



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

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

## Interested in learning more?

Check out the list of upcoming events offering  
"Auditing Systems, Applications, and the Cloud (Audit 507)"  
at <http://www.giac.org/registration/gсна>

**AUDITING A MICROSOFT WINDOWS 2000  
TERMINAL SERVER**

**GSNA PRACTICAL  
ASSIGNMENT**

Version 3.2 Option 1

William Driskell

January 6, 2005

## TABLE OF CONTENTS

<b>ABSTRACT</b>	<b>III</b>
<b>SECTION 1: RESEARCH - AUDIT, SCOPE, RISKS AND TOOLS</b>	<b>1</b>
1.1. Environment to be audited	1
1.2. Scope of the Audit	4
1.2.1. Limitations of scanning and testing	4
1.3. Risks to the system	5
1.3.1. Overview	5
1.3.2. Threats	6
1.3.3. Vulnerabilities	8
1.4. Current State of Practice	9
1.4.1. Tools and Utilities	10
1.4.2. Control References	10
<b>SECTION 2: AUDIT CHECKLIST</b>	<b>12</b>
2.1. Physical	12
2.1.1. Item PH1: Physical	12
2.2. Server Hardening	13
2.2.1. Item SH1: Unneeded Windows Components Removed	13
2.2.2. Item SH2: File ACL	17
2.2.3. Item SH3: Computer Configuration - Audit Policy and Event Log	20
2.2.4. Item SH4: Computer Configuration - User Rights	24
2.2.5. Item SH5: Computer Configuration - Security Options	27
2.2.6. Item SH6: Computer Configuration – Registry Settings	30
2.2.7. Item SH7: Account Policies, PassProp and Protected Tools	38
2.2.8. Item SH8: Terminal Server Specific	47
2.3. Internal Scan for Open Ports and Services	50
2.3.1. Item IPS1: Internal Nessus Scan	50
2.4. External (Internet based) Scan for Open Ports and Services	52
2.4.1. Item EPS1: External Nessus Scan	52

<b>SECTION 3: RESULTS - AUDIT, MEASUREMENTS, AND CONTROLS</b>	<b>54</b>
<b>3.1. Physical</b>	<b>54</b>
3.1.1. Item PH1: Results - Physical	54
<b>3.2. Server Hardening</b>	<b>55</b>
3.2.1. Item SH1: Results - Unneeded Windows Components Removed	55
3.2.2. Item SH2: Results - File ACL	57
3.2.3. Item SH3: Results - Computer Configuration - Audit Policy and Event Log	60
3.2.4. Item SH4: Results - Computer Configuration - User Rights	61
3.2.5. Item SH5: Results - Computer Configuration - Security Options	62
3.2.6. Item SH6: Results - Computer Configuration - Registry Settings	63
3.2.7. Item SH7: Results - Account Policies, PassProp and Protected Tools	70
3.2.8. Item SH8: Results - Terminal Server Specific	86
<b>3.3. Internal Scan for Open Ports and Services</b>	<b>89</b>
3.3.1. Item IPS1: Results - Internal Nessus Scan	89
<b>3.4. External (Internet based) Scan for Open Ports and Services</b>	<b>92</b>
3.4.1. Item EPS1: Results - External Nessus Scan	92
 <b>SECTION 4: RISK ASSESSMENT</b>	 <b>94</b>
 <b>REFERENCES</b>	 <b>101</b>
 <b>APPENDIXES</b>	 <b>102</b>
<b>Appendix A – Checking File Permissions for SH2 and SH7</b>	<b>102</b>

## **Abstract**

The following paper is comprised of a security assessment of a small CPA firm (XZ CPA, LLC) that has deployed QuickBooks Accounting Edition on a Microsoft Windows 2000 Terminal Server for use by their customers via the Internet. The paper looks at the threat and vulnerabilities the current configuration poses to the firm and to the customers' information.

The audit was conducted to evaluate the current security posture of the terminal server and to provide information for the firm to decide on whether it needs to pursue alternative means to provide 24/7 availability to its customer book-keeping records. The paper will evaluate the terminal server configuration, the QuickBooks application configuration, and any protective measures, if any, in place.

1. Section 1 will describe the systems environment; define the scope of the audit to be performed, risks, and tools.
2. Section 2 will detail agreed on audit checklists to be conducted against the server.
3. Section 3 will document the results of each checklist item.
4. Section 4 will provide the overall risk assessment and findings, including any recommendations.

## **Section 1: Research - Audit, Scope, Risks and Tools**

### **1.1.Environment to be audited**

XZ CPA, LLC is a small accounting firm located in Colorado Springs, Co. The firm provides a wide variety of financial services to a number of small and medium sized businesses situated in the Colorado Springs Metro area. The owner of XZ CPA, LLC contracted a local computer company to deploy a Microsoft 2000 Terminal Server with QuickBooks 2002 Accounting Edition installed to allow customers to access their accounting books on a 24/7 availability basis from the Internet. The Terminal Server was deployed in early 2002 and has a small number of companies currently utilizing it from the Internet.

The initial discussions with the owner detailed the desire to expand the offering to all of his current QuickBooks customers in order to reduce the time he spends traveling to each customer site to update and audit that respective company accounting records. In response to some customer's questions concerning the security of such a configuration, the owner requested an evaluation of the current configuration and deployment of the Terminal Server and to make recommendations for changes to address security concerns.

The Server is a small single processor AMD server running Microsoft Windows 2000 Server SP4. Terminal Services is enabled in Application Mode with five Terminal Services Client Access Licenses.

System Information using the "Computer Management" MMC:

[System Summary]

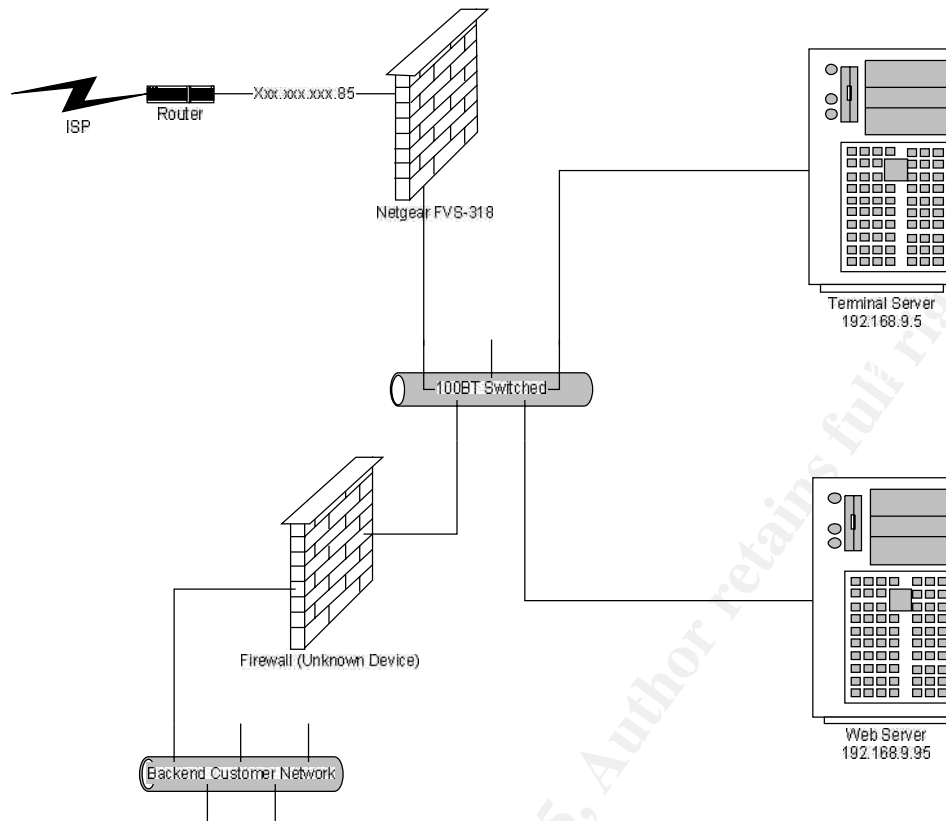
Item	Value
OS Name	Microsoft Windows 2000 Server
Version	5.0.2195 Service Pack 4 Build 2195
OS Manufacturer	Microsoft Corporation
System Name	SERVER1
System Manufacturer	Intel Corporation
System Model	GS81010A
System Type	X86-based PC
Processor	x86 Family 6 Model 8 Stepping 3 GenuineIntel ~697 Mhz
BIOS Version	04/19/00
Windows Directory	C:\WINNT
System Directory	C:\WINNT\system32
Boot Device	\Device\Harddisk0\Partition1
Locale	United States
User Name	XXXXXXXXXXXX\XXXX
Time Zone	Mountain Daylight Time

Total Physical Memory	522,544 KB
Available Physical Memory	245,468 KB
Total Virtual Memory	3,110,260 KB
Available Virtual Memory	2,657,648 KB
Page File Space	2,587,716 KB
Page File	C:\pagefile.sys
Page File	D:\pagefile.sys

The Internet connection is filtered through a NetGear FVS-318 Router/Firewall to create a DMZ. The Terminal server shares the DMZ with a Web Server. There is another firewall device on the network protecting a backend customer network that is currently out of scope of the audit and auditor has been requested to not scan any other devices or that backend network.



**Figure 1. Current Network configuration**



Both the Terminal Server and the NetGear FVS-318 are managed by an independent computer consultant on behalf of XZ CPA. Physical and logical access to the server will be coordinated through the consultant in order to perform this evaluation.

## **1.2. Scope of the Audit**

XZ CPA has requested the audit be limited solely to the Microsoft Terminal Server and its “Internet” presence.

### *1.2.1. Limitations of scanning and testing*

Scanning and testing will be performed only from within the DMZ that the Microsoft Terminal Server resides and from a predefined Internet location. All scans are to be performed directly against the single server and Internet IP address in coordination with the client’s computer consultant and during agreed upon time windows to avoid possible

loss of availability to customers. Ingress filter testing will be allowed against the single Internet IP. Egress Filtering will not be done at the request of the client.

Scanning against any other servers, networks, device or IP address is strictly forbidden.

### **1.3. Risks to the system**

#### *1.3.1. Overview*

Evaluating the risks and threats to this configuration requires an understanding of both the use of the system and what type of data is being accessed.

In this case, the use of the system is a remote user using the Microsoft Windows Terminal Services client or Remote Connection client to connect to the Terminal Server via a RDP session from the Internet. Each user has a unique account ID with an expiring password and specific NTFS permissions to the assigned QuickBooks data directory and account home directories. Information entered is normal accounting books transactions associated with that respective businesses operations. No File sharing, Telnet, FTP, or other remote access services are configured or allowed.

The end users are not currently utilizing the VPN capabilities of the NetGear FVS-318, however there is a single VPN configured for use by the computer consultant to perform normal system maintenance. Interviews with the computer consultant indicated that the original deployment defined the use of the NetGear ProSafe VPN Client, but was never implemented due to current customers not willing to purchase the software.

Risk shall be determined by evaluating the Threat, Vulnerability, and Likelihood.  
**(RISK=THREAT + VULNERABILITY + LIKELIHOOD)**

Auditor uses a 1-30 scale where 1 represents the lowest risk and 30 represents the highest risk. If a "Threat" or "Vulnerability" rating is not applicable to an evaluated item, a zero will be used.

Each Threat, Vulnerability, and Likelihood will be given a 1-10 rating in determining the quantitative threat score. The sum of the ratings will determine the RISK score for that

item. For each check with multiple items that are evaluated, the total of all risks will be averaged by dividing the sum of all the risk scores by the number of items (Total Risk = Sum of Risks / Number of items checked). Items meeting the test criteria will not be evaluated for a risk score.

### 1.3.2. Threats

Threats to the system are weighted based upon the amount of damage that can be done. A scale of 1-10 is used. 1 being a low potential of damage and 10 representing a high damage potential.

Threat	Capacity to do Damage
Administration Errors	<ul style="list-style-type: none"><li>• Data Loss</li><li>• Data Theft</li><li>• Data corruption</li><li>• Data destruction</li><li>• Loss of Availability (Denial of Service)</li></ul>
Physical	<ul style="list-style-type: none"><li>• Theft (Data and Hardware)</li><li>• Destruction (Data and Hardware)</li><li>• Data Loss</li><li>• Loss of Availability (Denial of Service)</li></ul>
Hackers	<ul style="list-style-type: none"><li>• Data Loss</li><li>• Data Theft</li></ul>

	<ul style="list-style-type: none"> <li>• Data corruption</li> <li>• Data destruction</li> <li>• Loss of Availability (Denial of Service)</li> </ul>
User Error	<ul style="list-style-type: none"> <li>• Data Loss</li> <li>• Data Theft</li> <li>• Data corruption</li> <li>• Data destruction</li> <li>• Loss of Availability (Denial of Service)</li> </ul>
Viruses	<ul style="list-style-type: none"> <li>• Data Loss</li> <li>• Data Theft</li> <li>• Data corruption</li> <li>• Data destruction</li> <li>• Loss of Availability (Denial of Service)</li> </ul>
MalWare	<ul style="list-style-type: none"> <li>• Data Loss</li> <li>• Data Theft</li> <li>• Data corruption</li> <li>• Data destruction</li> </ul>

	<ul style="list-style-type: none"> <li>• Loss of Availability (Denial of Service)</li> </ul>
--	--

### 1.3.3. Vulnerabilities

Threats to the system are weighted based upon the amount of damage that can be done. A scale of 1-10 is used. 1 being a low potential of damage and 10 representing a high exposure.

Vulnerabilities	Potential Impact
Misconfigured Software	Unauthorized access can lead to data loss, alteration, theft, and/or loss of availability  Introduction of MaWare and Viruses
Poor Software Access Controls	Unauthorized access can lead to data loss, alteration, theft, and/or loss of availability  Introduction of MaWare and/or Viruses
Poor Firewall configuration	Unauthorized access can lead to data loss, alteration, theft, and/or loss of availability – Not part of SOW
Unauthorized Remote Access	Unauthorized access can lead to data loss, alteration, theft, and/or loss of availability
No or Poor Documentation, including change management	Unauthorized access can lead to data loss, alteration, theft, and/or loss of availability  Unauthorized changes to the configuration can lead to data loss,

	<p>alteration, theft, and/or loss of availability</p> <p>Unable to restore systems/software/data to original or updated configuration in a reasonable period of time resulting in loss of company image/reputation</p> <p>Not part of SOW</p>
No or poor software/configuration backups	<p>Unable to restore systems/software/data to original or updated configuration in a reasonable period of time resulting in loss of company image/reputation</p> <p>Unable to restore systems/software/data to original or updated configuration in a reasonable period of time resulting in loss of customer data</p> <p>Not part of SOW</p>
Physical	<ul style="list-style-type: none"> <li>• Destruction/damage to the server or supporting networks can lead to loss of availability</li> <li>• Theft of the server can result in loss of data, potential loss of customer proprietary information, and loss of availability</li> <li>• Unauthorized access can lead to data loss, alteration, theft, and/or loss of availability</li> </ul> <p>Not part of SOW</p>

#### 1.4. Current State of Practice

The following references, tools and utilities are useful during the course of the audit.

### *1.4.1. Tools and Utilities*

#### *1.4.1.1. Nessus*

Nessus is a very powerful vulnerability scanner. Nessus is installed on a SuSe 9.0 Laptop and controlled via the Windows Client, for use in this audit.

<http://www.nessus.org>

#### *1.4.1.2. Security Configuration and Analysis Snap-In*

This is part of the Security Configuration Editor (SCE) MMC that is used in conjunction with the Security Templates to analyze and configure systems settings. It is extremely useful for conducting comparisons between existing and desired settings. It also significantly reduces the time and effort required to conduct base system setting checks.

[http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/snap\\_secmanager.htm](http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/snap_secmanager.htm)

More detailed information concerning the Snap-In can be found in the Microsoft Windows 2000 Security Hardening Guide, Chapter 6.

<http://www.microsoft.com/technet/Security/prodtech/win2000/win2khg/06tmpltts.mspx>

### *1.4.2. Control References*

Control References I used for the development of checklists for the Microsoft Terminal Server.

#### *1.4.2.1. Microsoft Terminal Server Checklist guides and references*

What better source than the OEM of the product? Microsoft has a convenient URL for accessing many of the checklists and recommendations for hardening Microsoft Servers. I placed an extremely heavy reliance on the checklists available from Microsoft. I would suggest downloading the hardcopy of the guide.

<http://www.microsoft.com/technet/security/topics/hardsys/default.mspx>

#### 1.4.2.2. *Checklist - Lachniet*

Another person by the name of Mark Lachniet very nicely posted one of his security checklists. Many of his URL references within this checklist are no longer valid, but it is a great starting point.

<http://mtip.net/aware/MarkLachnietChecklist.pdf>

#### 1.4.2.3. *Checklist – Corp-Sec*

Corp-Sec is a Non-Profit group that provides checklists and other information as Open-Source. I also used these checklists to cross-reference and expand the checklists developed in conjunction with the Microsoft provided checklists.

<http://www.corp-sec.net>

#### 1.4.2.4. *Windows 2000 and 2003 Server Physical/Logical Security Primer*

I found this online reference to be a wonderful resource for basic physical security recommendations.

