Global Information Assurance Certification Paper

Using the NT Resource Kit C2 Configuration Manager

For Microsoft Windows NT 4.0

Practical for SANS GIAC track 6

Manuel A.H. Offenberg
Academic Hospital Vrije Universiteit
Amsterdam, The Netherlands
m.offenberg@azvu.nl
phone: +31 20 444432

1 INTRODUCTION

On December 02, 1999, the US Government announced that Microsoft Windows NT Server and Workstation 4.0 had successfully completed a C2 evaluation according to the Trusted Computer System Evaluation Criteria (TCSEC) [1]. The TCSEC, also known as the "Orange Book", is a widely accepted evaluation process for secure IT systems. The Windows NT 4.0 evaluation included servers and workstations in six different roles, operating in both TCP/IP networked and stand-alone modes.

The evaluation is done according to a set of predefined criteria, which are divided into four divisions. Each division contains one or more classes and within each class, four major sets of criteria are addressed: Security Policy, Accountability, Assurance, and Documentation. The divisions are ordered in a hierarchical manner:

A. Verified protection

   Class A1: verified design;

   Beyond class A1: additional features and assurances on top of the ones in A1.

B. Mandatory protection

   Class B1: labeled security protection;

   Class B2: structured protection;

   Class B3: security domains.

C. Discretionary design

   Class C1: discretionary security protection;

   Class C2: controlled access protection.

D. Minimal protection: contains systems that fail to meet the criteria set for any higher division or class.

As Windows NT 4 was successfully evaluated for class C2, implying that it had to meet requirements such as fine grained discretionary access control by allowing users to specify and control sharing of objects, user identity authentication, maintain an audit trail of access to objects, and isolation of resources on the system.

One has to keep in mind that there is a difference between deploying a system in a C2-evaluated configuration and having a C2-certified system. A C2 evaluation considers if a particular product, here Windows NT, can be part of a C2 certification when correctly configured. A C2 certification indicates the degree of security that a certain deployed system configuration provides, and considers additional factors on top of how Windows NT is configured.

2 C2 CONFIGURATION MANAGER

This chapter will explain how the C2 Configuration Manager, a tool which is part of the Window NT 4 Resource Kit, works. It can be used as a guideline for securing a Windows NT box. As the tool was released before NT 4 was C2 evaluated in an network environment, running the C2 Configuration Manager does not automatically constitute to a C2 configured system. When a C2 compliant system is required, one has to comply to the steps outlined in

Microsoft's "C2 Administrator's and User's Security Guide Revision 1.1; Microsoft® Windows NT® Version 4.0" (further on called the "C2 Guide") [3] and briefly mentioned in Chapter 3 of this paper.

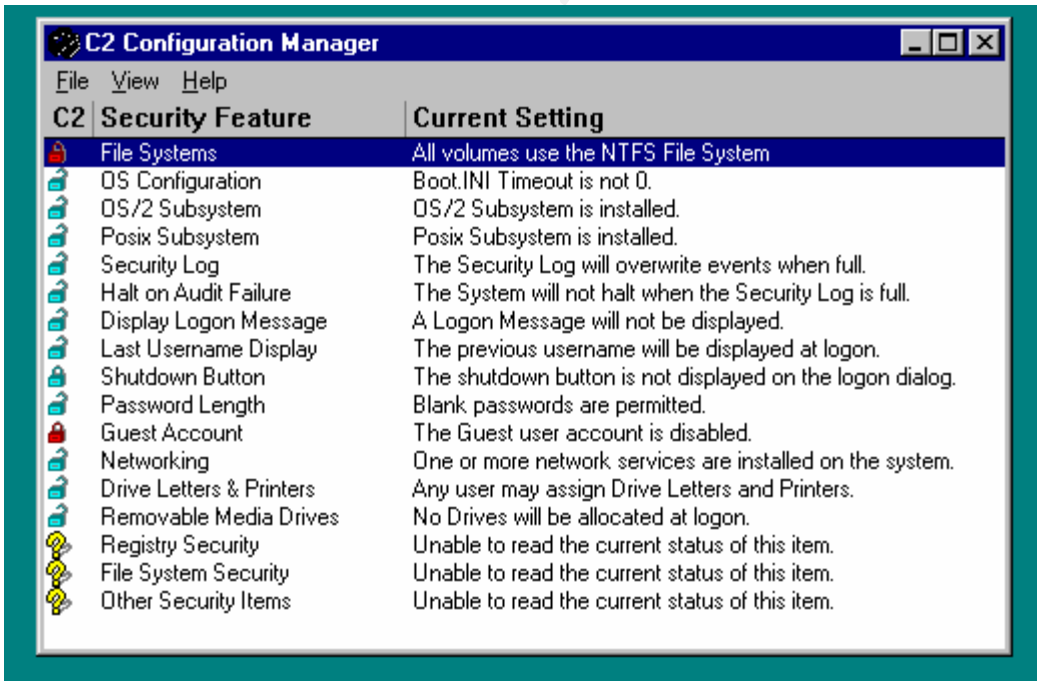
2.1 Preliminary steps

Before using the tool, the following prerequisites are important [2]:

1. install Windows NT 4 on NTFS partitions;
2. remove MS Peer Web Services;
3. install latest service pack (by then SP 3);
4. update Emergency Repair Disk (ERD) information;
5. increase registry size to 20 MB;
6. apply hotfixes;
7. update Emergency Repair Disk (ERD) information;
8. install Windows NT 4 Resource Kit.

