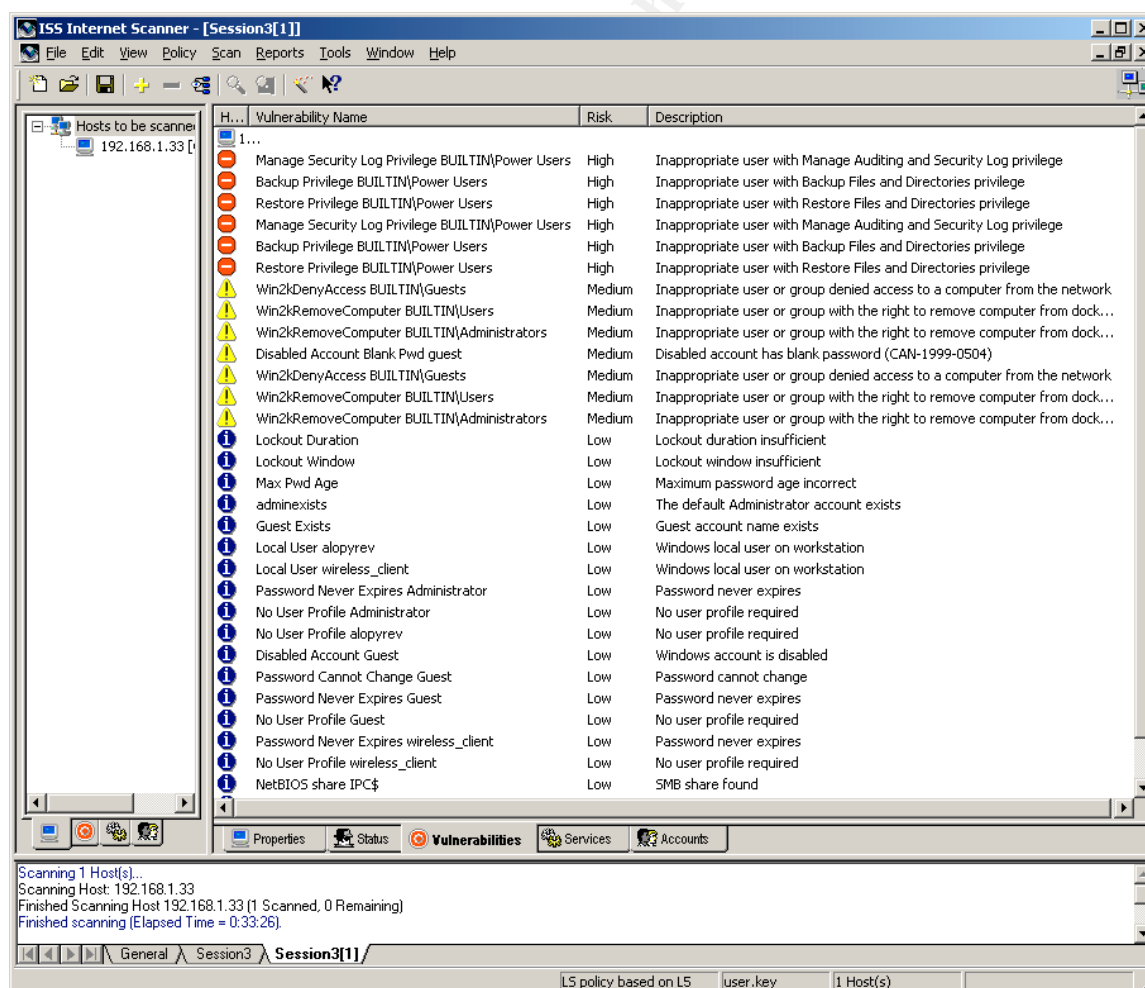configuring the computer. The administrator's account was also synchronized on both the ISS scanner PC and the wireless laptop. The resulting screenshot is presented on the Figure 11. The results show that the ISS scanner considered the assignment of certain rights to Power User inappropriate. As well, L5 policy has a different rating for user lockout.

Figure 11. ISS Vulnerability Assessment scan.