<http://www.windowsecurity.com/articles/Windows-2000-2003-Server-Physical-Security-Part1.html>



## Section 2: Audit Checklist

### 2.1. Physical

#### 2.1.1. Item PH1: Physical

Reference:	<p>Robert J. Shimonski :Windows 2000 and 2003 Server Physical/Logical Security Primer at <a href="http://www.windowsecurity.com/articles/Windows-2000-2003-Server-Physical-Security-Part1.html">http://www.windowsecurity.com/articles/Windows-2000-2003-Server-Physical-Security-Part1.html</a></p> <p>Security Disciplines for Objective 1: Support at <a href="http://it.ojp.gov/documents/asp/disciplines/section1-2.htm">http://it.ojp.gov/documents/asp/disciplines/section1-2.htm</a></p> <p>Personal Experience</p>
Risk	<p>Lack of Physical security</p> <ul style="list-style-type: none"><li>• Damage and/or destruction of the server (Intentional or accidental)</li><li>• Loss and/or compromise of customers accounting data</li><li>• Loss of Productivity</li></ul>
Testing Criteria / Compliance Criteria	<p>Locate the server and evaluate the physical security of the room.</p> <ul style="list-style-type: none"><li>• Environmentally controlled?</li><li>• Locked Room?</li><li>• Access Control to room?</li><li>• Is room monitored?</li></ul>

	<ul style="list-style-type: none"> <li>• Backup AC Power?</li> </ul> <p>A Yes answer to all the questions will indicate Compliance</p>
--	--

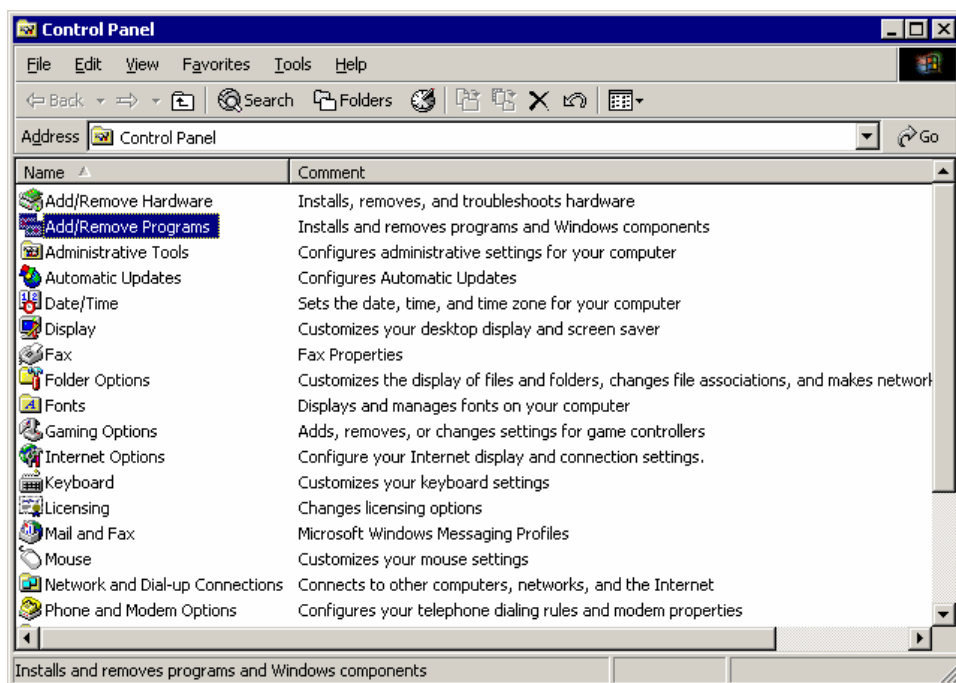
## 2.2. Server Hardening

### 2.2.1. Item SH1: Unneeded Windows Components Removed

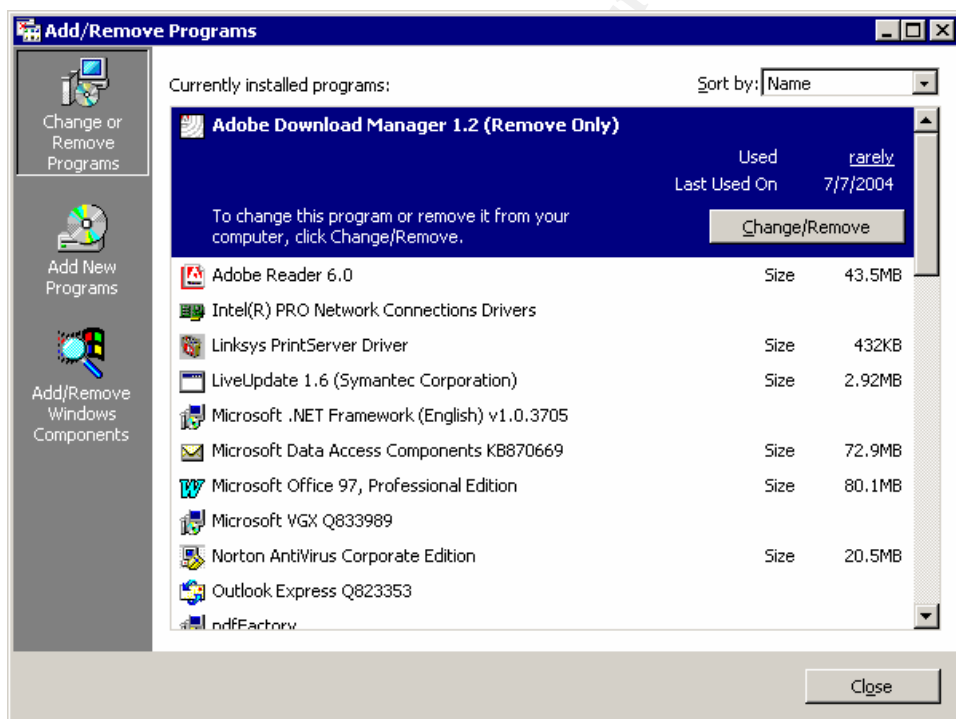
Reference:	<p>Corp Sec – Practical Security for the Corporate World at <a href="http://www.corp-sec.net/Hardening/win2k_h.html">http://www.corp-sec.net/Hardening/win2k_h.html</a></p> <p>Microsoft Windows 2000 Security Hardening Guide at <a href="http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&amp;displaylang=en">http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&amp;displaylang=en</a></p>
Risk	<p>Leaving unneeded windows components installed poses a risk of users abusing the services.</p> <p>Future application vulnerabilities may pose risks to the server</p> <ul style="list-style-type: none"> <li>• Abuse of non-business related applications</li> <li>• MalWare</li> </ul>
Testing Criteria / Compliance	<p>Tests and what determines compliance</p> <p>Check that the following applications have been removed or not installed.</p>

Criteria	<ul style="list-style-type: none"> <li>• Desktop Wallpaper</li> <li>• Document Templates</li> <li>• Communications (Chat, etc)</li> <li>• Games</li> <li>• Multimedia</li> <li>• IIS (Including FTP, NNTP, SMTP, FrontPage Extensions, Visual Interdev RAD)</li> <li>• Index Services</li> </ul> <p>A YES to the above checks will indicate Compliance.</p>
Test Nature	Objective

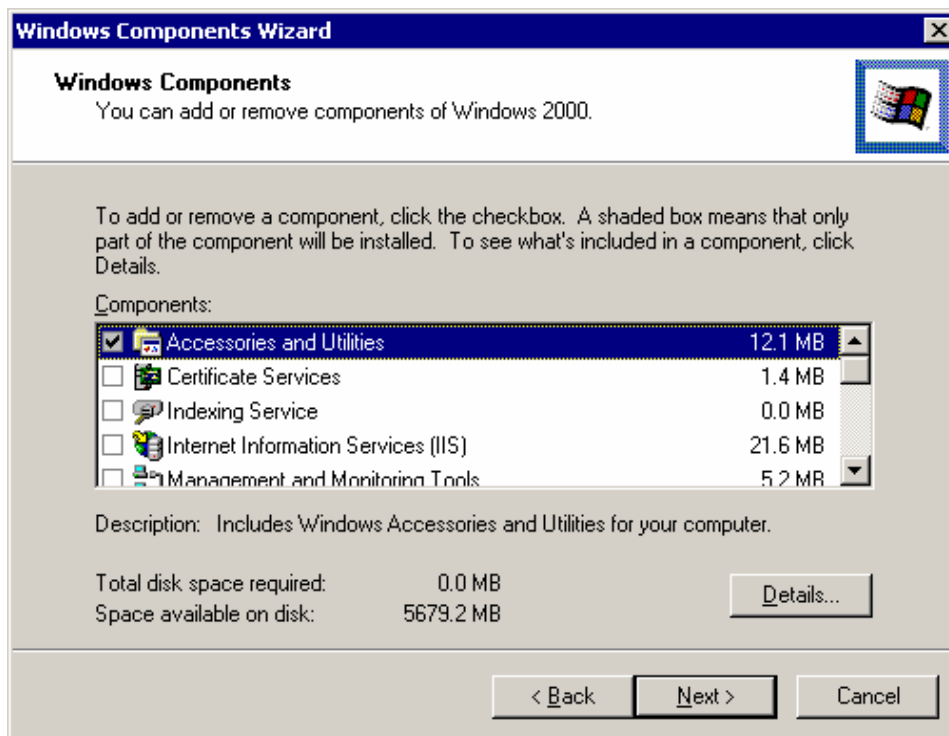
To check this setting, use the “Add/Remove Programs” wizard in the Control Panel.



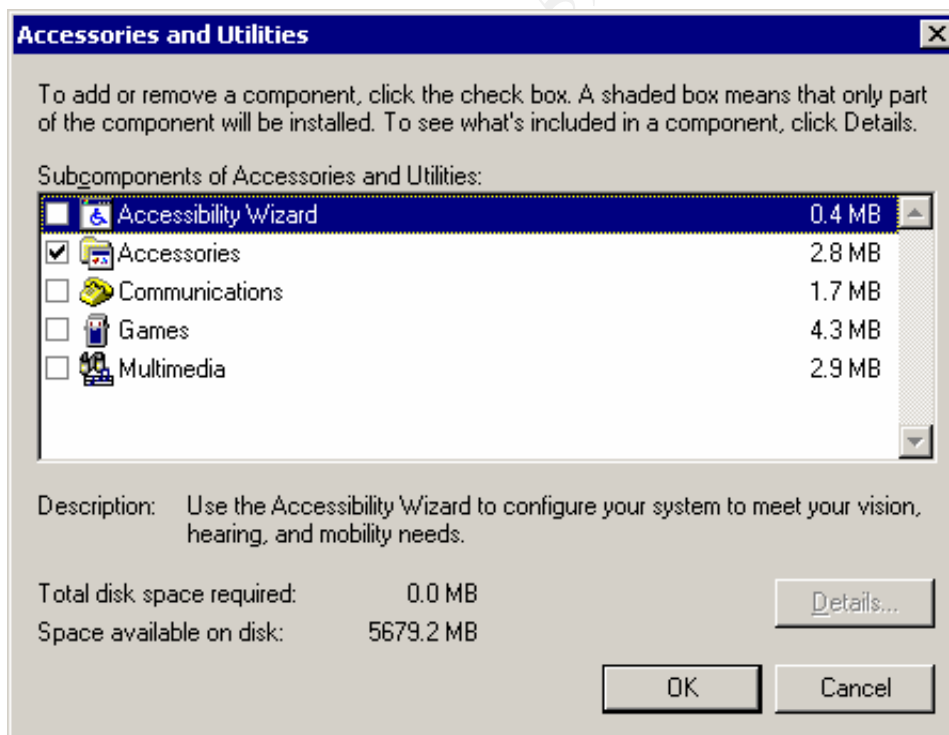
Click the “Add/Remove Windows Components” button on the left of the wizard.



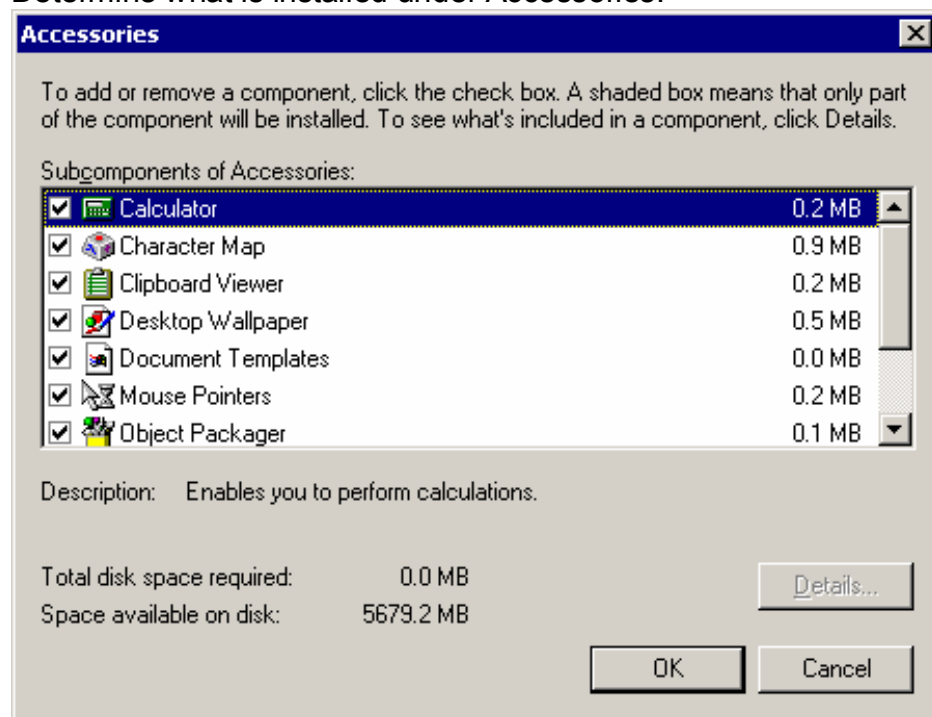
Check for installed components (IIS, Network Services, etc)



Check under “Accessories and Utilities” – Accessories should have some items selected. Highlight Accessories and click details.



Determine what is installed under Accessories:



Manually document deviations from the recommendations.

### 2.2.2. Item SH2: File ACL

Reference:	Corp Sec – Practical Security for the Corporate World P22 at <a href="http://www.corp-sec.net/Hardening/win2k_h.html">http://www.corp-sec.net/Hardening/win2k_h.html</a>
Risk	<p>Improper File ACL's on sensitive system directories and files can result in unintended access to system components.</p> <ul style="list-style-type: none"> <li>• MaWare installation</li> <li>• Access to system configuration data</li> <li>• Compromise, alteration, or destruction of data</li> <li>• Unauthorized activities (Bypassing of security mechanisms, corruption of the operating system,</li> </ul>

	installation of unauthorized software)
Testing Criteria / Compliance Criteria	<p>Using the Security Configuration and Analysis Snap-in – compare the following desired settings to the existing configuration using the pre-developed security template.</p> <p><b>NTFS Permissions settings</b></p> <p><b>C:\</b></p> <ul style="list-style-type: none"> <li>• Administrators (Full Control)</li> <li>• System (Full Control)</li> <li>• Authenticated Users (Read &amp; Execute)</li> </ul> <p><b>C:\boot.ini, c:\ntdetect.com, c:\ntldr</b></p> <ul style="list-style-type: none"> <li>• Administrators (Full Control)</li> <li>• System (Full Control)</li> <li>• Authenticated Users (Read &amp; Execute)</li> </ul> <p><b>C:\Program Files</b></p> <ul style="list-style-type: none"> <li>• Administrators (Full Control)</li> <li>• System (Full Control)</li> <li>• Authenticated Users (Read &amp; Execute)</li> </ul>

	<p><b>%systemroot%\repair</b></p> <ul style="list-style-type: none"> <li>• Administrators (Full Control)</li> <li>• System (Full Control)</li> <li>• Remove all others</li> </ul> <p><b>%systemroot%\security</b></p> <ul style="list-style-type: none"> <li>• Administrators (Full Control)</li> <li>• System (Full Control)</li> <li>• Remove all others</li> </ul> <p><b>%systemroot%\system32\config</b></p> <ul style="list-style-type: none"> <li>• Administrators (Full Control)</li> <li>• System (Full Control)</li> <li>• Remove all others</li> </ul> <p><b>%systemroot%\system32\dlcache</b></p> <ul style="list-style-type: none"> <li>• Administrators (Full Control)</li> <li>• System (Full Control)</li> <li>• Remove all others</li> </ul> <p><b>%systemroot%\system32\logfiles</b></p>
--	---



	<ul style="list-style-type: none"> <li>• Administrators (Full Control)</li> <li>• System (Full Control)</li> <li>• Remove all others</li> </ul> <p>A YES to the above checks will indicate Compliance</p>
Test Nature	Objective

Permissions can be checked manually or by a command script.