2.2 Using the C2 Configuration Manager

In this section, we will explain how C2 Configuration Manager works. The next picture shows the tool just after it was started.



The first column (C2) indicates how the security feature in the second column is configured by displaying one of four possible icons:

1. closed red lock: feature is C2 compliant;
2. closed blue lock: feature is secure but not required in a C2 configured system;

3. open blue lock: feature is not secure and must be configured;
4. question mark: C2 Configuration Manager is unable to detect the status of the feature.

The last column provides a short explanation on the current state of a security feature, indicating possible actions to take. When double-clicking a feature, a message box is displayed indicating the actions the Configuration Manager will take.

2.2.1 File systems

In order to support C2 security on a Windows NT4 box all disk volumes must be on the NTFS filesystem. Only then discretionary access control to files and directories can be enforced, as the other supported filesystem (FAT) does not provide any security features.

By selecting the File Systems feature, the user will be able to convert the non-NTFS volumes into NTFS volumes. This conversion will only be executed after the system is restarted. In our case, the NT4 box was already on NTFS.

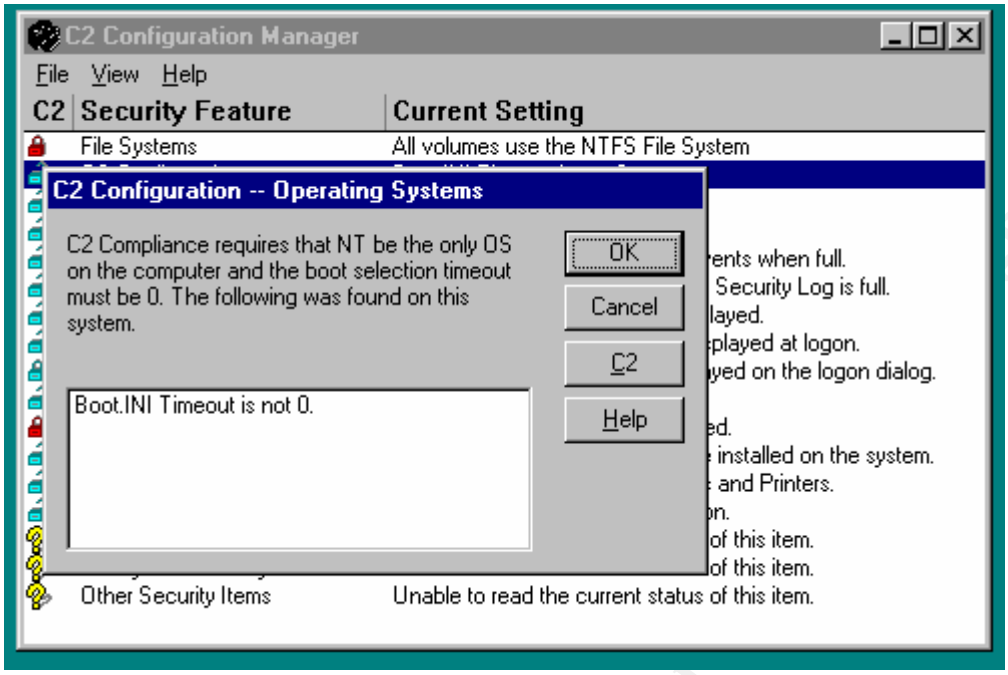
2.2.2 OS configuration

The OS configuration feature of the C2 Configuration Manager checks if Windows NT is the only operating system on the box and that the timer in the BOOT.INI file is set to zero. Dual-boot systems and a timer greater then zero opens the opportunity for booting to a different OS. When this is the case, one can load NTFS drivers and circumvent the NTFS security.

The dialog displayed shows that, in our case, only the BOOT.INI timer is non-zero. Clicking the C2-button will select all items in the dialog box; then clicking OK will display a warning dialog; confirm by clicking OK again and the timer in the BOOT.INI file is set to zero. A red lock will show up in front of the OS configuration feature.

In our case, the entries in BOOT.INI will look like:

```
-----------------------------------------------------
[boot loader]
timeout=0
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Server Version
4.00"
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Server Version
4.00 [VGA mode]" /basevideo /sos
-------------------------------------
```



2.2.3 OS/2 and POSIX subsystems

There is little available information on the trustworthiness of the POSIX and OS/2 subsystems. This, combined with the fact that these subsystems where not included in the C2 evaluated configuration, means that removal of the subsystems is necessary for C2 compliance.