Vulnerability Name	Risk	Description
Manage Security Log Privilege BUILTIN\Power Users	High	Inappropriate user with Manage Auditing and Security Log privilege
Backup Privilege BUILTIN\Power Users	High	Inappropriate user with Backup Files and Directories privilege
Restore Privilege BUILTIN\Power Users	High	Inappropriate user with Restore Files and Directories privilege
Manage Security Log Privilege BUILTIN\Power Users	High	Inappropriate user with Manage Auditing and Security Log privilege
Backup Privilege BUILTIN\Power Users	High	Inappropriate user with Backup Files and Directories privilege
Restore Privilege BUILTIN\Power Users	High	Inappropriate user with Restore Files and Directories privilege
Win2kDenyAccess BUILTIN\Guests	Medium	Inappropriate user or group denied access to a computer from the network
Win2kRemoveComputer BUILTIN\Users	Medium	Inappropriate user or group with the right to remove computer from dock...
Win2kRemoveComputer BUILTIN\Administrators	Medium	Inappropriate user or group with the right to remove computer from dock...
Disabled Account Blank Pwd guest	Medium	Disabled account has blank password (CAN-1999-0504)
Win2kDenyAccess BUILTIN\Guests	Medium	Inappropriate user or group denied access to a computer from the network
Win2kRemoveComputer BUILTIN\Users	Medium	Inappropriate user or group with the right to remove computer from dock...
Win2kRemoveComputer BUILTIN\Administrators	Medium	Inappropriate user or group with the right to remove computer from dock...
Lockout Duration	Low	Lockout duration insufficient
Lockout Window	Low	Lockout window insufficient
Max Pwd Age	Low	Maximum password age incorrect
adminexists	Low	The default Administrator account exists
Guest Exists	Low	Guest account name exists
Local User alopyrev	Low	Windows local user on workstation
Local User wireless_client	Low	Windows local user on workstation
Password Never Expires Administrator	Low	Password never expires
No User Profile Administrator	Low	No user profile required
No User Profile alopyrev	Low	No user profile required
Disabled Account Guest	Low	Windows account is disabled
Password Cannot Change Guest	Low	Password cannot change
Password Never Expires Guest	Low	Password never expires
No User Profile Guest	Low	No user profile required
Password Never Expires wireless_client	Low	Password never expires
No User Profile wireless_client	Low	No user profile required
NetBIOS share IPC$	Low	SMB share found

Scanning 1 Host(s)...
Scanning Host: 192.168.1.33
Finished Scanning Host 192.168.1.33 (1 Scanned, 0 Remaining)
Finished scanning (Elapsed Time = 0:33:26).

Test the system's functionality.

Configuring of RRAS for L2TP.

To simplify implementation of the IPSec policy for L2TP VPN, two assumptions were made:

- Traffic between the wireless laptop and the wireless VPN server should be IPSec encrypted. It will force other non-L2TP traffic to be encrypted or entirely blocked.
- For testing purpose, a pre-shared key will be an adequate solution in comparison with a certificate based L2TP for production implementation.

Two options may be used to create and activate static IPSec policy. The first, and most user-friendly, is invoked by wizards in the GUI interface of "IP Security Policy" Snap-in in MMC. The second option requires the *ipsecpol* command-line tool from Resource Kit. It is very useful for large-scale deployments of IPSec policies, to include a creation policies procedure as part of an automated server build process. This command-line utility allows one to script the creation of IPSec policies.

For the task of the practical assignment, the second option was selected. The MS Knowledge Base Q240262[18] article recommends the creation of a mirrored policy for both peers. However, that recommendation only covers filters for L2TP ports and UDP protocol. To lock down all traffic between the wireless server and the wireless laptop the IPSec filter should be extended for ALL protocols and ALL ports. Based on the current configuration the following batch file was created to inject and activate IPSec policy for both laptops.

> ***ipsecpol -f 192.168.0.1/255.255.255.255+192.168.0.128/255.255.255.255***
> ***192.168.0.1/255.255.255.255:1701+192.168.0.128/255.255.255.255:0:UDP***
> ***-n AH[SHA]+ESP[3DES,SHA] -a PRESHARE:"#maJ!3kD."***
> ***-w REG -p "My Wireless VPN policy" -r "My Wireless VPN rule" –x***

This command creates static policy and stores it in the registry. The batch file is symmetrical and can be used on both laptops. All protocols and ports will use Preshared Key to negotiate security for the Authenticated header (SHA1) and the Encapsulating Security Payload (3DES, SHA1). The second filter is designated for L2TP traffic for RRAS. It does not pose any problem to add additional Negotiation policy to the batch file above. (like ESP[3DES,SHA], etc.) However, I decided to limit the script with one set. Furthermore, instead of Negotiating security for NON L2TP traffic, it can be simply blocked.