Run the following commands to determine current permissions on the respective directories.

```
cacIs c:\
cacIs c:\boot.ini
cacIs c:\ntldr
cacIs c:\ntdetect.com
cacIs c:\winnt\repair
cacIs c:\winnt\security
cacIs c:\winnt\system32\config
cacIs c:\winnt\system32\dlcache
cacIs c:\winnt\system32\logfiles
```

The output will look something like this.

```
c:\winnt\repair BUILTIN\Users:R
      BUILTIN\Users:(CI)(IO)(special access:)GENERIC_READ
      GENERIC_EXECUTE

      BUILTIN\Power Users:C
      BUILTIN\Power Users:(OI)(CI)(IO)C
      BUILTIN\Administrators:F
      BUILTIN\Administrators:(OI)(CI)(IO)F
      NT AUTHORITY\SYSTEM:F
      NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
      BUILTIN\Administrators:F
      CREATOR OWNER:(OI)(CI)(IO)F
```

### 2.2.3. Item SH3: Computer Configuration - Audit Policy and Event Log

Reference:	Corp Sec – Practical Security for the Corporate World at <a href="http://www.corp-sec.net/Hardening/win2k_h.html">http://www.corp-sec.net/Hardening/win2k_h.html</a>
------------	--

	<p>Microsoft Windows 2000 Security Hardening Guide Version 1.3 Checklist Chapter 5, Section 5.2 Local Policies page 24 at</p> <p><a href="http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&amp;displaylang=en">http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&amp;displaylang=en</a></p> <p>Personal Experience</p>
Risk	<p>If auditing is not enabled, then activities will not be logged.</p> <p>Unauthorized access attempts will not be logged</p> <p>Unauthorized user activity will not be logged</p> <p>Possible attacks/hacking attempts will not be logged/detected</p> <p>Log size too small to retain events for a reasonable period of time</p>
Testing Criteria / Compliance Criteria	<p>Using the Security Configuration and Analysis Snap-in – compare the following desired settings to the existing configuration using the pre-developed security template.</p> <p>Event Log;</p> <ul style="list-style-type: none"> <li>• Application Log : 5120 MB or greater, Overwrite as needed</li> <li>• Security Log : 10240 MB or greater, Overwrite as needed</li> <li>• System Log : 5120 MB or greater, Overwrite as</li> </ul>

	<p>needed</p> <ul style="list-style-type: none"> <li>• Restrict Guest Access to the Application Log – Enabled</li> <li>• Restrict Guest Access to the System Log – Enabled</li> <li>• Restrict Guest Access to the Security Log – Enabled</li> </ul> <p>Audit Policy:</p> <ul style="list-style-type: none"> <li>• Audit account logon events – Success, Failure</li> <li>• Audit account management – Success, Failure</li> <li>• Audit directory service access - Failure</li> <li>• Audit logon events – Success, Failure</li> <li>• Audit object access – Failure</li> <li>• Audit policy change – Success, Failure</li> <li>• Audit privilege use – No auditing</li> <li>• Audit process tracking – No auditing</li> <li>• Audit system events – Success, Failure</li> </ul> <p>A match or more stringent setting to the above checks will indicate Compliance.</p>
--	--

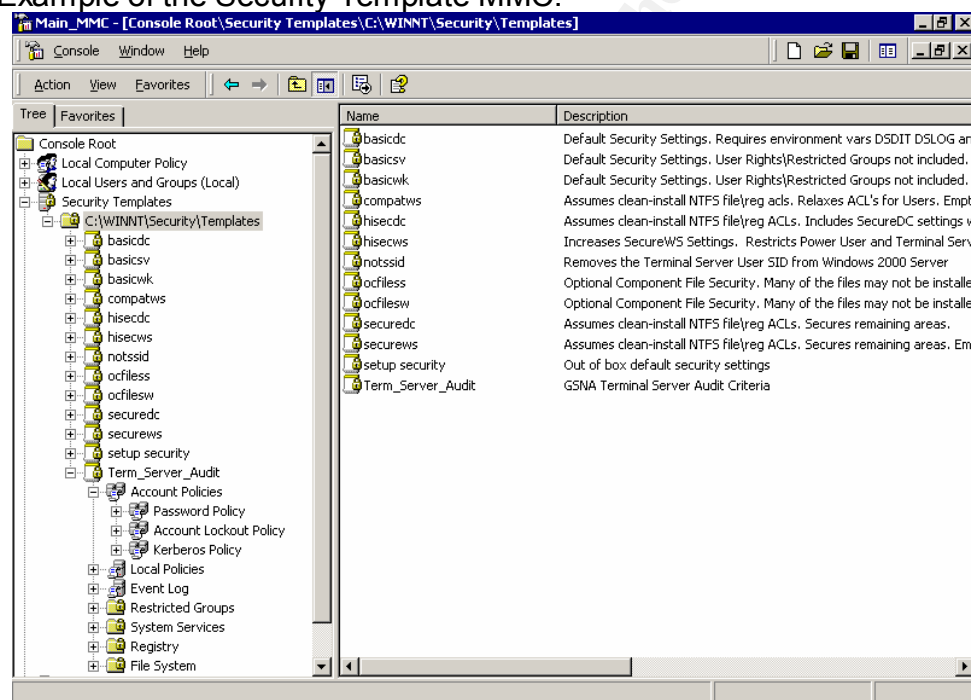
Test Nature	Objective
-------------	-----------

Permissions can be checked manually using the Windows File manager. However, to make the process repeatable and to provide a mechanism to implement the changes desired the auditor should use the “Security Templates MMC” to construct a template that the Security configuration and Analysis Snap-In can use to perform a comparison to the existing system configuration.

It is suggested that the template be based upon the Basicsv.inf security template as a starting point. Then using the Security Templates MMC set each parameter desired to be checked to the desired settings. By saving the template, the auditor can reuse the template in other audits.

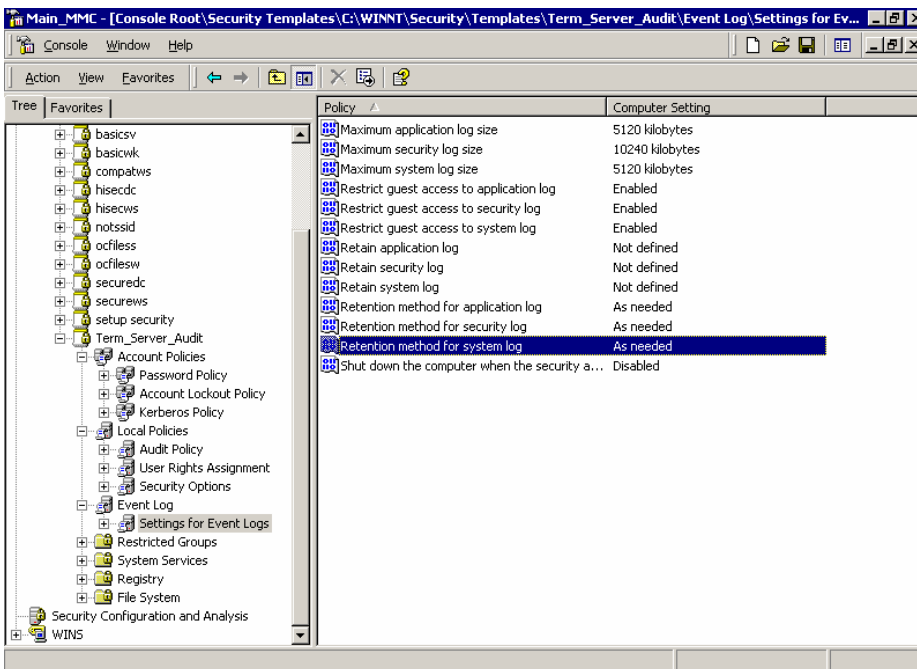
Items that cannot be checked via a security template should be checked manually or via a script file (depending on the complexity of the check).

#### Example of the Security Template MMC:

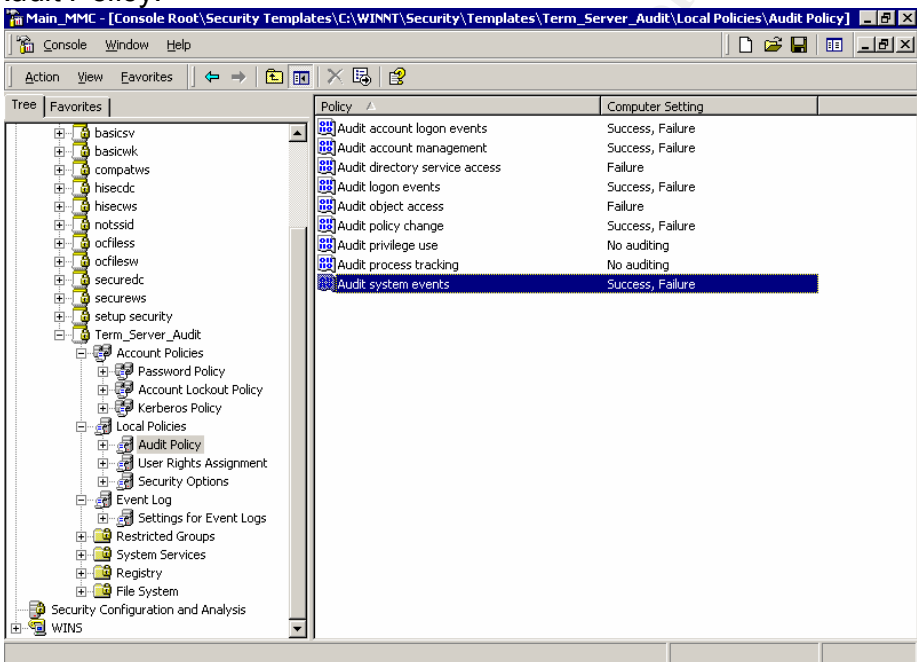


Now access the appropriate section of the template to set the desired settings you wish to test

#### Event Logs:



### Audit Policy:



### 2.2.4. Item SH4: Computer Configuration - User Rights

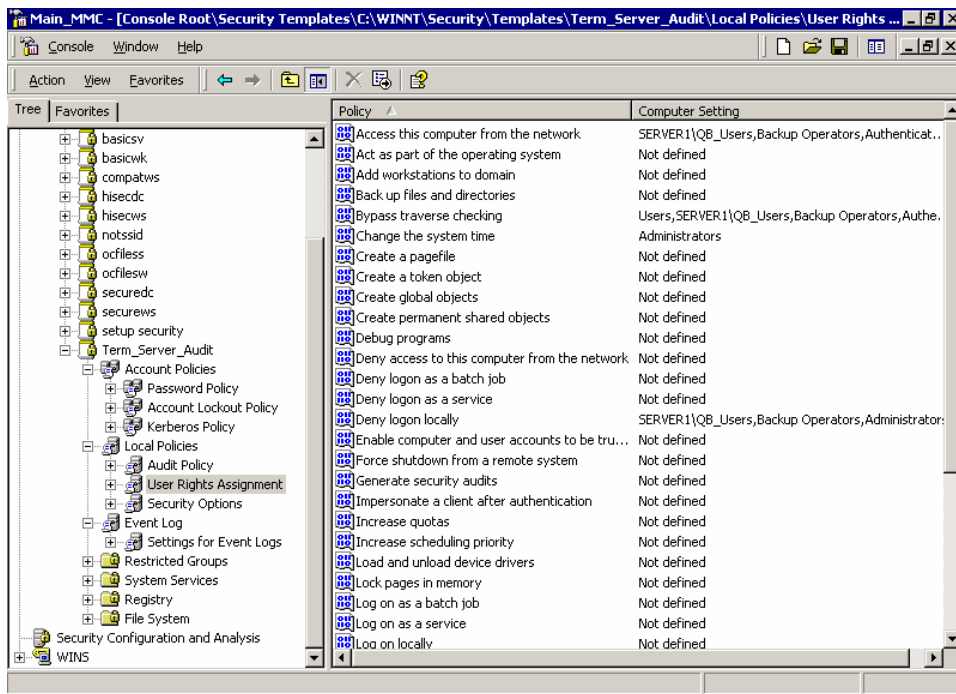
Reference:	Corp Sec – Practical Security for the Corporate World at <a href="http://www.corp-sec.net/Hardening/win2k_h.html">http://www.corp-sec.net/Hardening/win2k_h.html</a>
------------	--

	<p>Microsoft Windows 2000 Security Hardening Guide Version 1.3 Chapter 5, Section 5.2.2 Logon Rights and Privileges Page 27 at <a href="http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&amp;displaylang=en">http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&amp;displaylang=en</a></p> <p>Personal Experience</p>
Risk	<p>Improper User Rights can result in unintended access to system components.</p> <ul style="list-style-type: none"> <li>• MalWare installation</li> <li>• Access to other users data</li> <li>• Compromise, alteration, or destruction of data</li> <li>• Unauthorized activities (Shutdown the server, change system time, installation of unauthorized software)</li> </ul>
Testing Criteria / Compliance Criteria	<p>Using the Security Configuration and Analysis Snap-in – compare the following desired settings to the existing configuration using the pre-developed security template.</p> <ul style="list-style-type: none"> <li>• Access this computer from the network – Authenticated Users, Backup Operators, Administrators, TSA Users (define group)</li> </ul> <p style="text-align: center;"><b>Client users Group called “QB Users” for TSA Users</b></p> <ul style="list-style-type: none"> <li>• Act as part of the operating system – “Blank”</li> <li>• Add workstations to domain – “Blank”</li> <li>• Bypass traverse checking – Authenticated Users, Users,</li> </ul>

	<p>Backup Operators, Administrators</p> <ul style="list-style-type: none"> <li>• Change system time – Administrators</li> <li>• Deny logon through Terminal Services - ASPNET</li> <li>• Logon locally – Administrators, Backup Operators, TSE Users (<i>remove Users, and TsInternetUser</i>)</li> </ul> <p><b>Client users Group called “QB Users” for TSA Users</b></p> <ul style="list-style-type: none"> <li>• Profile single process - Administrators</li> <li>• Shutdown the system – Administrators, Backup Operators</li> </ul> <p>A YES to the above checks will indicate Compliance</p>
Test Nature	Objective

By this point, it will be assumed the auditor knows how to access the Security Templates MMC.

To set the User Rights to test, Go to “Local Policies, User Rights” and define all the desired test settings.



### 2.2.5. Item SH5: Computer Configuration - Security Options

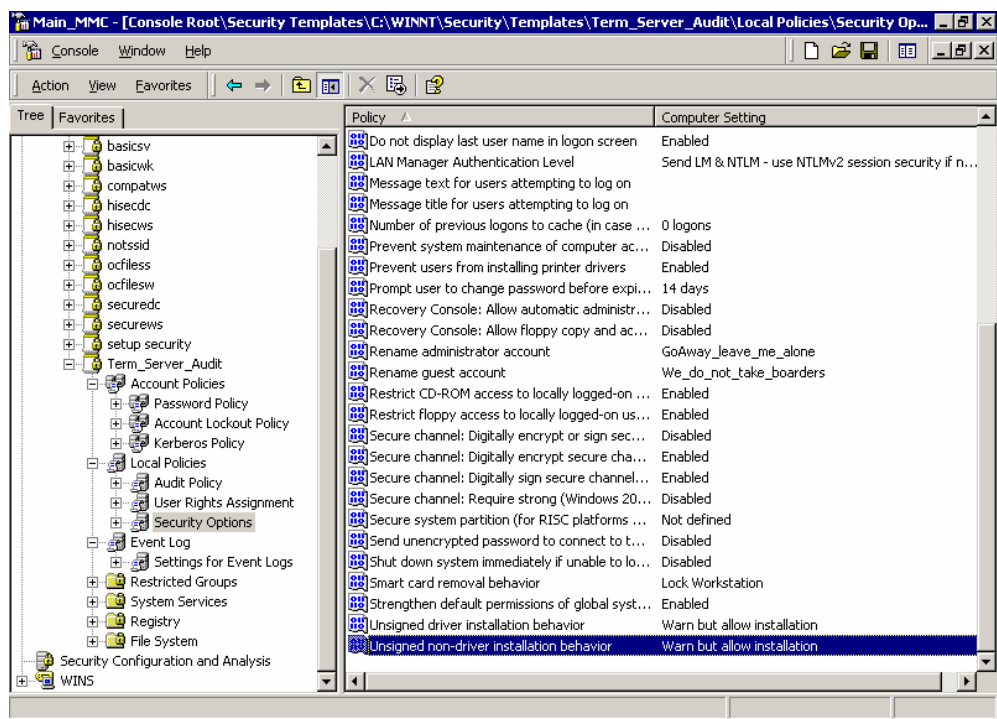
Reference:	<p>Corp Sec – Practical Security for the Corporate World at <a href="http://www.corp-sec.net/Hardening/win2k_h.html">http://www.corp-sec.net/Hardening/win2k_h.html</a></p> <p>Microsoft Windows 2000 Security Hardening Guide Version 1.3 Chapter 5, Section 5.2.3 Modify Security Options Page 30 at <a href="http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&amp;displaylang=en">http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&amp;displaylang=en</a></p> <p>Personal Experience</p>
Risk	<p>Improper Security Options can result in unintended access to system components.</p> <ul style="list-style-type: none"> <li>• MaWare installation</li> </ul>



	<ul style="list-style-type: none"> <li>• Access to other users data</li> <li>• Compromise, alteration, or destruction of data</li> <li>• Unauthorized activities (Share and account enumeration, unauthorized shutdown, removable media access, etc.)</li> <li>• Exposure of internal network resources</li> </ul>
Testing Criteria / Compliance Criteria	<p>Using the Security Configuration and Analysis Snap-in – compare the following desired settings to the existing configuration using the pre-developed security template.</p> <ul style="list-style-type: none"> <li>• Additional restrictions for anonymous connections – Do not allow enumeration of accounts and shares</li> <li>• Allow system to be shutdown without having to log on - Disabled</li> <li>• Digitally sign server communication (when possible) - Enabled</li> <li>• Do not display last name in logon screen - Enabled</li> <li>• LAN Manager Authentication Level – Send LM &amp; NTLM – use NTLM security if negotiated</li> <li>• Message Text for users attempting to log on – <i>“Warning message for users attempting access” Check with client for wording.</i></li> <li>• Message Title for users attempting to log on – WARNING!</li> <li>• Number of previous logons to cache – 0 logons</li> </ul>

	<ul style="list-style-type: none"> <li>• Rename administrator account – To client standard</li> <li>• Rename guest account – To client standard</li> <li>• Restrict CD-ROM access to locally logged-on user only – Enabled</li> <li>• Restrict floppy access to locally logged-on user only – Enabled</li> <li>• Smart card removal behavior – Lock Workstation</li> <li>• Strengthen default permissions of global system objects - Enabled</li> <li>• Unsigned driver installation behavior – Warn</li> <li>• Unsigned non-driver installation behavior - Warn</li> </ul> <p>A matching or more stringent setting to the above checks will indicate Compliance</p>
Test Nature	Objective

Using the “Security Templates MMC” define the settings desired under “Local Policies, Security Options”