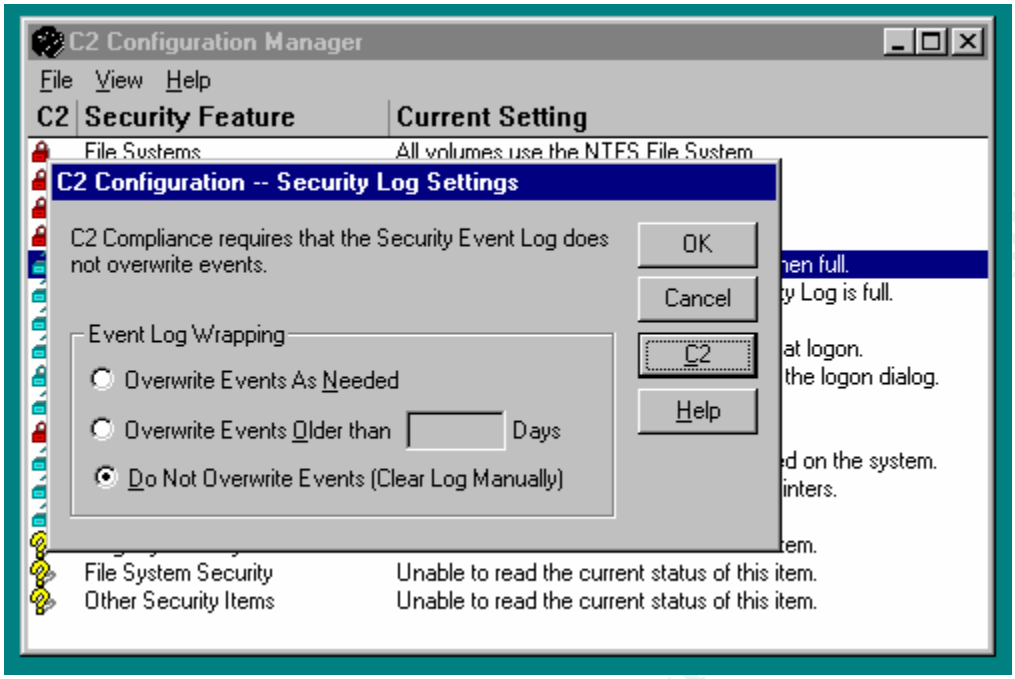
Executing the OS/2 Subsystem and Posix subsystem features will remove OS2.EXE, OS2SS.EXE and PSXSS.EXE from System32 directory that resides under the system root.

Note: Although indicated by the C2 Configuration Manager, these actions are not sufficient for a C2 compliant system.

2.2.4 Security Log

This feature will set the wrapping options on the security log. By clicking the C2 button the option "Do Not Overwrite Events (Clear Log Manually)" is selected, which is the required option for a C2 configuration. After applying the Security Log feature, the value Retention in the registry will change in FFFFFFFF Hex.

HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security
Name: Retention
Type: REG_DWORD
Data: 0xffffffff



Notes:

1. Make sure the size of the log file is sufficient and that enough space is available for the file to grow. By default, the security log is stored in the boot-partition.
2. The problem is that the system administrator must manually backup and clear the security log when using the C2 compliant configuration of the security log. To automate this process, the tool DUMPEVT.EXE from SomarSoft (http://www.somarsoft.com) can be used. It will clear the log file and dump its contents in different formats.

2.2.5 Halt on audit failure

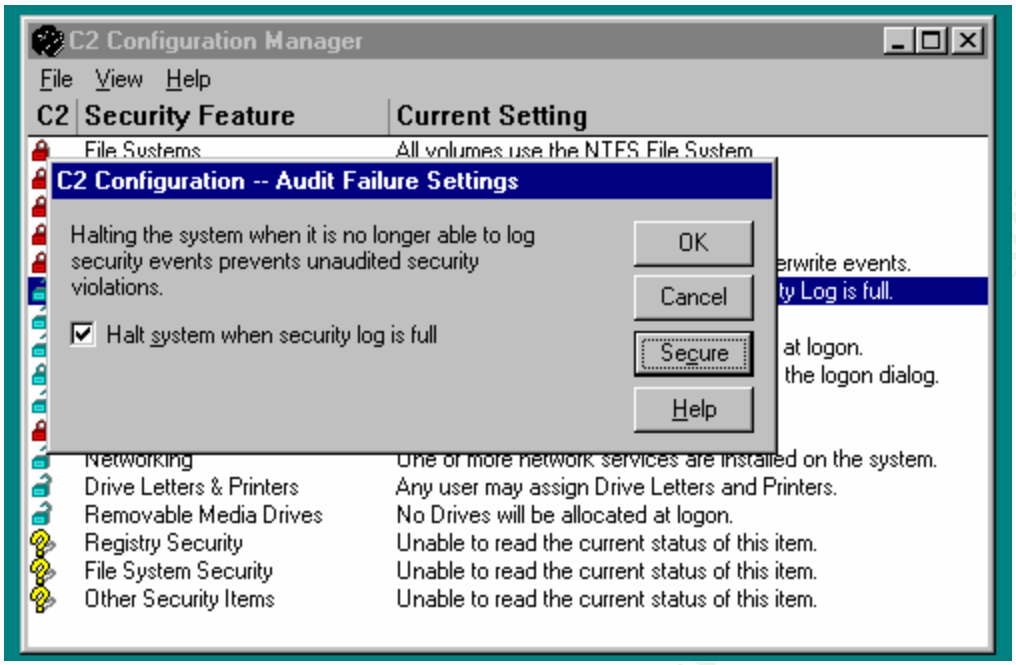
Clicking the Secure button will enable the "Halt system when security log is full" option. If used together with the log options "Overwrite Events Older than X Days" or "Do Not Overwrite Events (Clear Log Manually)" the system will halt when the log is full. A System Administrator must then logon to clear the log and reboot the system.

This security feature will add a entry in the registry under:

HKLM\SYSTEM\CurrentControlSet\Control\Lsa
Name: CrashOnAuditFail
Type: REG_DWORD
Data: 0x1

Notes:

1. Changes made by this feature will only take effect after a restart of the system.
2. The icon of this security feature will change into a closed blue lock, instead of a red lock. This is a result of the fact that the "Halt on audit failure" feature is not a C2 required setting.