The IPSec policies are stored in the registry and require administrative rights in order to save and activate them.

Testing Encrypted Wireless Communication.

After the *ipsecpol* batch file was executed, the IPSec polity was activated. The IPSec monitor can confirm whether wireless secured communications are successful, by displaying the active security associations on local or remote computers   See Figure 12 below shows the screenshot of the IPSECMON windows.
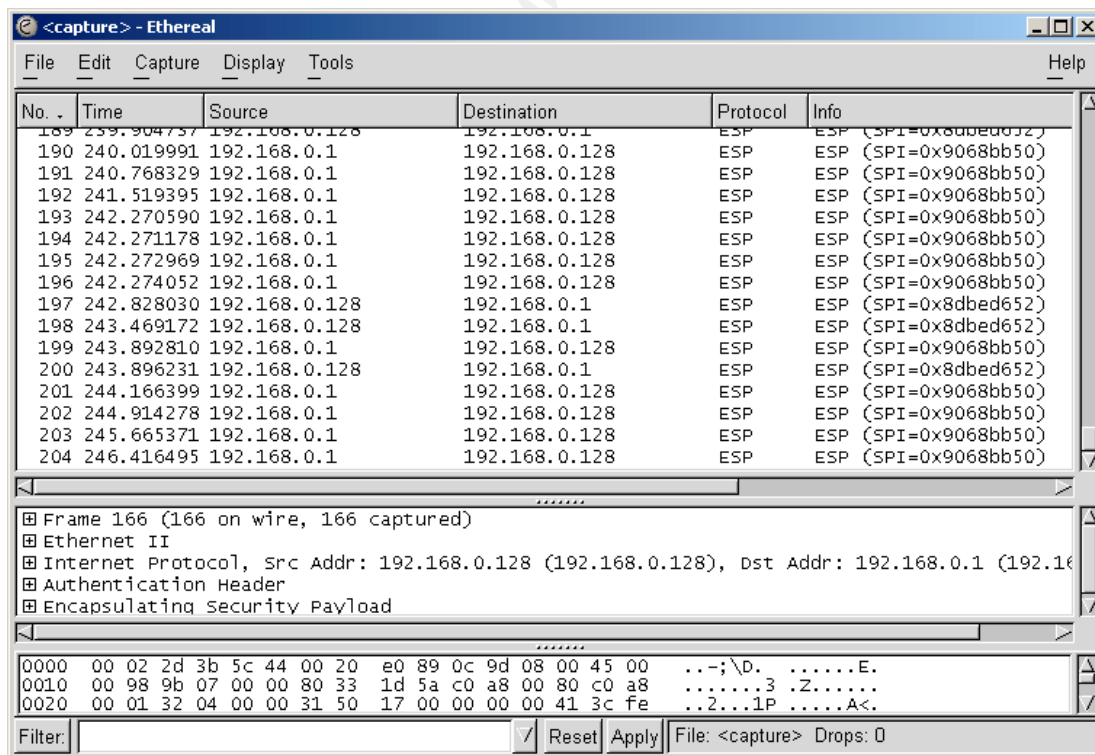
---

[18] How to Configure a L2TP/IPSec Connection Using Pre-shared Key Authentication.
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q240262

Figure 12. Result of negotiation of the IPSEC policies.
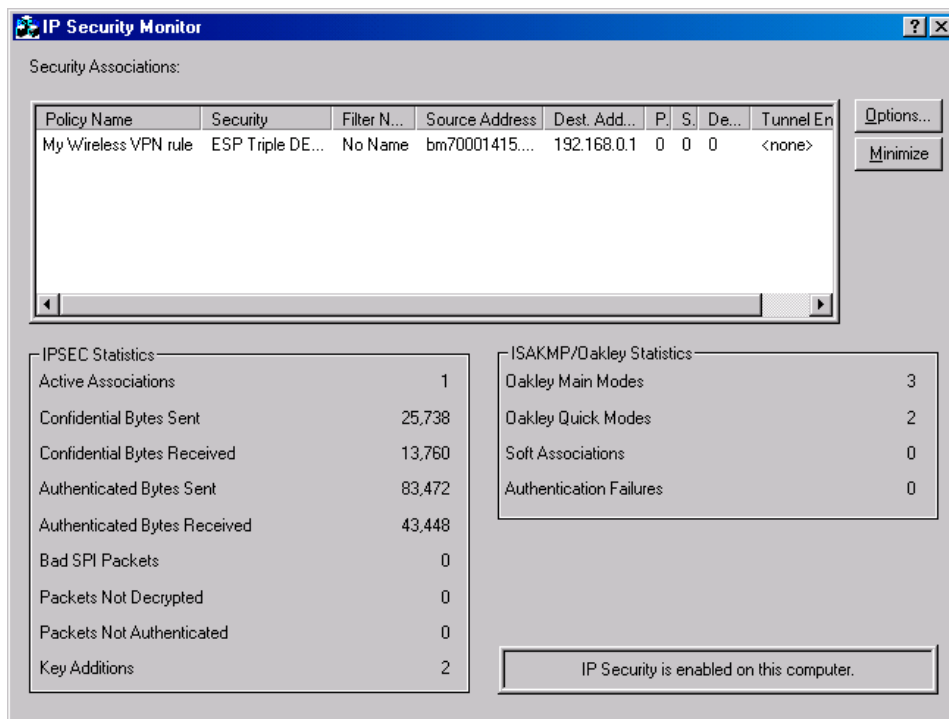
Activation of the policy on both sides completely encrypting the traffic.