### 2.2.6. Item SH6: Computer Configuration – Registry Settings

Reference:	<p>Corp Sec – Practical Security for the Corporate World at <a href="http://www.corp-sec.net/Hardening/win2k_h.html">http://www.corp-sec.net/Hardening/win2k_h.html</a></p> <p>Microsoft Windows 2000 Security Hardening Guide Version 1.3 Chapter 5, Section 5.2.4 Additional Security Settings Page 46 at <a href="http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&amp;displaylang=en">http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&amp;displaylang=en</a></p> <p>Mclure, Scambray, Kurtz. "Hacking Exposed: Fourth Edition" 2003 ISBN: 0-07-222742-7</p> <p>Personal Experience</p>
Risk	<p>Improper Security Options can result in unintended access to system components.</p> <ul style="list-style-type: none"> <li>• MalWare installation</li> <li>• Access to other users data</li> </ul>

	<ul style="list-style-type: none"> <li>• Compromise, alteration, or destruction of data</li> <li>• Unauthorized activities (Network Browsing, removable media access, etc.)</li> <li>• Exposure of internal network resources</li> </ul>
Testing Criteria / Compliance Criteria	<p>Using Regedt32.exe – compare the following desired settings to the existing configuration. Check that the following registry settings are defined.</p> <p><b>Remove OS2 and POSIX Subsystems</b> Hive: HKEY_LOCAL_MACHINE\System Key: \CurrentControlSet\Control\Session Manager\Subsystems Value: various Value Type: REG_MULTI_SZ Remove all entries</p> <p><b>Restrict Null Session Access</b> Hive: HKEY_LOCAL_MACHINE\System Key: \CurrentControlSet\Services\LanmanServer Value Type: REG_DWORD Value Name: RestrictNullSessAccess Value: 1</p> <p><b>Restrict null Session access over named pipes and shares</b> Hive: HKEY_LOCAL_MACHINE\System Key: \CurrentControlSet\Services\LanmanServer Value Type: REG_MULTI_SZ Value Name: NullSessionPipes Value Name: NullsessionShares Delete all entries</p> <p><b>Hide computer from the network browse list</b> Hive: HKEY_LOCAL_MACHINE\System Key: \CurrentControlSet\Services\LanmanServer Value Type: REG_DWORD Value Name: hidden Value: 1</p> <p><b>Disable 8.3 Filename Creation</b> Hive: HKEY_LOCAL_MACHINE\System Key: \CurrentControlSet\Control\FileSystem Value Type: REG_DWORD Value Name: NTFSDisable8dot3NameCreation Value: 1</p> <p><b>Syn Attack Protect</b> Hive: HKEY_LOCAL_MACHINE\SYSTEM</p>

	<p>Key: CurrentControlSet\Services\Tcpip\Parameters\  Name: SynAttackProtect  Type: REG_DWORD  Value: 2</p> <p><b>TcpMaxPortsExhausted</b>  Hive: HKEY_LOCAL_MACHINE\SYSTEM  Key: CurrentControlSet\Services\Tcpip\Parameters\  Name: TcpMaxPortsExhausted  Type: REG_DWORD  Value: 5</p> <p><b>Change TcpMaxDataRetransmissions</b>  Hive: HKEY_LOCAL_MACHINE\SYSTEM  Key: CurrentControlSet\Services\Tcpip\Parameters\  Name: TcpMaxDataRetransmissions  Type: REG_DWORD  Value: 3</p> <p><b>Dead Gateway Protection</b>  Hive: HKEY_LOCAL_MACHINE\SYSTEM  Key: CurrentControlSet\Services\Tcpip\Parameters\  Name: EnableDeadGWDetect  Type: REG_DWORD  Value: 0</p> <p><b>Router Discovery</b>  Hive: HKEY_LOCAL_MACHINE\SYSTEM  Key:  CurrentControlSet\Services\Tcpip\Parameters\Interfaces\[InterfaceName]  Name: PerformRouterDiscovery  Type: REG_DWORD  Value: 0</p> <p><b>Disable ICMP Redirects</b>  Hive: HKEY_LOCAL_MACHINE\SYSTEM  Key: CurrentControlSet\Services\Tcpip\Parameters\  Name: EnableICMPRedirect  Type: REG_DWORD  Value: 0</p> <p><b>Disable IP Source Routing</b>  Hive: HKEY_LOCAL_MACHINE  Key: System\CurrentControlSet\Services\Tcpip\Parameters  Name: DisableIPSourceRouting  Type: REG_DWORD  Value: 2</p> <p><b>TCP/IP KeepAlive Time</b>  Hive: HKEY_LOCAL_MACHINE  Key: System\CurrentControlSet\Services\Tcpip\Parameters</p>
--	---

	<p>Name: KeepAliveTime  Type: REG_DWORD  Value: 300000</p> <p><b>Disable External Name Release</b>  Hive: HKEY_LOCAL_MACHINE  Key: System\CurrentControlSet\Services\Tcpip\Parameters  Name: NoNameReleaseOnDemand  Type: REG_DWORD  Value: 1</p> <p><b>Enable PMTU Discovery</b>  <i>Note from Corp-Sec : Disabling PMTU discovery sets the default MTU to 576 for all foreign networks. In a properly segmented environment, this setting can cause 3X the amount of packets sent between VLANs.</i>  Hive: HKEY_LOCAL_MACHINE  Key: System\CurrentControlSet\Services\Tcpip\Parameters  Name: EnablePMTUDiscovery  Type: REG_DWORD  Value: 0</p> <p><b>TcpMaxConnectResponseRetransmissions</b>  Hive: HKEY_LOCAL_MACHINE  Key: System\CurrentControlSet\Services\Tcpip\Parameters  Name: TcpMaxConnectResponseRetransmissions  Type: REG_DWORD  Value: 2</p> <p><b>TcpMaxConnectRetransmissions</b>  Hive: HKEY_LOCAL_MACHINE  Key: System\CurrentControlSet\Services\Tcpip\Parameters  Name: TcpMaxConnectRetransmissions  Type: REG_DWORD  Value: 3</p> <p><b>Security Filters</b>  Hive: HKEY_LOCAL_MACHINE  Key: System\CurrentControlSet\Services\Tcpip\Parameters  Name: EnableSecurityFilters  Type: REG_DWORD  Value: 1</p> <p><b>Disable LMHASH creation</b>  Hive: HKEY_LOCAL_MACHINE  Key: System\CurrentControlSet\Control\LSA  Name: NoLMHASH  Key based setting, no Value required</p> <p><b>Disable All Autorun</b>  Hive: HKEY_LOCAL_MACHINE</p>
--	--

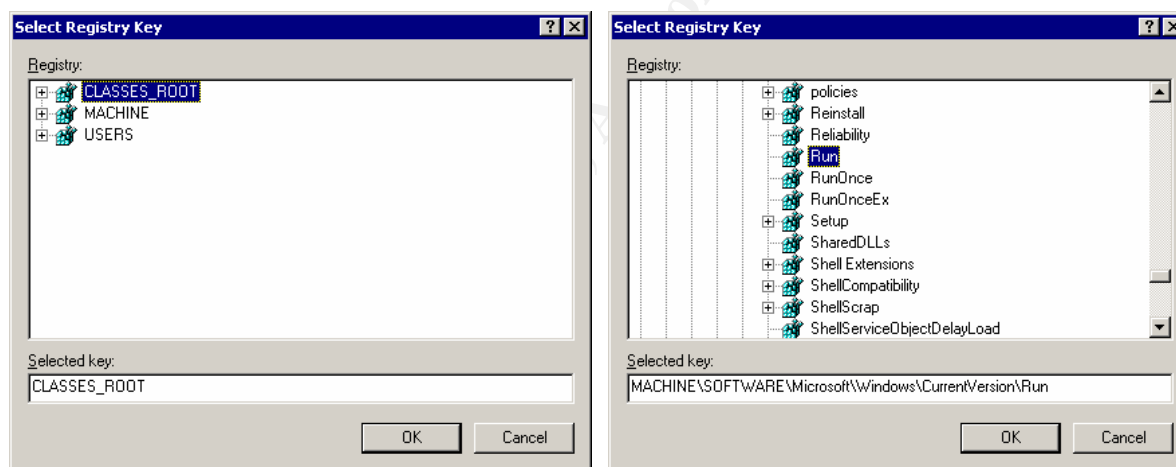
	<p>Key: Software\Microsoft\Windows\CurrentVersion\Policies\Explorer  Name: NoDriveTypeAutoRun  Type: REG_DWORD  Value: 0xFF  Key based setting, no Value required  Key based setting, no Value required  <b>Harden NTLM SSP</b>  Hive: HKEY_LOCAL_MACHINE  Key: System\CurrentControlSet\Control\LSA  Name: NtlmMinClientSec and NtlmMinServerSec  Type: REG_DWORD  Value: 0x20080030  <b>Permissions on the Registry (do these Manually)</b>  Using the Security Configuration and Analysis Snap-in – compare the following desired settings to the existing configuration using the pre-developed security template.  <i><b>If setting the permissions - Allow Inheritance is <u>disabled</u>, copy the permissions when resetting the Key/Value permissions</b></i>  Hive: HKEY_LOCAL_MACHINE  Key: <b>Software\Microsoft\Windows\CurrentVersion\Run</b> <ul style="list-style-type: none"> <li>• Administrator (Full Control)</li> <li>• SYSTEM (Full Control)</li> <li>• Creator Owner (Full Control)</li> <li>• Authenticated Users (Read)</li> </ul> Hive: HKEY_LOCAL_MACHINE  Key: <b>Software\Microsoft\Windows\CurrentVersion\RunOnce</b> <ul style="list-style-type: none"> <li>• Administrator (Full Control)</li> <li>• SYSTEM (Full Control)</li> <li>• Creator Owner (Full Control)</li> <li>• Authenticated Users (Read)</li> </ul> Hive: HKEY_LOCAL_MACHINE  Key: <b>Software\Microsoft\Windows\CurrentVersion\RunOnceEx</b> </p>
--	--

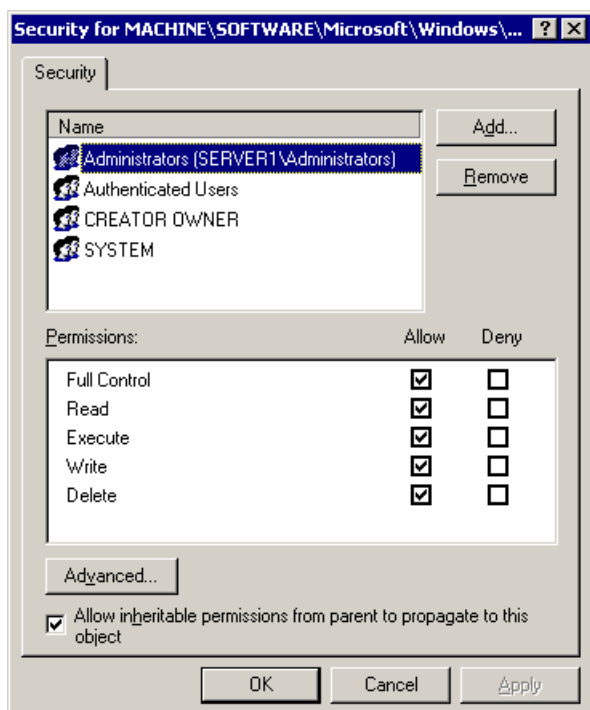
	<ul style="list-style-type: none"> <li>• Administrator (Full Control)</li> <li>• SYSTEM (Full Control)</li> <li>• Creator Owner (Full Control)</li> <li>• Authenticated Users (Read)</li> </ul> <p>Hive: HKEY_LOCAL_MACHINE Key: <b>Software\Microsoft\Windows\CurrentVersion\Uninstall</b></p> <ul style="list-style-type: none"> <li>• Administrator (Full Control)</li> <li>• SYSTEM (Full Control)</li> <li>• Creator Owner (Full Control)</li> <li>• Authenticated Users (Read)</li> </ul> <p>Hive: HKEY_LOCAL_MACHINE Key: <b>Software\Microsoft\Windows\CurrentVersion\AeDebug</b></p> <ul style="list-style-type: none"> <li>• Administrator (Full Control)</li> <li>• SYSTEM (Full Control)</li> <li>• Creator Owner (Full Control)</li> <li>• Authenticated Users (Read)</li> </ul> <p>Hive: HKEY_LOCAL_MACHINE Key: <b>Software\Microsoft\Windows\CurrentVersion\WinLogon</b></p> <ul style="list-style-type: none"> <li>• Administrator (Full Control)</li> <li>• SYSTEM (Full Control)</li> <li>• Creator Owner (Full Control)</li> </ul>
--	--



	<ul style="list-style-type: none"> <li>Authenticated Users (Read)</li> </ul> <p>Hive: HKEY_LOCAL_MACHINE Key: <b>Software\Microsoft\Rpc</b></p> <ul style="list-style-type: none"> <li>Administrator (Full Control)</li> <li>SYSTEM (Full Control)</li> <li>Authenticated Users (Read)</li> </ul> <p>A matching or more stringent setting to the above checks will indicate Compliance</p>
Test Nature	Objective

To check/set the Permissions on a Registry Key, use the Security template to compare to:

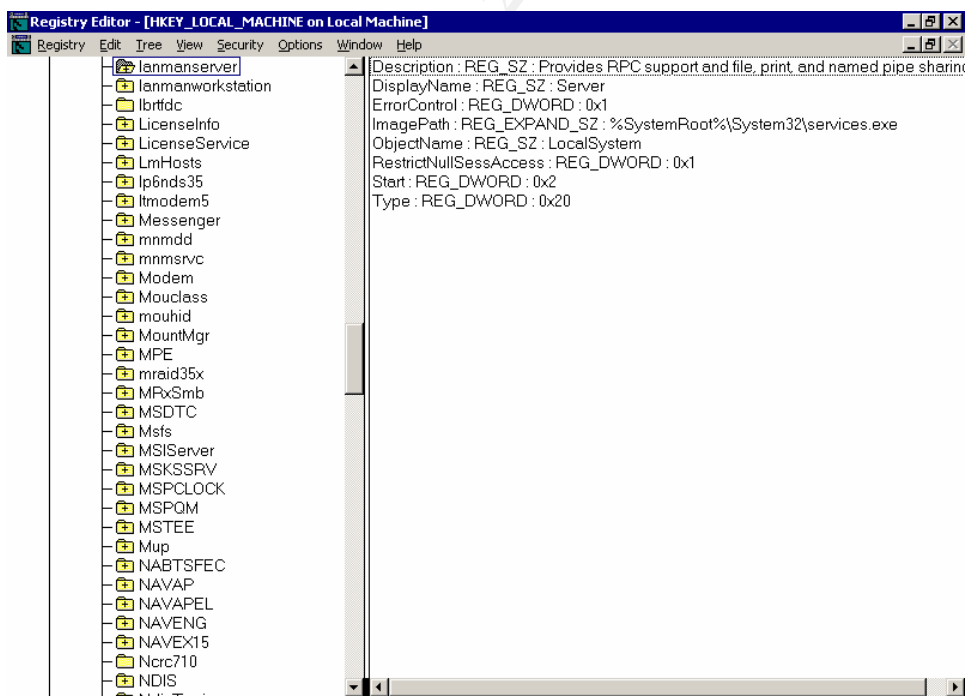




For the Registry contents. Manually check the entries or create a script to dump the contents.