2.2.6 Display logon message

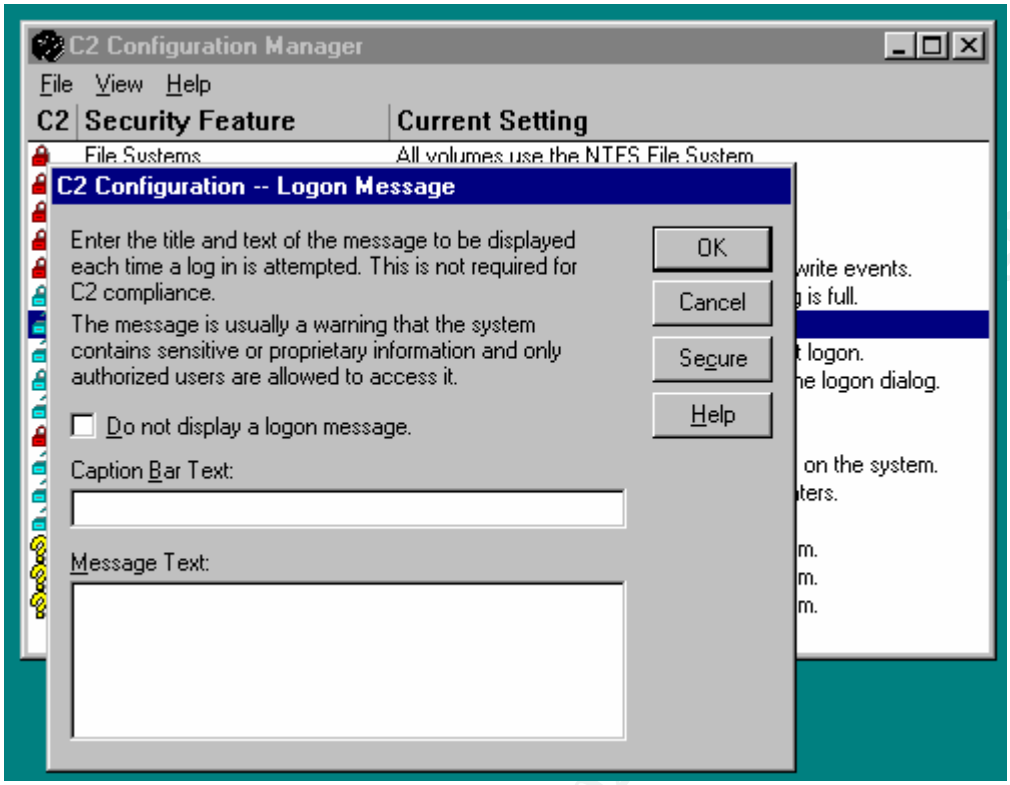
This feature will create a message that is displayed during a logon. The message box has a caption bar and a text area that can be configured by entering a user defined text. It can e.g. be used for displaying a legal notice when a user logs on to a Windows NT box.

Using this configuration feature will modify the following registry entries:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Name: LegalNoticeCaption
Type: REG_SZ
Data: Legal notice
Name: LegalNoticeText
Type: REG_SZ
Data: Here the text of the legal notice.

When clicking the Secure button, an alert will be displayed stating that "You must enter a logon message and caption bar text."

Note: Not required for a C2 compliant system.



2.2.7 Last username display

On a Windows NT system, the username of the last person who logged on the system is displayed in the username textbox of the logon screen. This is a possible security thread as the username displayed provides a potential intruder with a valid username in the domain.

Executing this feature will add the registry value:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Name: DontDisplayLastUserName
Type: REG_SZ
Data: 1

Note: Is not required for a C2 compliant system.

2.2.8 Shutdown button

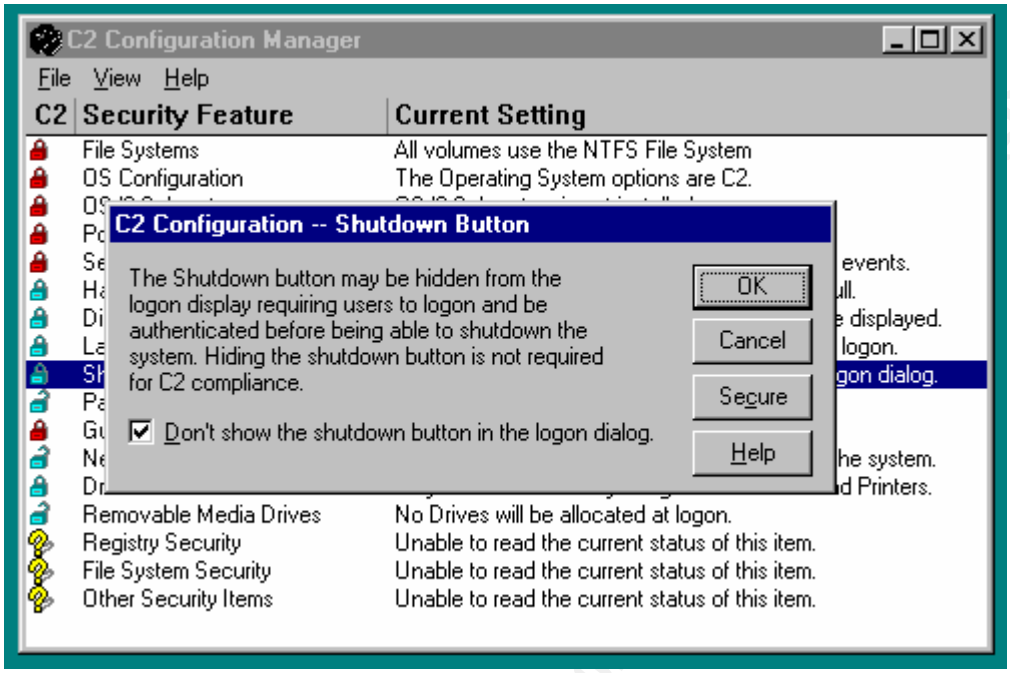
With Windows NT Workstation a user can shutdown the system by clicking the Shutdown button that appears on the Logon dialog box. This is by default disabled on Windows NT Server, making proper system shutdown only capable for logged on users.