**Figure 13. Encrypted wireless traffic.**

To test that after activation of the IPSec filter the wireless laptop is not listening on any ports the nmap scan was conducted from wireless server. This required a temporary deactivation of IPSec policy on the wireless sever. It took significant time to wait until *nmap* failed to find any open ports on the wireless laptop.

Testing VPN connectivity.

To test VPN connectivity after the IPSec policy was activated the "Virtual Private Connection" icon, created during the testing of PPTP RRAS, was used. The property of the connection was modified in order to use L2TP.

Figure 14
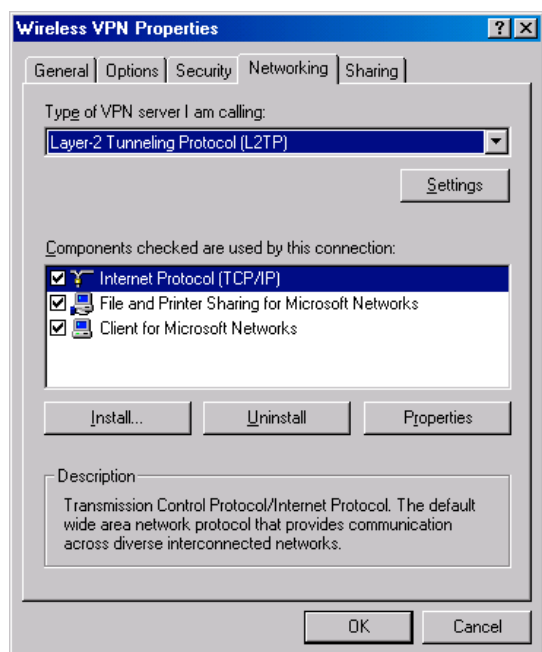
,
When connection was established; the simplest way to check connectivity is to verify ability for the wireless_client user to browse the Internet. All settings were correct, and L2TP connection though the wireless link was successfully established. The client's routing table was updated, according to RRAS settings, and futher observation showed no problem with the Internet access. Sniffing of the wireless traffic showed the same results as presented on Appendix 1

Testing Shared resources and MS Office applications.

Connection to the shared resources after the VPN was established does not poses any problem. For the wireless_client the network resources were accessible if he was connected directly to the network. The same may be said about MS Office Applications. The wireles_client was able to open the VBA editor, write and debug a code, and then distribute it on rewritable CD.

Evaluate the template

The security templates, the Security Configuration and Analysis Snap-in, the Resource Kit Tools, and the other aspects of the Windows 2000 Security Administration model is a significant step forward in converting Security Administration from a time-consuming task to a fully automated centralized process. Using security templates, based on "Best Practice", helps to quickly implement a required level of security on an enterprise-wide environment.

The template, selected for evaluation, accumulated many of recommendations to securing a Windows 2000 based system. Almost all articles I have found published on the Internet to a certain degree have been included into the NIST template. The template requires minor modifications to be implemented in various environments. Moreover, in most cases the security level that can be achieved by following the NIST recommendation is very high.

One of the problems I meet during the testing of system functionality is inability for ordinary users to change their password via the Control Panel. It appears to be a violation of the user's permission to some dll's in the system folder or registry. I believe that it is not a shortcoming, however, it should be investigated as a next step in evaluation of the NIST template.