Using Regedt32, browse to each desired Key and read the Value:

Example of trying to find the  
HKLM\CurrentControlSet\Services\LanmanServer\RestrictNullAccess Key Value:



### 2.2.7. Item SH7: Account Policies, PassProp and Protected Tools

Reference:	Corp Sec – Practical Security for the Corporate World Windows 2000 Server Hardening Checklist v3.0 Page 11 at <a href="http://www.corp-sec.net/Hardening/win2k_h.html">http://www.corp-sec.net/Hardening/win2k_h.html</a> Personal Experience
Risk	Improper Security and Password Options can result in unintended access to system components. <ul style="list-style-type: none"><li>• Malware installation</li><li>• Unintended utility replacement</li><li>• Compromise, alteration, or destruction of data</li><li>• Unauthorized activities (Telnet, FTP, Network Browsing, Registry editing, etc.)</li><li>• Exposure of internal network resources</li></ul>
Testing Criteria / Compliance Criteria	<b>Protect the Administrator account from continual logon attempts by allowing lockout.</b> Auditor should check by running PassProp.exe with no parameters. You can obtain the PassProp utility from the Windows 2000 Resource Kit. Using the Security Configuration and Analysis Snap-in – compare the following desired settings to the existing configuration using the pre-developed security template. Password Policies <ul style="list-style-type: none"><li>• 15 passwords remembered</li><li>• Maximum Password Age = 90 Days</li><li>• Minimum Password Age = 5 days</li></ul>

	<ul style="list-style-type: none"> <li>• Minimum Password Length = 8 characters</li> <li>• Password must meet complexity requirements = Enabled</li> <li>• Store password in reversible encryption for all users in the domain = Disabled</li> </ul> <p>Account Lockout Policy</p> <ul style="list-style-type: none"> <li>• Account lockout duration = 30 minutes</li> <li>• Account lockout threshold = 5 attempts</li> <li>• Reset account lockout counter after = 30 minutes</li> </ul> <p><b>The following tools should have their permissions set to:</b></p> <ul style="list-style-type: none"> <li>• Administrator Group (Full Control)</li> <li>• Remove all others</li> </ul> <p>If the Windows 2000 resource kit has been installed (and is required by the systems administrators), locate the directory that the Administrator has installed it and set the directory and all files to the above permission settings.</p> <p>In the Winnt Subdirectory</p> <ul style="list-style-type: none"> <li>• RegEdit.exe</li> </ul> <p>In the Winnt\System32 directory:</p> <ul style="list-style-type: none"> <li>• append.exe</li> <li>• attrib.exe</li> <li>• cacls.exe</li> </ul>
--	--

	<ul style="list-style-type: none"><li>• change.exe</li><li>• chcp.com</li><li>• chglogon.exe</li><li>• chgport.exe</li><li>• chgusr.exe</li><li>• chkdisk.exe</li><li>• chkntfs.exe</li><li>• cipher.exe</li><li>• cluster.exe</li><li>• cmd.exe</li><li>• command.com</li><li>• compact.exe</li><li>• convert.exe</li><li>• cscript.exe</li><li>• dcpromo.exe</li><li>• debug.exe</li><li>• dfscmd.exe</li></ul>
--	---

	<ul style="list-style-type: none"><li>• diskcomp.com</li><li>• diskcopy.com</li><li>• doskey.exe</li><li>• edlin.exe</li><li>• exe2bin.exe</li><li>• expand.exe</li><li>• fc.exe</li><li>• find.exe</li><li>• findstr.exe</li><li>• finger.exe</li><li>• forcedos.exe</li><li>• format.com</li><li>• ftp.exe</li><li>• hostname.exe</li><li>• iisreset.exe</li><li>• ipconfig.exe</li><li>• ipxroute.exe</li></ul>
--	--

	<ul style="list-style-type: none"><li>• label.exe</li><li>• logoff.exe</li><li>• makecab.exe</li><li>• mem.exe</li><li>• mmc.exe</li><li>• mode.com</li><li>• more.com</li><li>• mountvol.exe</li><li>• msg.exe</li><li>• nbtstat.exe</li><li>• net.exe</li><li>• net1.exe</li><li>• netsh.exe</li><li>• netstat.exe</li><li>• nslookup.exe</li><li>• ntbackup.exe (May need to have Backup Operators as well)</li><li>• ntdsutil.exe</li></ul>
--	---

	<ul style="list-style-type: none"><li>• ntsd.exe</li><li>• os2.exe</li><li>• passprop.exe</li><li>• pathping.exe</li><li>• ping.exe</li><li>• posix.exe</li><li>• print.exe</li><li>• query.exe</li><li>• rasdial.exe</li><li>• rcp.exe</li><li>• recover.exe</li><li>• regedt32.exe</li><li>• regini.exe</li><li>• register.exe</li><li>• regsvr32.exe</li><li>• replace.exe</li><li>• reset.exe</li></ul>
--	---

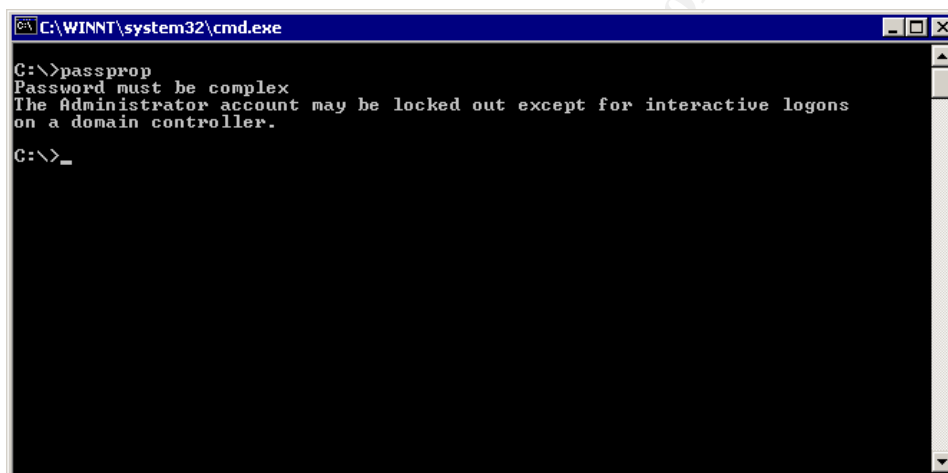


	<ul style="list-style-type: none"><li>• rexec.exe</li><li>• route.exe</li><li>• routemon.exe</li><li>• router.exe</li><li>• rsh.exe</li><li>• runas.exe</li><li>• runonce.exe</li><li>• secedit.exe</li><li>• setpwd.exe</li><li>• shadow.exe</li><li>• share.exe</li><li>• snmp.exe</li><li>• snmptrap.exe</li><li>• srvmgr.exe</li><li>• subst.exe</li><li>• sysedit.exe</li><li>• syskey.exe</li></ul>
--	---

	<ul style="list-style-type: none"><li>• taskmgr.exe</li><li>• telnet.exe</li><li>• termsrv.exe</li><li>• tftp.exe</li><li>• tlntadmn.exe</li><li>• tlntsess.exe</li><li>• tlntsrv.exe</li><li>• tracert.exe</li><li>• tree.com</li><li>• tsadmin.exe</li><li>• tscon.exe</li><li>• tsdiscon.exe</li><li>• tskill.exe</li><li>• tsprof.exe</li><li>• tsshutdn.exe</li><li>• usmgr.exe</li><li>• winmsd.exe</li></ul>
--	---

	<ul style="list-style-type: none"> <li>• winver.exe</li> <li>• wmimgmt.msc</li> <li>• wscript.exe</li> <li>• xcopy.exe</li> </ul> <p>(Based on the tool list from Corp-Sec Hardening Checklist P11 with some additions by myself) Matching or more stringent settings to the above checks will indicate Compliance</p>
Test Nature	Objective

To check if Passprop has been set correctly. Open a DOS Command Prompt and just type PassProp without any command switches.

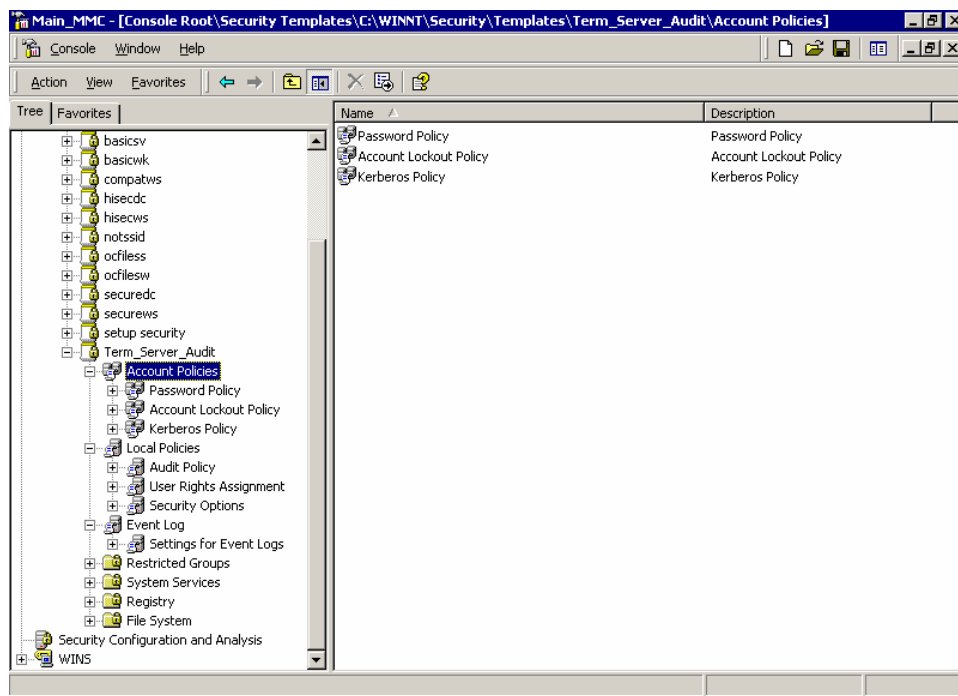


```

C:\WINNT\system32\cmd.exe
C:\>passprop
Password must be complex
The Administrator account may be locked out except for interactive logons
on a domain controller.
C:\>_

```

Set the desired test settings in the template under the Account Policies section.



For the remaining File permissions, these can be checked by using the `cacls` utility to list out the file permissions of each file:  
`cacls c:\winnt\system32\append.exe`

Would display something like  
`c:\winnt\system32\append.exe BUILTIN\Users:R`  
`BUILTIN\Power Users:R`  
`BUILTIN\Administrators:F`  
`NT AUTHORITY\SYSTEM:F`  
`Everyone:R`

This would be done against each file listed.  
This is best done by a batch file and output the results to a text file for comparison and documentation.

Appendix A contains the contents of the batch file I will run for this check.

### 2.2.8. Item SH8: Terminal Server Specific

Reference:	Corp Sec – Practical Security for the Corporate World - Windows 2000 Terminal Server Hardening Checklist v3.0Page 17 at
------------	---

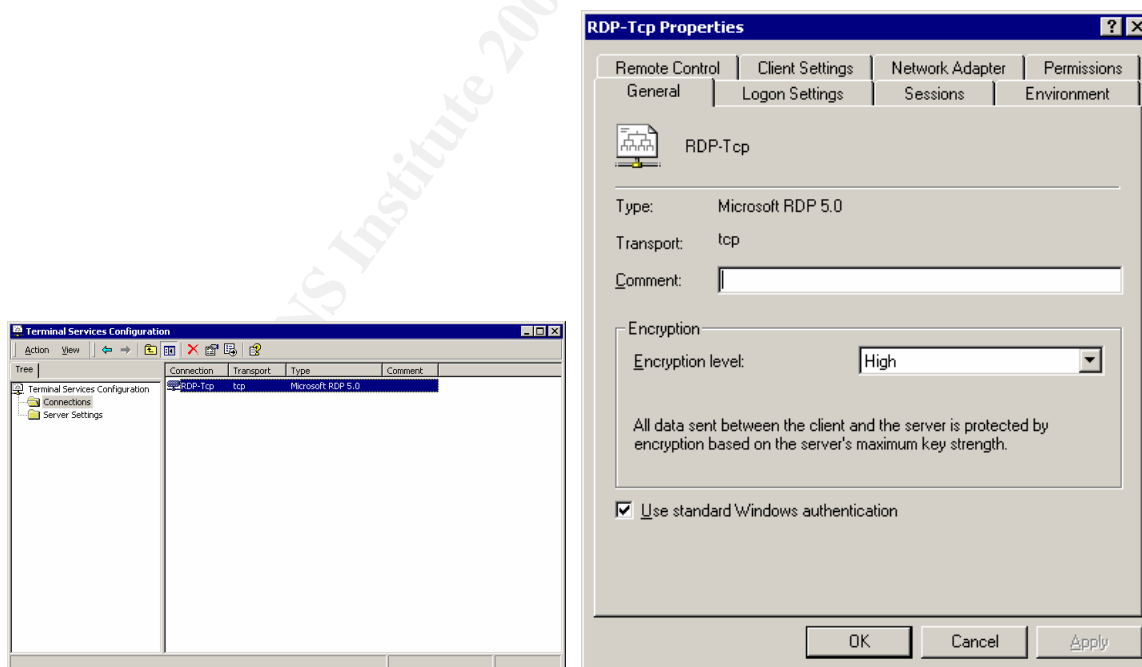
	<a href="http://www.corp-sec.net/Hardening/win2k_h.html">http://www.corp-sec.net/Hardening/win2k_h.html</a>  Personal Experience
Risk	Improperly configured terminal server settings can lead to unauthorized access, monitoring, and data corruption
Testing Criteria / Compliance Criteria	Terminal Services MMC  Under RDP Connections Properties  General Tab <ul style="list-style-type: none"> <li>• High Encryption selected</li> </ul> Sessions Tab <ul style="list-style-type: none"> <li>• End Disconnected Session = 30 Minutes</li> <li>• Active Session Limit = Never</li> <li>• Idle Session Limit = 1 hr</li> <li>• When a session limit is reached or connection is broken = End session</li> </ul> Client Settings Tab  (Note: Users need Printer and Clipboard Mapping in this configuration, we would normally disable these services) <ul style="list-style-type: none"> <li>• LPT port mapping = Disabled</li> <li>• COM port mapping = Disabled</li> </ul>

	<p>Permissions</p> <ul style="list-style-type: none"> <li>• Specific deny access to the local Administrator account and the ASPNET account (if present)</li> <li>• Grant Permission to the specific user groups allowed to access this server.</li> </ul>
Test Nature	Objective

This check is easier and faster to just do manually.

Open the Terminal Services Configuration MMC from the Control Panel

Select RDP Connection and right-click to select "Properties"



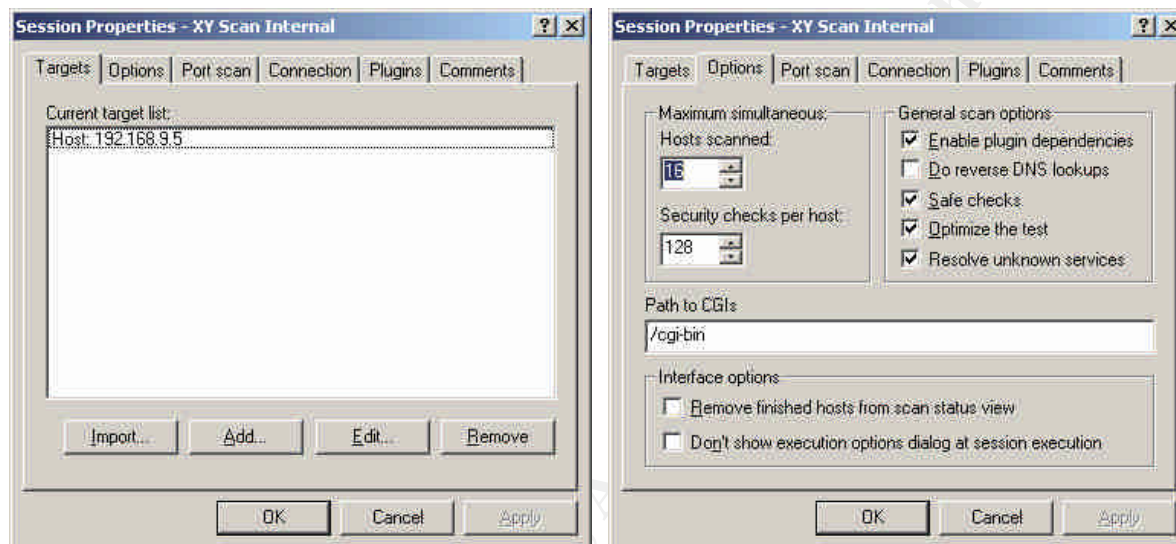
## 2.3. Internal Scan for Open Ports and Services

### 2.3.1. Item IPS1: Internal Nessus Scan

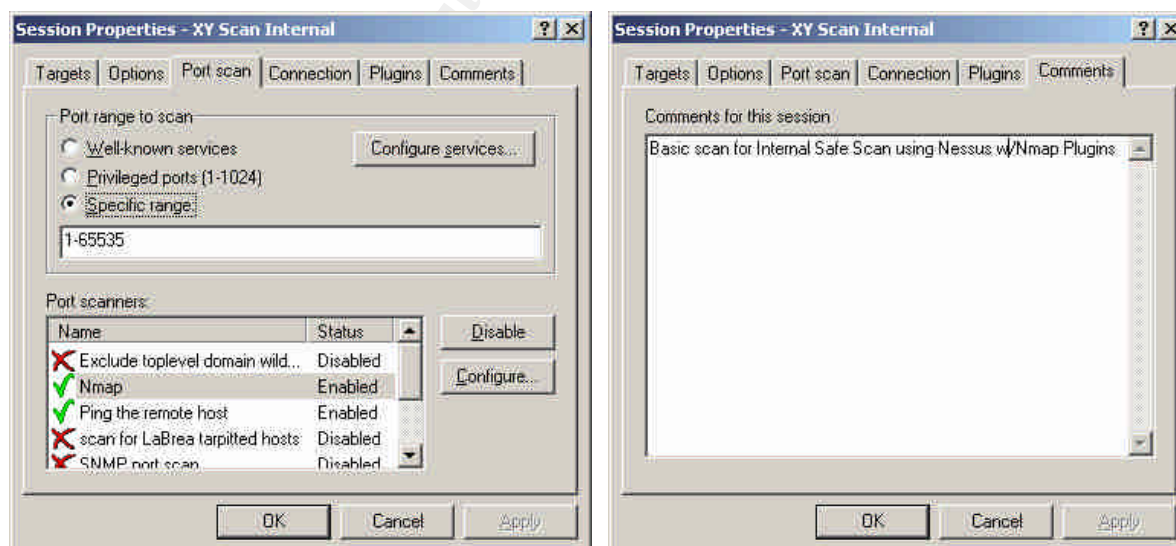
Reference:	<p>Nessus scanning on Windows Domain Version 1.0 – Sunil Vakharia at <a href="http://sunil.host.sk/">http://sunil.host.sk/</a> or <a href="http://www.nessus.org/doc/nessus_windows_scanning.pdf">http://www.nessus.org/doc/nessus_windows_scanning.pdf</a></p> <p>Nessus at <a href="http://www.nessus.org/documentation.html">http://www.nessus.org/documentation.html</a></p>
Risk	<p>Offering unintended services or misconfigured services can pose a threat to the server, data, and users.</p> <ul style="list-style-type: none"><li>• MalWare/Backdoor software could be installed or accessed without the users knowledge (MalWare)</li><li>• Data theft and/or corruption</li><li>• Loss of availability of the server (DOS)</li></ul>
Testing Criteria / Compliance Criteria	<p>Conduct a “safe” port scan against the server from a network location on the DMZ.</p> <p>Use Nessus to identify and check for open port vulnerabilities in “Safe Check” to prevent unintended damage to the system.</p> <p>Note that Egress Filter testing is <b><u>not being performed</u></b> per client request.</p> <p>Nessus Laptop will be connected to the DMZ network and will perform a “Default Scan” with Safe Check selected (see below image).</p>