According to the dialog that pops up when selecting this feature in the C2 Configuration Manager, this configuration setting is not required for a C2 compliant system. But, the "C2 Guide" states that it is compulsory.

The feature will add the following registry entry or set its value to 0:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Name: ShutdownWithoutLogon
Type: REG_SZ
Data: 0



2.2.9 Password length

Two options are displayed: "Allow Blank Passwords" or "Password must contain at least X characters". Only the section option is eligible for a C2 configured Windows NT box. When clicking the C2 button, the second option is selected and a value of 6 is assigned to X.

Notes:

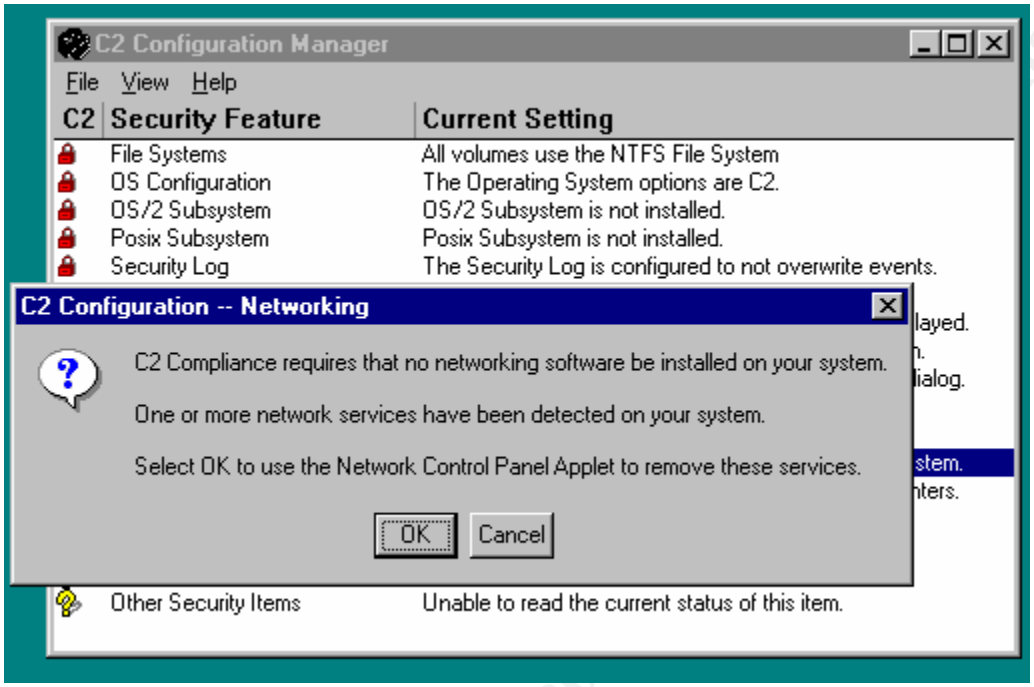
1. The "C2 Guide" only states that blank password have to be disabled, but says nothing about the length and/or complexity of the password. Therefore, additional measures have to be taken to enforce a sound password policy. Installation of a optional password filter (e.g. PASSFILT.DLL, provided in SP3 and higher) can help to filter out week user passwords.
2. Be aware of the fact that, when no appropriate measures are taken (set RestrictAnonymous to 1 in HKLM\SYSTEM\CurrentControlSet\Control\LSA, see [4]), null user sessions can list password policies.

2.2.10 Guest account

C2 level security does not allow anonymous users to access a system, therefore the Guest account must be disabled. This is the default configuration when Windows NT Server is installed, otherwise use User Manager or User Manager for Domains to disable or delete the Guest account.

2.2.11 Networking

When selecting this feature in the C2 Configuration Manager, the following message is displayed:



Windows NT 4 was evaluated in a TCP/IP networking environment, making this an invalid message. See [3, page 58] for the network services that were included during the evaluation process.

2.2.12 Drive letters and printers

According to the displayed information this security feature will allow only Administrators to assign printer ports and drive letters, but in fact adds the registry subkey with value 1:

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager
Name: ProtectionMode
Type: REG_DWORD
Data: 0x1