Based on the published information some issues cannot be covered by security template:

- **NetBIOS over TCP/IP**. NetBIOS can be completely disabled and it will not affect the system functionality. Unbinding NetBIOS from TCP/IP eliminates broadcasting of SMB messages. These settings are the property of network card and do not have a predefined registry place. It will vary from card to card depending on the installation order.
- **IPSec policy**. Even the policy can be stored in the registry; I did not find a way in which the IPSec policy can be assigned via security template. Each policy has a dynamically created unique ID number under which it is stored in registry. This number is hard to predict at the time of designing or modifying the template. So the IPSec policy should be implemented as post installation task or distributed as part of GPO in Active Directory environment.
- **RRAS policy**. The same said above will also be right in relation to Remote Access policy. The RRAS policy cannot be assigned by modifying security templates.

Final words.

Regardless to the limitation of the security settings for template the ISS Vulnerability Assessment scan conducted before and after the security template was implemented demonstrated that almost all high and medium level security holes were closed. It underlines the fact that in order to close new system vulnerability, modify system requirement, or change overlooked settings, the new approach can be chosen. Instead of publishing advisories or security guidance, the new security settings can be distributed in a powerful form of an incremental security template.

References.

1. Fossen, Jason. Windows 2000: Active Directory, DNS & Group Policy. (Version 5.1.3, 12/31/2001). SANS Institute.
2. Fossen, Jason. Windows 2000/XP IPSec, RRAS and VPNs (Version 4.0 12/05/2001). SANS Institute.
3. Microsoft Windows® 2000 Security. Technical Reference / Internet Security System, Inc.; Microsoft Press, 2000.
4. Designing Microsoft Windows® 2000 Network Security. MCSE Training Kit. ; Microsoft Press, 2001.
5. Windows 2000 Common Criteria Secure Configuration Guide. Appendix C - User Rights and Privileges.
   http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/W2kCCSCG/W2kSCGcc.asp
6. Intercepting Mobile Communications: The Insecurity of 802.11
   http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf
7. NIST Systems Administration Guidance for Windows 2000 Professional
   http://csrc.nist.gov/itsec/download_W2Kpro.html
8. How to Add Custom Registry Settings to Security Configuration Editor
   http://support.microsoft.com/default.aspx?scid=kb;en-us;214752
9. Predefined security templates
   http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_SCEdefaultpols.htm
10. Windows 2000 Security Templates Are Incremental
    http://support.microsoft.com/default.aspx?scid=KB;en-us;q234926
11. HOW TO: Apply Predefined Security Templates in Windows 2000
    http://support.microsoft.com/default.aspx?scid=KB;en-us;q309689
12. Comprehensive Review of Windows 2000 Security Policy Templates and Security Configuration Tool
    http://www.ists.dartmouth.edu/IRIA/knowledge_base/sectemplates/sectemplates.pdf
13. Disabling IPSEC Policy Used with L2TP.http://support.microsoft.com/default.aspx?scid=kb;en-us;Q258261
14. Microsoft Platform SDK: Security: Security Descriptor Definition Language.
    http://msdn.microsoft.com/library/en-us/security/Security/security_descriptor_definition_language.asp
15. Microsoft Platform SDK: Security: Security Descriptor String Format
    http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/Security/security_descriptor_string_format.asp
16. HOW TO: Reset Security Settings Back to the Defaults
    http://support.microsoft.com/default.aspx?scid=kb;en-us;Q313222
17. How to Configure a L2TP/IPSec Connection Using Pre-shared Key Authentication. http://support.microsoft.com/default.aspx?scid=kb;en-us;Q240262
18. CalNet Active Directory, University of California, Berkley
    http://calnetad.berkeley.edu/documentation/technical/configuration_files/

Appendices

Appendix 1. Modification for Sceregvl.inf file.

The following modifications should be done in the Sceregvl.inf to disable automatic injection of the dynamic IPSec policy.

[Register Registry Values]
; Automatic L2TP policy injection
MACHINE\System\CurrentControlSet\Services\Rasman\Parameters\ProhibitIpSec,4,%CreateDymamicL2TPpolicy%,0|,%DisableDymamicL2TPpolicy%,1

[Strings]
CreateDymamicL2TPpolicy= Enable automatic injection of a dynamic IPSec policy
DisableDymamicL2TPpolicy= Disable automatic injection of a dynamic IPSec policy

Appendix 2. Resulting IPSec policy.