Test Nature	Both Objective and Subjective
-------------	-------------------------------

Using the Windows Nessus Control console. Identify the Target IP and insure you select “Safe Checks”



Define your Port Scan Settings:





## 2.4. External (Internet based) Scan for Open Ports and Services

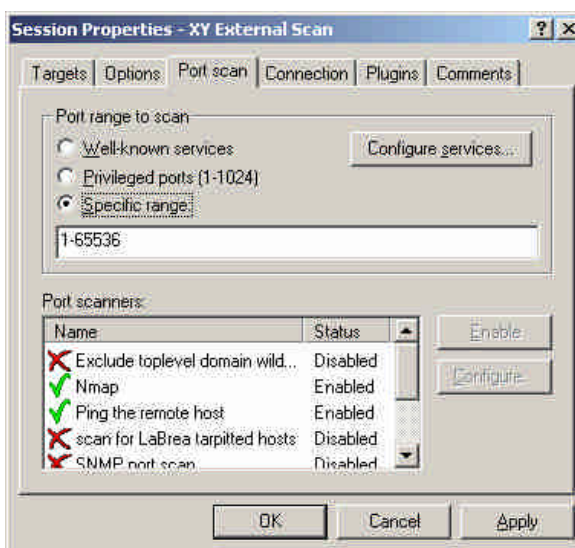
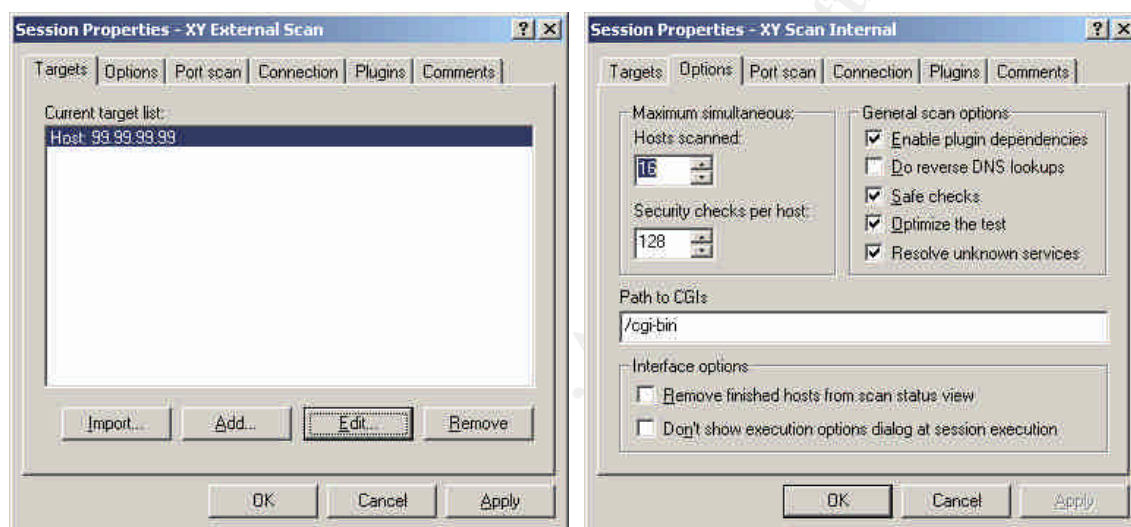
### 2.4.1. Item EPS1: External Nessus Scan

Reference:	<p>Nessus scanning on Windows Domain Version 1.0 – Sunil Vakharia at <a href="http://sunil.host.sk/">http://sunil.host.sk/</a> or <a href="http://www.nessus.org/doc/nessus_windows_scanning.pdf">http://www.nessus.org/doc/nessus_windows_scanning.pdf</a></p> <p>Nessus at <a href="http://www.nessus.org/documentation.html">http://www.nessus.org/documentation.html</a></p>
Risk	<p>Offering unintended services or misconfigured services can pose a threat to the server, data, and users.</p> <ul style="list-style-type: none"><li>• MaWAre/Backdoor software could be installed or accessed without the users knowledge (MaWAre)</li><li>• Data theft and/or corruption</li><li>• Loss of availability of the server (DOS)</li></ul>
Testing Criteria / Compliance Criteria	<p>Conduct a “safe” port scan against the server from an Internet location`.</p> <p>Use Nessus to identify and check for open port vulnerabilities in “Safe Check” to prevent unintended damage to the system.</p> <p>Nessus Laptop will be connected to the Internet at a remote location and will perform a “Default Scan” with Safe Mode selected (see below image) against the single external IP address as provided by the Client.</p> <p>This test will evaluate the Ingress Filtering.</p>

	Comparisons of results of Internal scan to be done.
Test Nature	Both Objective and Subjective

I will be using the identical scanning parameters as the internal scan with the exception of the target IP address.

Using the Windows Nessus Control console. Identify the Target IP and insure you select "Safe Checks"



Define your Port Scan Settings:

## Section 3: Results - Audit, Measurements, and Controls

### 3.1. Physical

#### 3.1.1. Item PH1: Results - Physical

Findings	<ul style="list-style-type: none"><li>• Environmentally controlled?  YES</li><li>• Locked Room?  YES</li><li>• Access Control to room?  YES, but no visitors log or physical guards</li><li>• Is room monitored?  YES, keypad security system with motion sensors and fire sensors</li><li>• Backup AC Power?  YES, UPS and manual backup generator</li></ul>
----------	---

Items that I feel should be addressed:

Improvements to the Access Controls are recommended. Lack of a visitor's log, video surveillance, or a physical security guard can lead to access by someone that could have obtained the security pad code AND Key to the door. Interviews with the computer consultant indicated that only four people hold keys to the room and the keypad access code is changed every 90 days.

Risk (9) = Threat (5) + Likelihood (1) + Vulnerability (3)

This item will be rated as a **LOW**.

Improvements to the Backup AC power are recommended. With the advent of winter in the Rocky Mountain area, long power outages can occur. Road conditions may prevent support personnel from reaching the site to connect the generator before the UPS fails.

Risk (18) = Threat (5) + Likelihood (5) + Vulnerability (8)

This item will be rated as a **Medium**

Total Risk (**13**) = (26/2)

The **Physical Security Risk** rating will be assigned a **MEDIUM** rating for this evaluation.

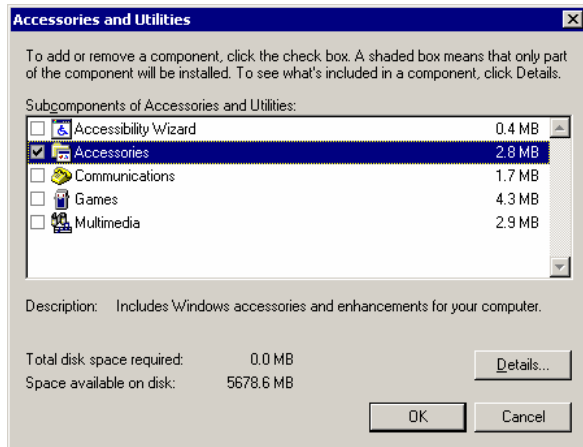
### 3.2. Server Hardening

#### 3.2.1. Item SH1: Results - Unneeded Windows Components Removed

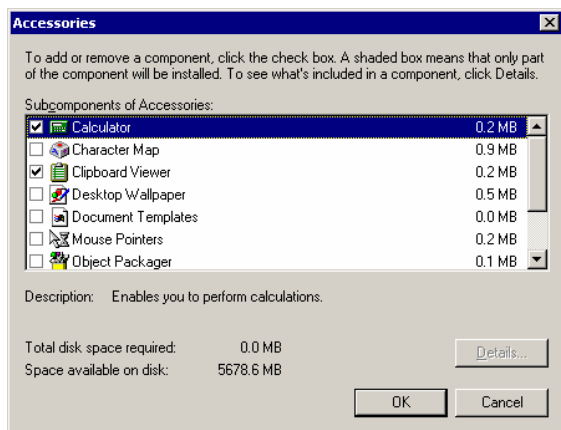
Findings	<p>Two services are installed that need to be considered for removal or moving to another server:</p> <ul style="list-style-type: none"><li>• DNS</li><li>• WINS</li></ul> <p>All original items to check are confirmed as <b><u>not installed</u></b>. Therefore the original check item would have <b>PASSED</b>. However, DNS and WINS may pose a potential risk when installed on an internet accessible Terminal Server. As a result, I will add this to the assessment and rate the RISK score as <b>MEDIUM</b>.</p>
----------	--

Accessories installed:

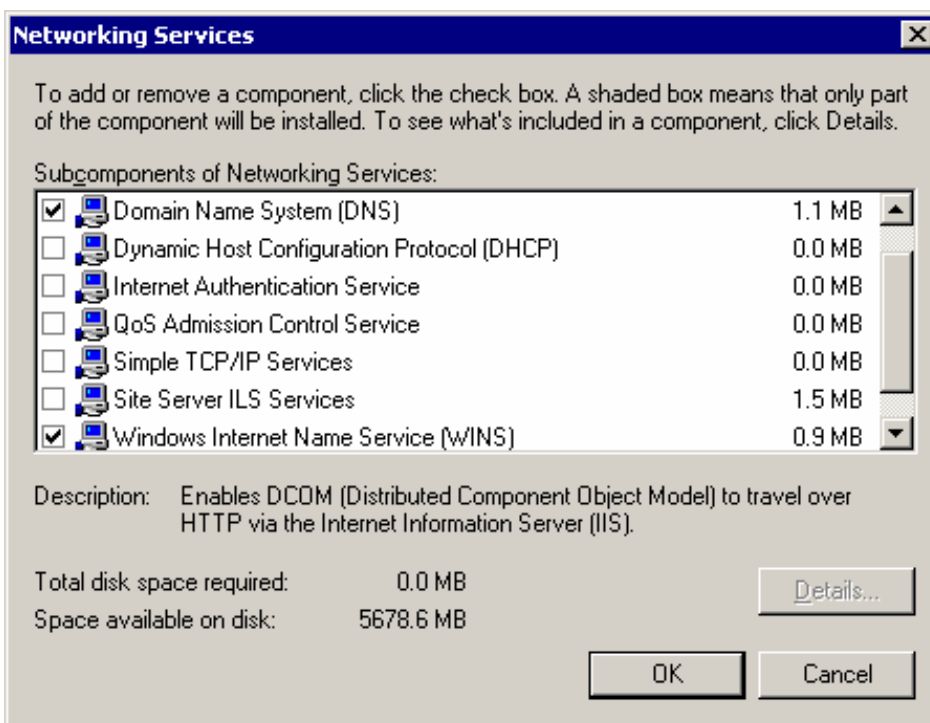
Games, Multimedia, communications, and Accessibility Wizard are **not installed**.



Document Templates and Desktop Wallpaper are not installed.



Unexpected items installed.



Varieties of risks are posed by WINS and DNS on a Terminal Server. Users can use the access to determine the internal network configuration, IP's, workstations, other servers, and services. The Firewall to the backend network should prevent most of this activity. However, the DMZ is shared with at least one other server used as a Web Server for the consultants company. An interview with the consultant indicates that other clients are hosted on this Webserver. I will recommend de-installing WINS and DNS and the Terminal Server be placed on an isolated DMZ. To gain access to the DNS and WINS information, an attacker would first need to obtain access to the Terminal Server itself through an RDP session. External scans did show that WINS and DNS services are not accessible directly from the Internet.

RISK (12) = Threat (5) + Vulnerability (5) = Likelihood (2)

The Risk of WINS/DNS installed on the Terminal server will be rated as a **MEDIUM**.

### 3.2.2. Item SH2: Results - File ACL

Findings	The most significant threat to the server and the data the server maintains is from the Users themselves.
----------	---

	<p>Therefore, we considered that even one item failing is considered a Failure of this check. Unauthorized access or changes to many of these file makes the system very vulnerable to users making changes to the server that can result in loss of data, unintended release of information or a total Denial of Service condition.</p> <p>The Risks to the system is that any user on the system may be able to change system files creating a system that will not boot, boot improperly, or change system boot parameters. MalWare installation to protected or sensitive directories can occur. Inadvertent changes can occur by a user exploring the directories out of simple curiosity (personal experience has proven this out).</p> <p>Total Risk (21) = Threat (7) + Vulnerability (10) = Likelihood (4)</p> <p>This Item will be rated as a <b>HIGH</b> risk.</p>
--	---

Red = Failed

Green = Passed or Exceeded

cacls c:\

c:\ Everyone:(OI)(CI)F

cacls c:\boot.ini

c:\boot.ini BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F

cacls c:\ntldr

c:\ntldr BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F

cacls c:\ntdetect.com

c:\NTDETECT.COM BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F

cacls c:\winnt\repair

c:\winnt\repair BUILTIN\Users:R  
BUILTIN\Users:(CI)(IO)(special access):

GENERIC\_READ

GENERIC\_EXECUTE

BUILTIN\Power Users:C

BUILTIN\Power Users:(OI)(CI)(IO)C

BUILTIN\Administrators:F

BUILTIN\Administrators:(OI)(CI)(IO)F

```
NT AUTHORITY\SYSTEM:F
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
BUILTIN\Administrators:F
CREATOR OWNER:(OI)(CI)(IO)F
```

```
cacls c:\winnt\security
```

```
c:\winnt\security BUILTIN\Users:R
BUILTIN\Users:(OI)(CI)(IO)(special access:)
```

```
GENERIC_READ
GENERIC_EXECUTE
```

```
BUILTIN\Power Users:R
BUILTIN\Power Users:(OI)(CI)(IO)(special access:)
```

```
GENERIC_READ
GENERIC_EXECUTE
```

```
BUILTIN\Administrators:F
BUILTIN\Administrators:(OI)(CI)(IO)F
NT AUTHORITY\SYSTEM:F
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
BUILTIN\Administrators:F
CREATOR OWNER:(OI)(CI)(IO)F
```

```
cacls c:\winnt\system32\config
```

```
c:\winnt\system32\config BUILTIN\Users:R
BUILTIN\Users:(CI)(IO)(special access:)
```

```
GENERIC_READ
GENERIC_EXECUTE
```

```
BUILTIN\Power Users:R
BUILTIN\Power Users:(CI)(IO)(special access:)
```

```
GENERIC_READ
GENERIC_EXECUTE
```

```
BUILTIN\Administrators:F
BUILTIN\Administrators:(OI)(CI)(IO)F
NT AUTHORITY\SYSTEM:F
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
BUILTIN\Administrators:F
CREATOR OWNER:(OI)(CI)(IO)F
```

```
cacls c:\winnt\system32\dlldata
```

```
c:\winnt\system32\dlldata BUILTIN\Administrators:F
BUILTIN\Administrators:(OI)(CI)(IO)F
NT AUTHORITY\SYSTEM:F
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
BUILTIN\Administrators:F
CREATOR OWNER:(OI)(CI)(IO)F
```

```
cacls c:\winnt\system32\logfiles
```

```
c:\winnt\system32\LogFiles BUILTIN\Users:R
BUILTIN\Users:(OI)(CI)(IO)(special access:)
```



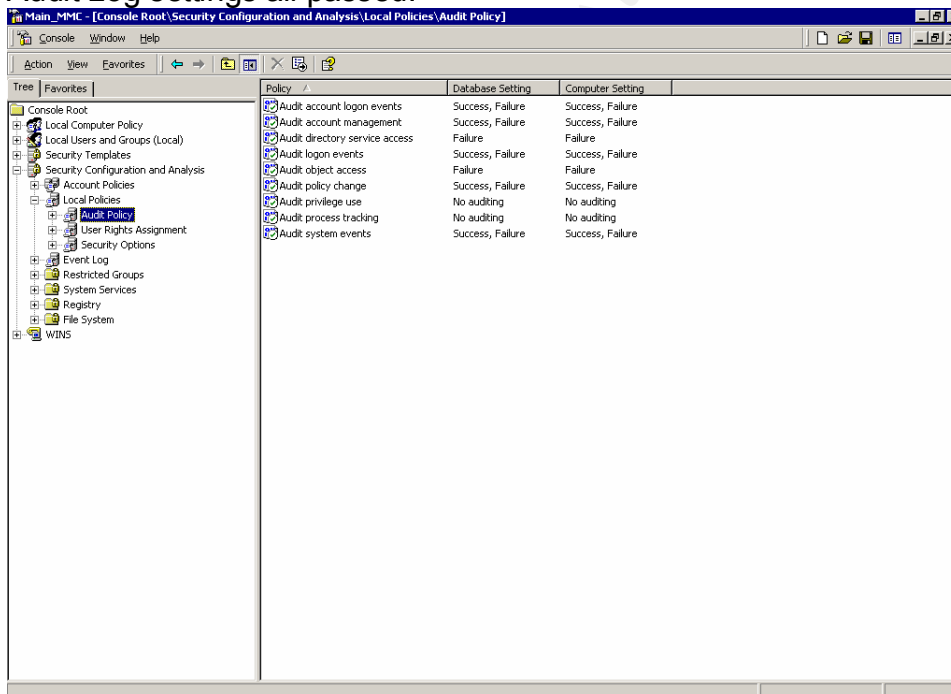
GENERIC\_READ  
GENERIC\_EXECUTE

BUILTINPower Users:C  
BUILTINPower Users:(OI)(CI)(IO)C  
BUILTINAdministrators:F  
BUILTINAdministrators:(OI)(CI)(IO)F  
NT AUTHORITY\SYSTEM:F  
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F  
CREATOR OWNER:(OI)(CI)(IO)F