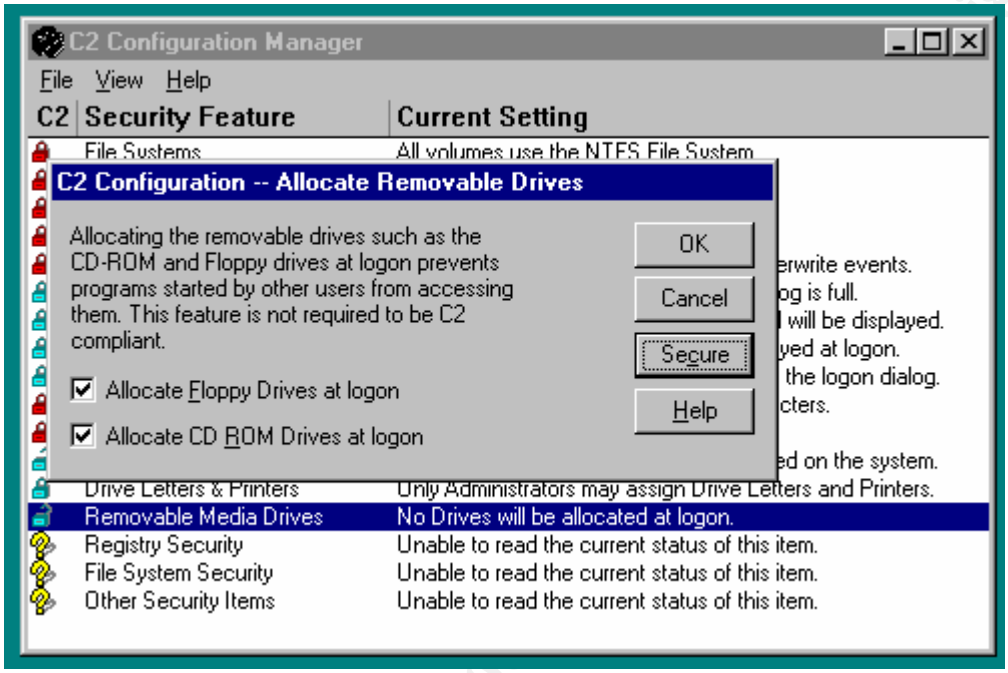
The impact of this registry modification is a little broader then suggested, as it tightens the security of all base objects on the system. Result: shared resources can only be managed by system administrators.

2.2.13 Removable media drives

When setting this security feature, it restricts access to floppy drives and cd-rom drives only to the current logged on user. This prevents programs or other users from accessing these resources during the time a user is active.

This feature will add the following registry entries:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Name: AllocateCdRoms
Type: REG_SZ
Data: 1
Name: AllocateFloppies
Type: REG_SZ
Data: 1



By clicking the Secure button both options are checked.

Note: According to the dialog box, this is not a required C2 feature, while in reality the "C2 Guide" does state that it is required for a C2 compliant system.

2.2.14 Registry security

Execution of this security feature will change the access rights to registry keys by using the settings provided in the C2REGACL.INF file, which comes with the C2 Configuration Manager. The keys are modified as follows:

HKLM\SOFTWARE

	Query Value	Set Value	Create Subkey	Enumer-ate Subkeys	Notify	Create Link	Delete	Read Con-trol	Write DAC	Write Owner	no access
ADMINISTRATORS, CREATOR OWNER, SYSTEM	√	√	√	√	√	√	√	√	√	√	
EVERYONE	√	√	√	√	√		√	√			

HKLM\SOFTWARE\Classes

	Query Value	Set Value	Create Subkey	Enumer-ate Subkeys	Notify	Create Link	Delete	Read Con-trol	Write DAC	Write Owner	no access
ADMINISTRATORS, CREATOR OWNER, SYSTEM	√	√	√	√	√	√	√	√	√	√	
EVERYONE	√	√	√	√	√		√	√			

All subkeys and default rights for new subkeys under HKLM\SOFTWARE\Classes\

	Query Value	Set Value	Create Subkey	Enumer-ate Subkeys	Notify	Create Link	Delete	Read Con-trol	Write DAC	Write Owner	no access
ADMINISTRATORS, CREATOR OWNER, SYSTEM	√	√	√	√	√	√	√	√	√	√	
EVERYONE	√	√	√	√	√		√	√			

HKLM\SOFTWARE\Description

	Query Value	Set Value	Create Subkey	Enumer-ate Subkeys	Notify	Create Link	Delete	Read Con-trol	Write DAC	Write Owner	no access
ADMINISTRATORS, CREATOR OWNER, SYSTEM	√	√	√	√	√	√	√	√	√	√	
EVERYONE	√	√	√	√	√		√	√			

All subkeys and default rights for new subkeys under HKLM\SOFTWARE\Description\

	Query Value	Set Value	Create Subkey	Enumer-ate Subkeys	Notify	Create Link	Delete	Read Con-trol	Write DAC	Write Owner	no access
ADMINISTRATORS, CREATOR OWNER, SYSTEM	√	√	√	√	√	√	√	√	√	√	
EVERYONE	√	√	√	√	√		√	√			

HKLM\SOFTWARE\Microsoft

	Query Value	Set Value	Create Subkey	Enumer-ate Subkeys	Notify	Create Link	Delete	Read Con-trol	Write DAC	Write Owner	no access
ADMINISTRATORS, CREATOR OWNER, SYSTEM	√	√	√	√	√	√	√	√	√	√	
EVERYONE	√	√	√	√	√		√	√			

All subkeys and default rights for new subkeys under HKLM\SOFTWARE\Microsoft\

	Query Value	Set Value	Create Subkey	Enumer-ate Subkeys	Notify	Create Link	Delete	Read Con-trol	Write DAC	Write Owner	no access
ADMINISTRATORS, CREATOR OWNER, SYSTEM	√	√	√	√	√	√	√	√	√	√	
EVERYONE	√	√	√	√	√		√	√			

HKLM\SOFTWARE\Program Groups

	Query Value	Set Value	Create Subkey	Enumer-ate Subkeys	Notify	Create Link	Delete	Read Con-trol	Write DAC	Write Owner	no access
ADMINISTRATORS, CREATOR OWNER, SYSTEM	√	√	√	√	√	√	√	√	√	√	
POWER USERS	√	√	√	√	√		√	√			
EVERYONE	√			√	√			√			