    Local IPSec Policy Active: 'My Wireless VPN policy'
    IP Security Policy Path: SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local\ipsecPolicy{E64E36FB-07D8-463C-BA4D-F41E77CD99E3}

    There are 4 filters
    No Name - Mirror
     Filter Id: {30EF3D4D-47E2-4244-9596-38EE04DA7F78}
     Policy Id: {C28066A1-6E00-4108-A5B2-6222AD608E7E}
       IPSEC_POLICY PolicyId = {C28066A1-6E00-4108-A5B2-6222AD608E7E}
            Flags: 0x0
            Tunnel Addr: 0.0.0.0
       PHASE 2 OFFERS Count = 1
            Offer #0:
       AH[SHA1 HMAC] AND ESP[3DES SHA1 HMAC]
       Rekey: 0 seconds / 0 bytes.
       AUTHENTICATION INFO Count = 1
            Method = Preshared key: #maJ!3kD.
     Src Addr : 192.168.0.128 Src Mask : 255.255.255.255
     Dest Addr : 192.168.0.1   Dest Mask : 255.255.255.255
     Tunnel Addr : 0.0.0.0   Src Port : 0   Dest Port : 1701
     Protocol : 17   TunnelFilter: No
     Flags : Outbound
    No Name
     Filter Id: {30EF3D4D-47E2-4244-9596-38EE04DA7F78}
     Policy Id: {C28066A1-6E00-4108-A5B2-6222AD608E7E}
       IPSEC_POLICY PolicyId = {C28066A1-6E00-4108-A5B2-6222AD608E7E}
            Flags: 0x0
            Tunnel Addr: 0.0.0.0
       PHASE 2 OFFERS Count = 1
            Offer #0:
       AH[SHA1 HMAC] AND ESP[3DES SHA1 HMAC]
       Rekey: 0 seconds / 0 bytes.
       AUTHENTICATION INFO Count = 1
            Method = Preshared key: #maJ!3kD.
     Src Addr : 192.168.0.1   Src Mask : 255.255.255.255

Dest Addr : 192.168.0.128 Dest Mask : 255.255.255.255
 Tunnel Addr : 0.0.0.0   Src Port : 1701 Dest Port : 0
 Protocol : 17   TunnelFilter: No
 Flags : Inbound
 No Name
 Filter Id: {21F4EEB1-3186-4441-909A-B73D5B079609}
 Policy Id: {C28066A1-6E00-4108-A5B2-6222AD608E7E}
   IPSEC_POLICY PolicyId = {C28066A1-6E00-4108-A5B2-6222AD608E7E}
        Flags: 0x0
        Tunnel Addr: 0.0.0.0
   PHASE 2 OFFERS Count = 1
        Offer #0:
   AH[SHA1 HMAC] AND ESP[3DES SHA1 HMAC]
   Rekey: 0 seconds / 0 bytes.
   AUTHENTICATION INFO Count = 1
        Method = Preshared key: #maJ!3kD.
 Src Addr : 192.168.0.1   Src Mask : 255.255.255.255
 Dest Addr : 192.168.0.128 Dest Mask : 255.255.255.255
 Tunnel Addr : 0.0.0.0   Src Port : 0   Dest Port : 0
 Protocol : 0   TunnelFilter: No
 Flags : Inbound
 No Name - Mirror
 Filter Id: {21F4EEB1-3186-4441-909A-B73D5B079609}
 Policy Id: {C28066A1-6E00-4108-A5B2-6222AD608E7E}
   IPSEC_POLICY PolicyId = {C28066A1-6E00-4108-A5B2-6222AD608E7E}
        Flags: 0x0
        Tunnel Addr: 0.0.0.0
   PHASE 2 OFFERS Count = 1
        Offer #0:
   AH[SHA1 HMAC] AND ESP[3DES SHA1 HMAC]
   Rekey: 0 seconds / 0 bytes.
   AUTHENTICATION INFO Count = 1
        Method = Preshared key: #maJ!3kD.
 Src Addr : 192.168.0.128 Src Mask : 255.255.255.255
 Dest Addr : 192.168.0.1   Dest Mask : 255.255.255.255
 Tunnel Addr : 0.0.0.0   Src Port : 0   Dest Port : 0
 Protocol : 0   TunnelFilter: No
 Flags : Outbound

Appendix 3. Resulting Template file.

Resulting template file for wireless laptop is included as file due to its size.

wireless_wks.inf