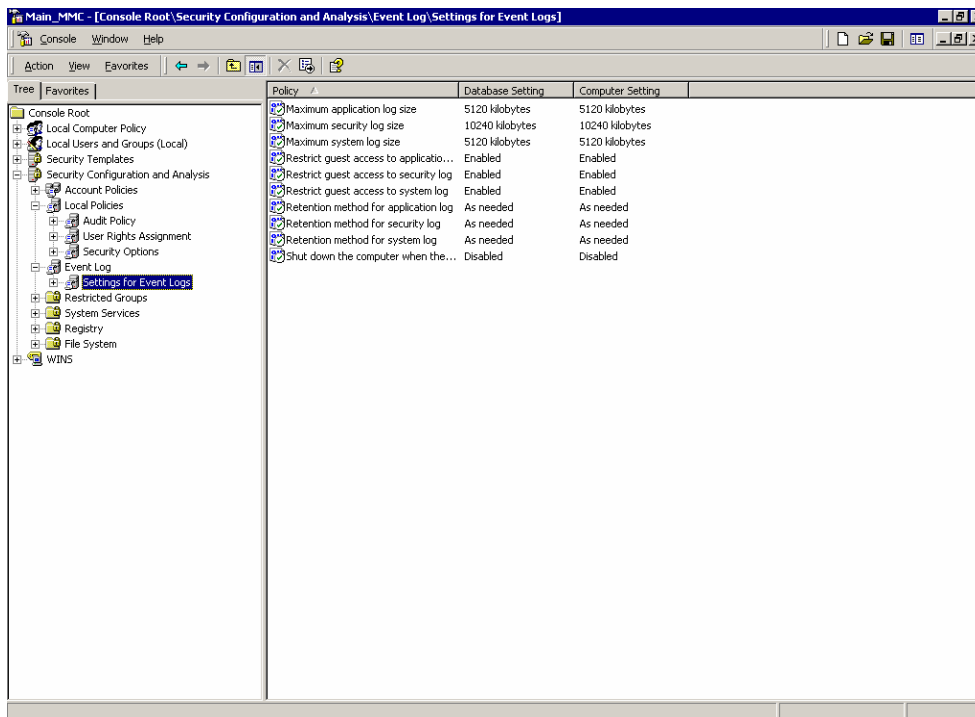
### 3.2.3. Item SH3: Results - Computer Configuration - Audit Policy and Event Log

Findings	All checks to this item passed or exceeded the desired settings.  Audit Policy settings – Passed  Event Log Settings - Passed
----------	---

Audit Log settings all passed:



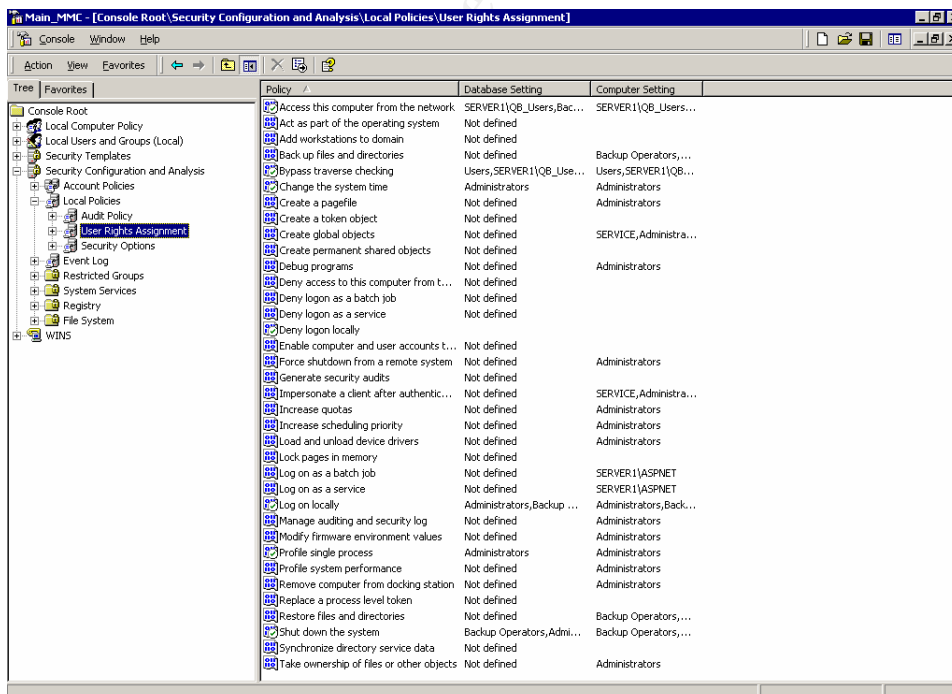
Event Log Settings all Passed



### 3.2.4. Item SH4: Results - Computer Configuration - User Rights

Findings	This Item - <b>Passed</b>
----------	---------------------------

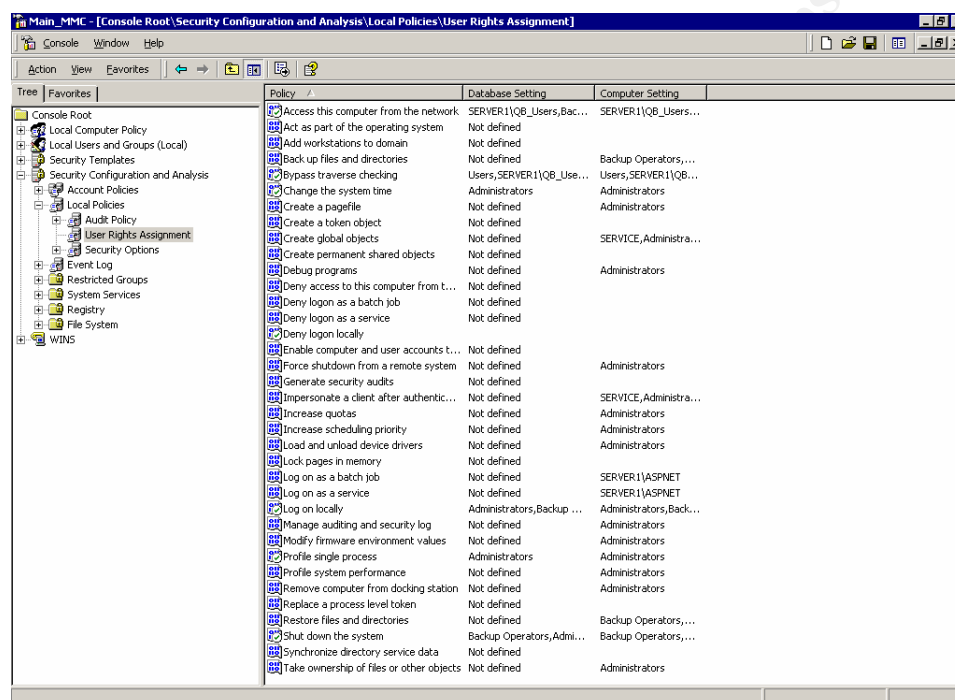
Users Rights – All checks are green!

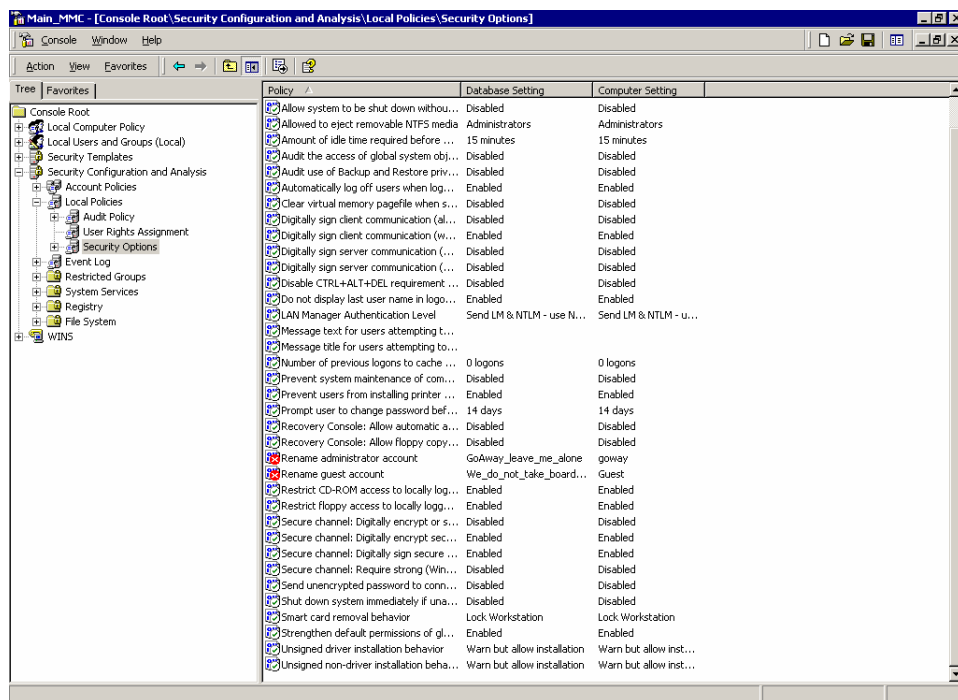


### 3.2.5. Item SH5: Results - Computer Configuration - Security Options

Findings	<p>The Administrator account *IS* changed to goaway – Passed</p> <p>The Guest Account is not changed, but is disabled – <b>Failed</b></p> <p>Risk (9) = Threat (1) + Vulnerability (1) + Likelihood (7)</p> <p>The risk will be rated as a <b>LOW</b></p> <p>All other checked passed.</p>
----------	--

The Guest account is not changed. Little Threat or Vulnerability due to other security settings and the account disabled status. Likelihood that an attacker will try to access the account is higher simple because it is a default account. Recommend changing the guest account name to a relatively obscure name.

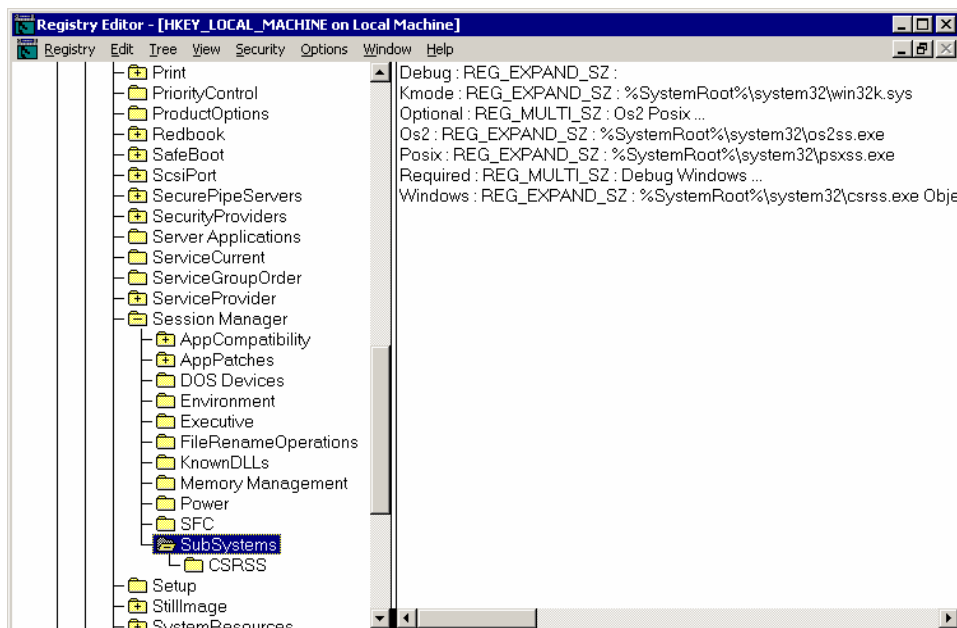




### 3.2.6. Item SH6: Results - Computer Configuration – Registry Settings

Findings	<p>Item Failed</p> <p>Users access to the various Registry Keys and/or Subsystems pose a threat to the server which can result in the installation of Viruses/Malware or other unauthorized programs and services.</p> <p>This can affect server operation, other users operability, corruption of data, loss of data, or theft of data.</p>
----------	--

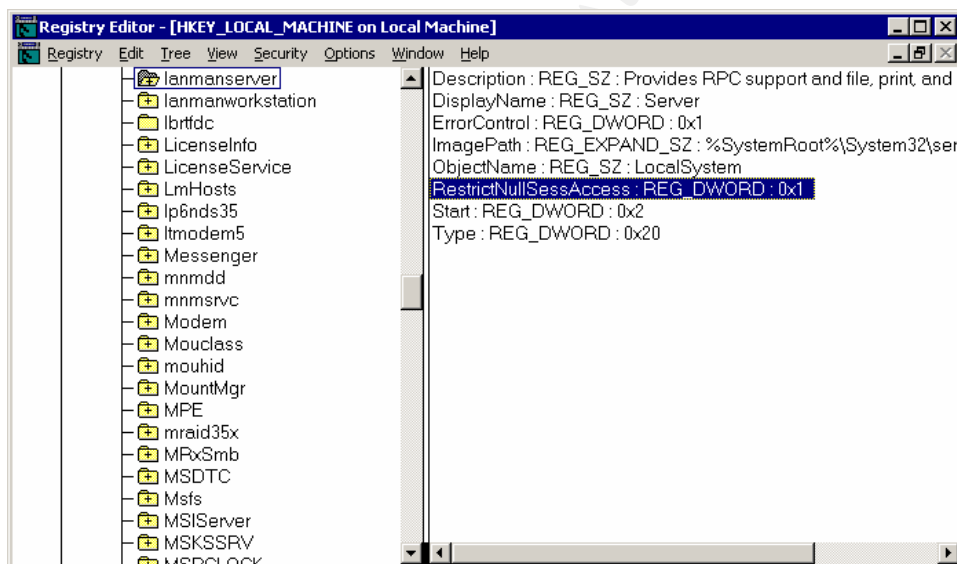
OS2 and POSIX Subsystems – FAILED



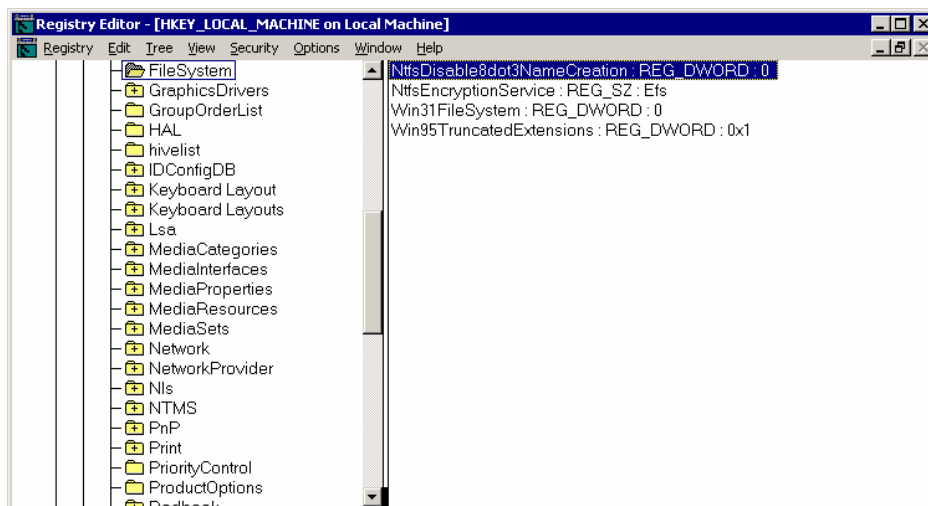
Restrict Null Session Access – PASSED

Restrict null session access over named pipes and shares - PASSED

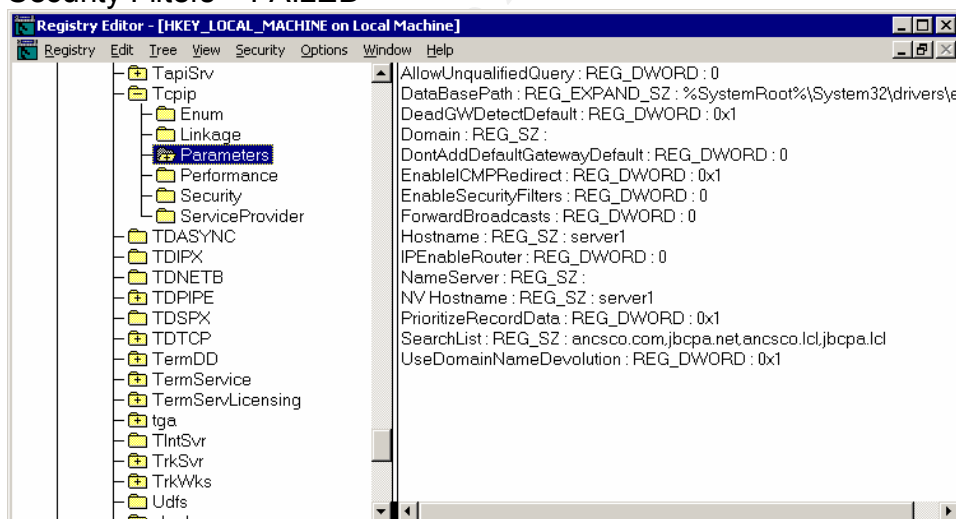
Hide computer from the network browse list - FAILED