HKLM\SOFTWARE\Secure

	Query Value	Set Value	Create Subkey	Enumer-ate Subkeys	Notify	Create Link	Delete	Read Con-trol	Write DAC	Write Owner	no access
ADMINISTRATORS, CREATOR OWNER, SYSTEM	√	√	√	√	√	√	√	√	√	√	
EVERYONE	√			√	√			√			

HKLM\SOFTWARE\Windows 3.1 Migration Status and default rights for all new subkeys

	Query Value	Set Value	Create Subkey	Enumer-ate Subkeys	Notify	Create Link	Delete	Read Con-trol	Write DAC	Write Owner	no access
ADMINISTRATORS, CREATOR OWNER, SYSTEM	√	√	√	√	√	√	√	√	√	√	
EVERYONE	√			√	√			√			

Note: The above listed changes of access rights do not match the ones defined in the "C2 Guide", see [3, pages 61 and 62].

2.2.15 File system security

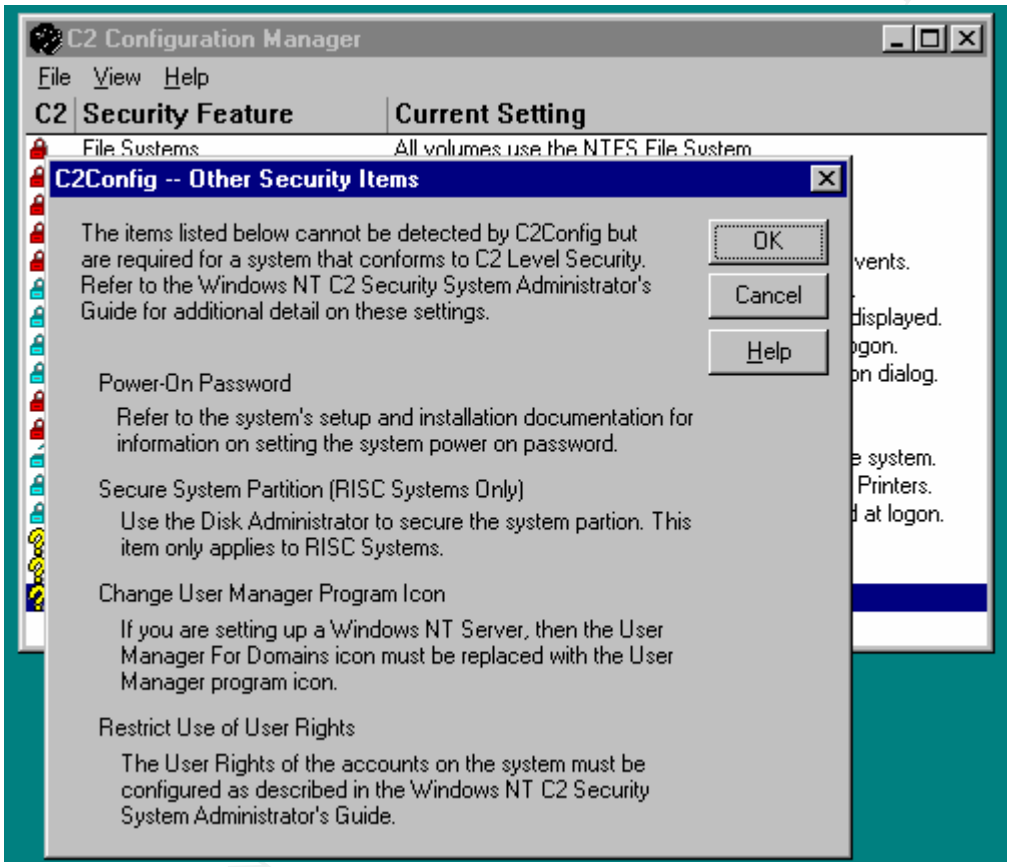
This security feature sets the access rights of files and directories on the system by modifying the ACL's. Exact details on ACL values to be set are found in the file C2NTFACL.INF, which resides in the root directory of the NT Resource Kit.

When the C2 Configuration Manager has executed this security feature, access rights are set for the Administrators, Replicator, Creator Owner, and Everyone groups, and for the System account.

Note: file and directory ACL's defined in the C2NTFACL.INF file do not match the ones in the "C2 Guide", see [3, page 61].

2.2.16 Other items

The C2 Configuration Manager is not capable of detecting all aspects of the system it is running on. Therefore, when selecting this feature the following text box is displayed:



It is a remainder for the additional actions to take when setting up a C2 compliant system.

Note: The third item on the list does not hold anymore, as the User Manager for Domains was part of the Windows NT 4 evaluation process. It can be used in a C2 compliant system.

2.2.17 Reboot system

When closing the tool, it displays a screen in which the user has the opportunity to reboot the system. This is necessary because some security features will only be activated after a system restart.

3 C2 EVALUATION OF NETWORKED WINNT4

In this section we will discuss how the C2 Configuration Manager can help to obtain a C2 secure system. Windows NT was successfully evaluated and the exact details of how to create a C2 compliant system are outlined in the "C2 Guide" [3]. We will show in which configuration steps the C2 Configuration Manager can support the configuration of C2 compliant system. Remind though, that only using the tool will not be sufficient.

3.1 C2 evaluation

In 1992 the National Computer Security Center (NCSC) began evaluating Windows NT Workstation and Windows NT Server. During December of 1999 Windows NT was successfully evaluated in a networked environment and found C2 compliant. The configuration consisted of Windows NT 4 SP6a in six different roles for Server (e.g. as PDC or BDC) and Workstation on Compaq hardware, operating in both TCP/IP networked and stand-alone modes.

Only the following components are allowed on a C2 system (as they were included during the evaluation process):

1. Microsoft DNS Server;
2. Microsoft WINS Server;
3. TCP/IP network protocol with static IP address;
4. Administrator tools: Control Panel, Event Viewer, User Manager and User Manager for Domains, Server Manager, Print Manager, Windows NT Backup, Registry Editors, Disk Administrator, DNS Manager, WINS Manager, DCOM Configuration Utility, and Windows NT Explorer.

One has to be aware of the fact that a C2-compliant system consists of hardware, software, application programs, and network services.

3.2 Using the C2 Configuration Manager for 'true' C2

In this subsection we will make clear which steps of the official C2 configuration process, as described in chapter 4 of the "C2 Guide", are supported by the C2 Configuration Manager, and which are not.

N.S. = Not Supported by C2 Configuration Manager

Unpack and set up hardware:

N.S.

Set power-on password:

The C2 Configuration manager will remind you in a message box under the security feature Other Security Items of setting this password, but is not capable of checking this setting.

Install Windows NT:

The only filesystem that was included during the evaluation process is NTFS. Therefore, one must, according to the "C2 Guide", select NTFS during installation, or one can use the C2

Configuration Manager to convert to NTFS. Nothing is said about the timer in the BOOT.INI.

Restart Windows NT as Administrator:

N.S.

Verify video driver:

N.S.

Install Printer and Tape Drivers:

N.S.

Install Service Pack 6a:

N.S.

Install C2 Update:

See [5]; N.S.

Enable hardware boot protection:

N.S.

Remove the NetBIOS Interface service:

N.S.

Disable unnecessary devices:

N.S.

Disable unnecessary services:

N.S.

Disable Guest account:

Supported.

Remove OS/2 and POSIX subsystems:

The C2 Configuration Manager only removes the executables of these subsystems; but the "C2 Guide" states that you have to:

1. remove the \winnt\system32\os2 directory and all of its subdirectories;
2. modify the following registry keys:

   HKLM\SOFTWARE\Microsoft\OS/2 Subsystem for NT
   Action: delete all subkeys;

   HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment
   Action: remove the value
   Name: Os2LibPath
   Type: REG_EXPAND_SZ
   Data: %SystemRoot%\system32\os2\dll;

   HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems
   Action: remove values
   Name: Optional
   Type: REG_MULTI_SZ
   Data: Os2

	Posix;
Name:	Os2
Type:	REG_EXPAND_SZ
Data:	%SystemRoot%\system32\os2ss.exe
Name:	Posix
Type:	REG_EXPAND_SZ
Data:	%SystemRoot%\system32\psxss.exe

Secure base objects:

Is done by the C2 Configuration Manager when executing the Drive Letters & Printers feature.

Secure additional base named objects:

N.S.

Protect kernel object attributes:

N.S.

Protect files and directories:

The settings implemented by the C2 Configuration Manager look more fine grained then the required settings as mentioned in the "C2 Guide", but they do violate them at several occasions. Apart from that, it is recommended that one makes its own settings based upon the guidelines in the "C2 Guide".

Protect the registry:

The settings implemented by the C2 Configuration Manager violate the C2 requirements. On top of that, the C2 Configuration Manager does not restrict remote access to the registry by setting the correct permissions on HKLM\SYSTEM\CurrentControlSet\ControlSecurePipeServers\winreg.

Restrict access to public Local Security Authority (LSA) information:

N.S.

Restrict null session access over named pipes:

N.S.

Restrict untrusted users' ability to plant Trojan horse programs:

N.S.

Disable caching of logon information:

N.S.

Allow only Administrators to create shares:

N.S.

Disable direct draw:

N.S.

Restrict printer driver installation to Administrators and Power Users only:

N.S.

Set the paging file to be cleared at system shutdown:

N.S.

Restrict floppy disk drive and CD-ROM drive access to the interactive user only:

Supported.

Enable NetBT to open TCP and UDP ports exclusively:

N.S.

Modify user rights memberships:

Is mentioned as one of the additional actions to take in the message box that is displayed when selecting Other Security Items.

Set auditing (if enabled) for base objects and for backup and restore:

N.S.

Disable blank passwords:

Supported.

Restrict system shutdown to logged-on users only:

Supported.

Set security log behavior:

Supported.

Be aware that the "Halt On Audit Failure" setting is not required for a C2 compliant system.

Restart the computer:

When finished with the C2 Configuration Manager, the user is queried if he/she wants to reboot the system.

Update the Emergency Repair Disk:

N.S.

4 REFERENCES

[1] Department of Defense, "Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, December 1995
http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

[2] US Navy, "Secure Windows NT Installation and Configuration Guide; Windows NT for Navy IT-21", version 1.3, December 1988

[3] Microsoft Corporation, "C2 Administrator's and User's Security Guide Revision 1.1; Microsoft® Windows NT® Version 4.0"
http://www.microsoft.com/security/issues/C2SecGuide.exe

[4] Fossen, J. & J. Johansson, "Windows NT Security: Step-by-Step", SANS GIAC, Version 3.5, May 2000

[5] Microsoft Corporation, "Fixes required in TCSEC C2 Security Evaluation Configuration for Windows NT 4.0 Service Pack 6a", knowledge base article Q244599