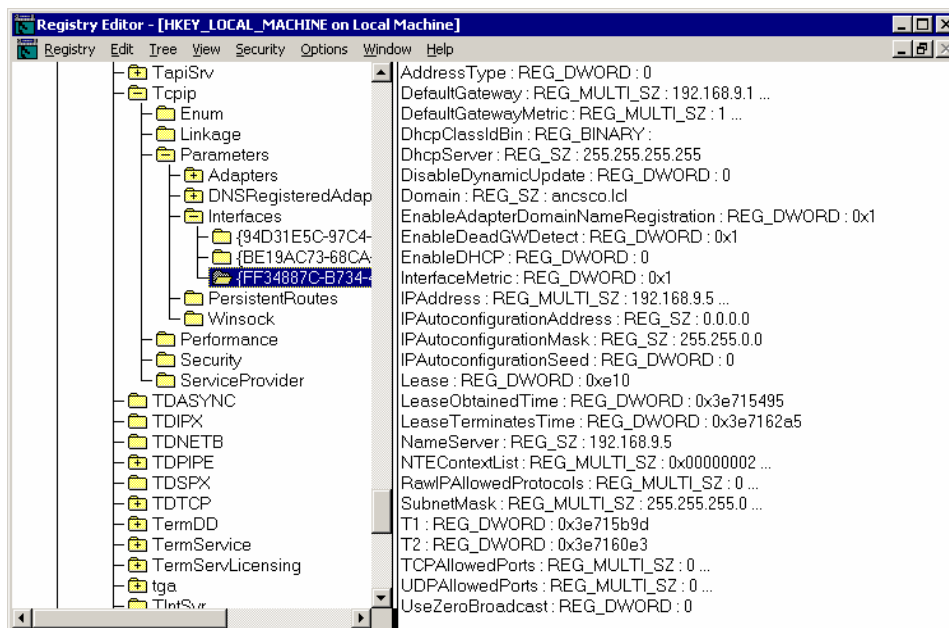
Disable 8.3 Filename Creation – FAILED



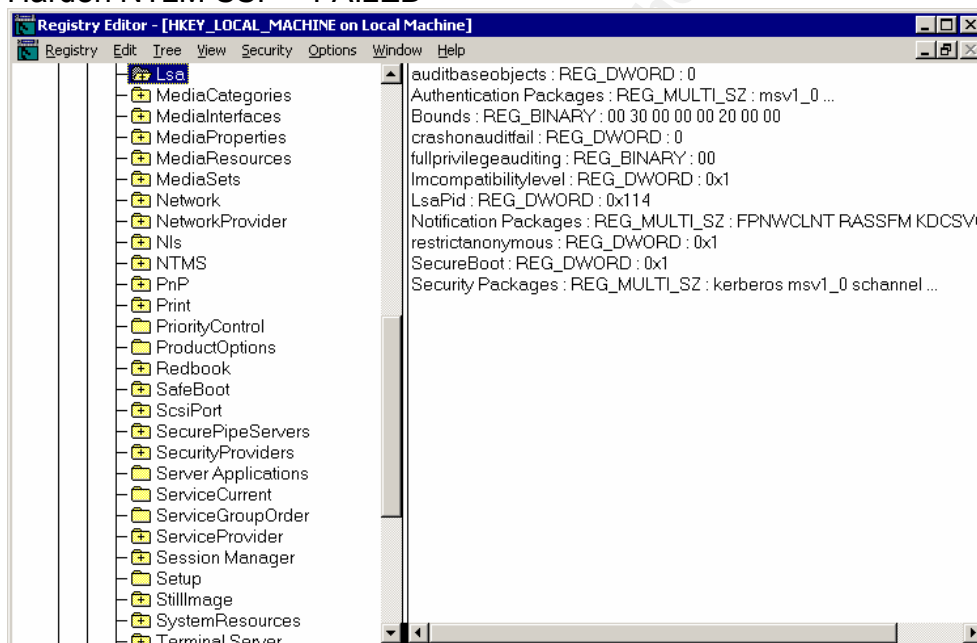
Syn Attack Protection – FAILED  
 TcpMaxPortsExhausted – FAILED  
 TcpMaxDataRetransmissions = FAILED  
 Dead Gateway Protection – FAILED  
 Disable ICMP Redirects – FAILED  
 Disable IP Source Routing – FAILED  
 TCP/IP KeepAlive Time – FAILED  
 Disable External Name Release – FAILED  
 Enable PTMU Discovery – FAILED  
 TcpMaxConnectResponseRetransmissions – FAILED  
 TcpMaxConnectRetransmissions – FAILED  
 Security Filters – FAILED



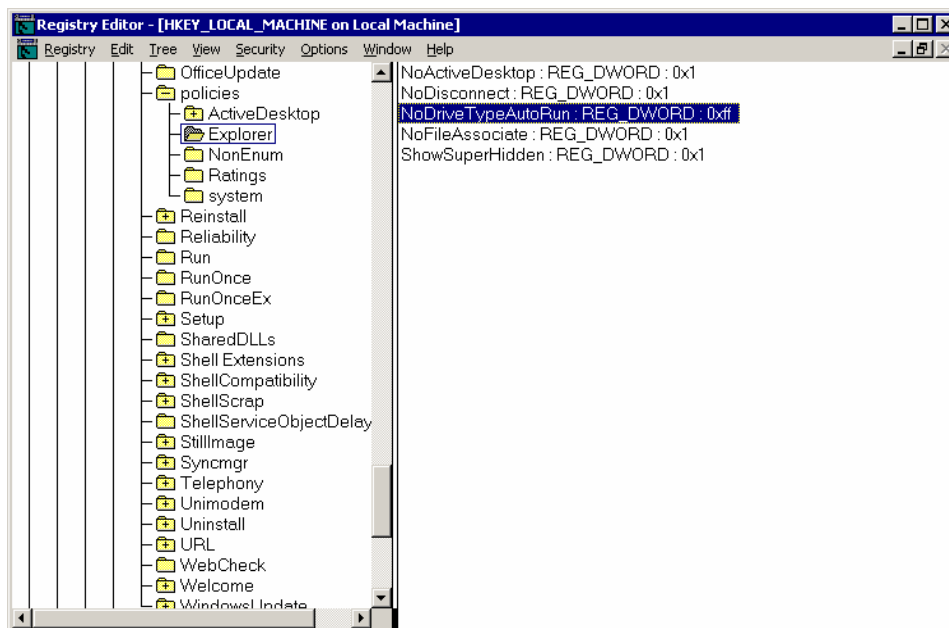
Router Discovery – FAILED



Disable LMHASH Creation – FAILED  
Harden NTLM SSP – FAILED

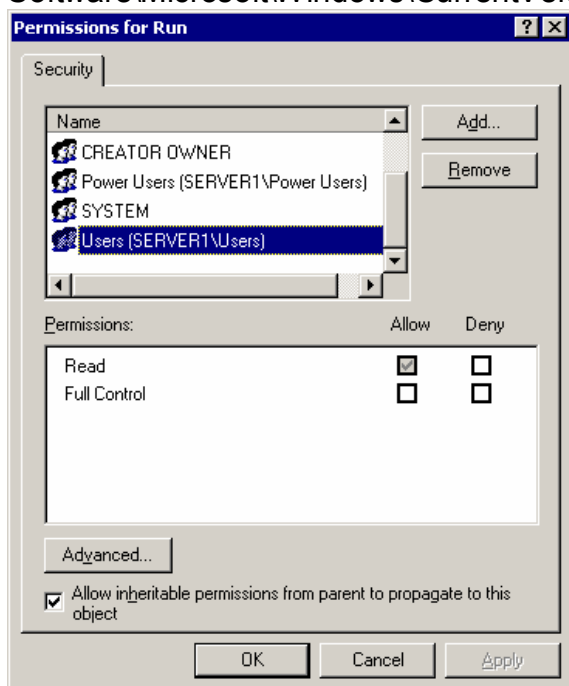


Disable all Autorun – PASSED



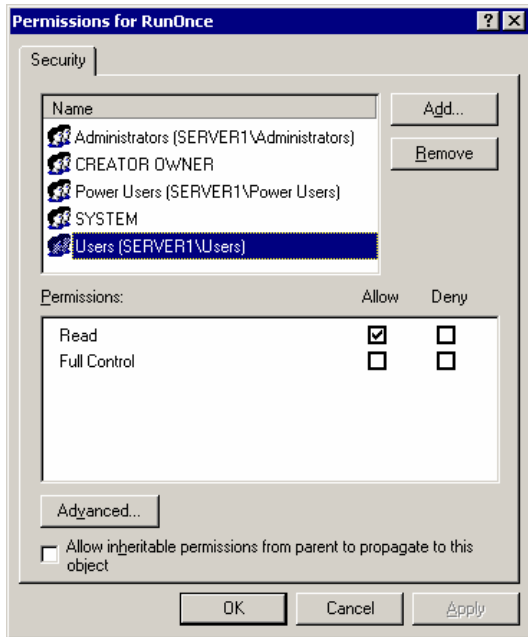
## Registry Permissions

Software\Microsoft\Windows\CurrentVersion\Run – FAILED

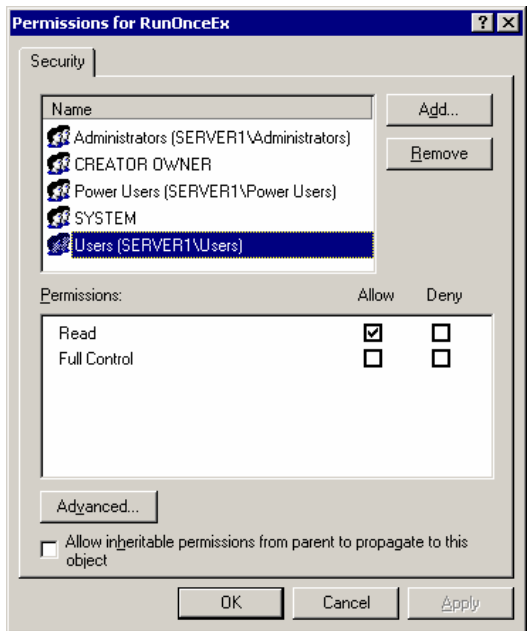




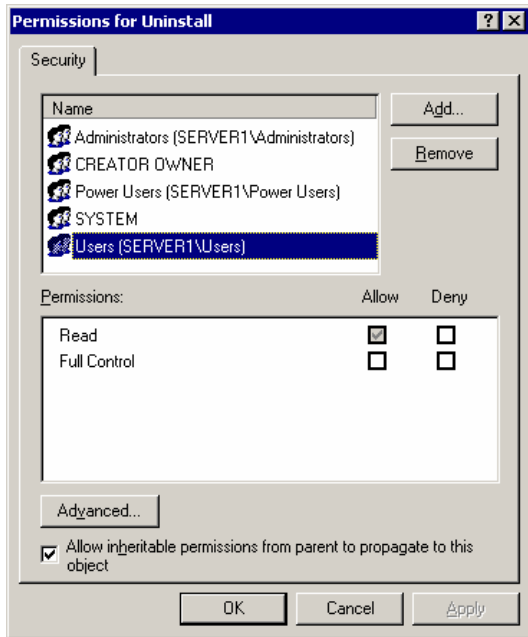
Software\Microsoft\Windows\CurrentVersion\RunOnce – FAILED



Software\Microsoft\Windows\CurrentVersion\RunOnceEx – FAILED



Software\Microsoft\Windows\CurrentVersion\Uninstall – FAILED



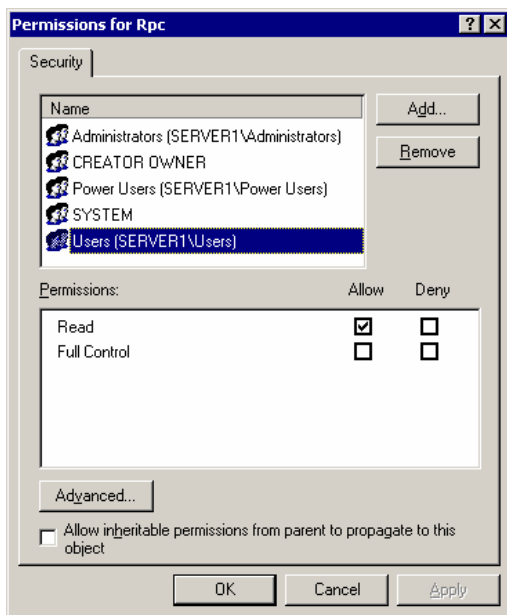
Software\Microsoft\Windows\CurrentVersion\AeDebug – PASSED

Key does not exist

Software\Microsoft\Windows\CurrentVersion\WinLogon – PASSED

Key does not exist

Software\Microsoft\Rpc – FAILED

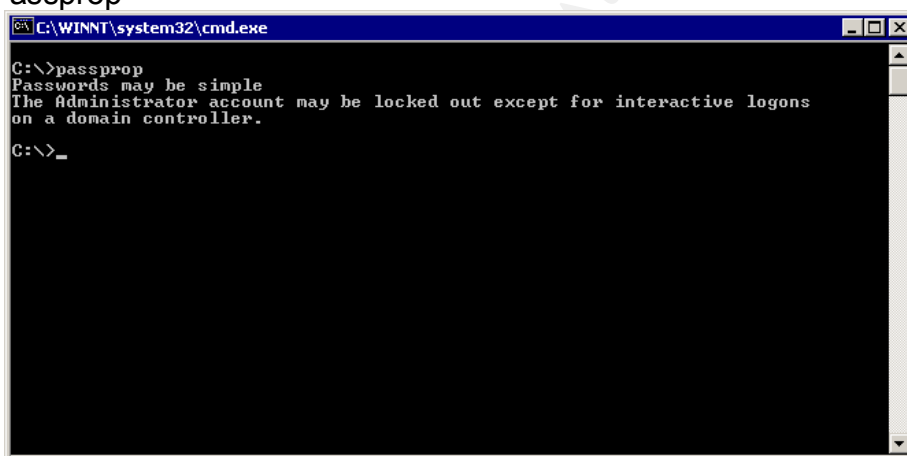


### 3.2.7. Item SH7: Results - Account Policies, PassProp and Protected Tools

Findings	<p>Passprop settings – <b>Passed</b></p> <p>Password Policies – <b>Failed</b></p> <p>Minimum Password Age 45 days is MORE stringent than recommendation – Passed</p> <p>Minimum Password Age 0 days – Would allow a user to change password immediately. This is commonly used to bypass the number of passwords remembered. (i.e. User changes password 5 times and the 6<sup>th</sup> time sets the password back to the original password)</p> <p>Recommend setting this to 5</p> <p>Risk (8) = Threat (2) + Vulnerability (4) + Likelihood (2)</p> <p>The risk for this finding is <b>LOW</b></p> <p>Recommended more stringent password policy for Minimum password length. Current setting allows NO PASSWORD. Many users would use NO PASSWORD out of convenience.</p> <p>This may not threaten system as much as user data, but system would be under threat from possible DOS if an attacker used the account to login and use all available TCP connections.</p> <p>Risk (26) = Threat (8) + Vulnerability (10) + Likelihood (8)</p> <p>The Risk for this finding is <b>HIGH</b></p> <p>Protected utilities – <b>Failed</b></p> <p>Many utilities listed can be used by a user to bypass many</p>
----------	---

	<p>protected executables. FTP, for instance, can be used to download a desired executable that bypasses the local system executable to attack the system or attack other systems. This does require more knowledge of the utilities and what they can do. Interviews with the computer consultant indicates that the proposed userbase for this server do have a more complete working knowledge of their computers than an everyday user.</p> <p>Therefore, protecting these utilities is more critical on a Terminal Server and especially one exposed to the Internet. Granting access to any of these utilities should be carefully reviewed on a case-by-case basis with a clear understanding of the purpose of the server.. In this case, a QuickBooks Bookkeeping system.</p> <p>Risk (27) = Threat (8) + Vulnerability (10) + Likelihood (9)</p> <p>The Risk for this finding is <b>HIGH</b></p> <p>The Windows 2000 Resource kit is NOT installed – <b>Passed</b></p> <p>Total Risk (20.6) = (62/3)</p> <p>The Total Risk for this Check Item is <b>HIGH</b></p>
--	--

## Passprop

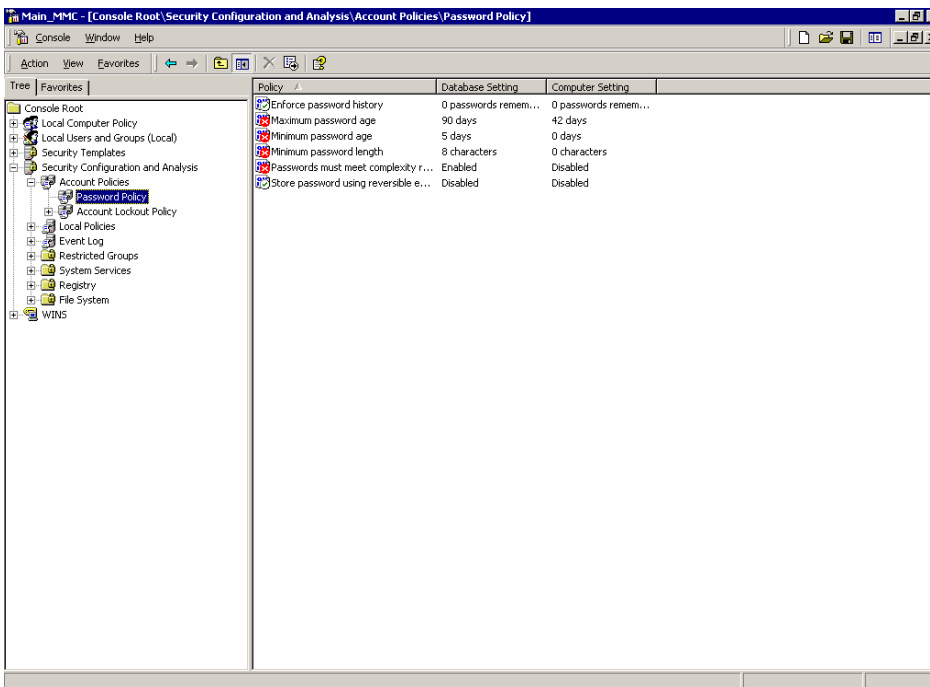


```

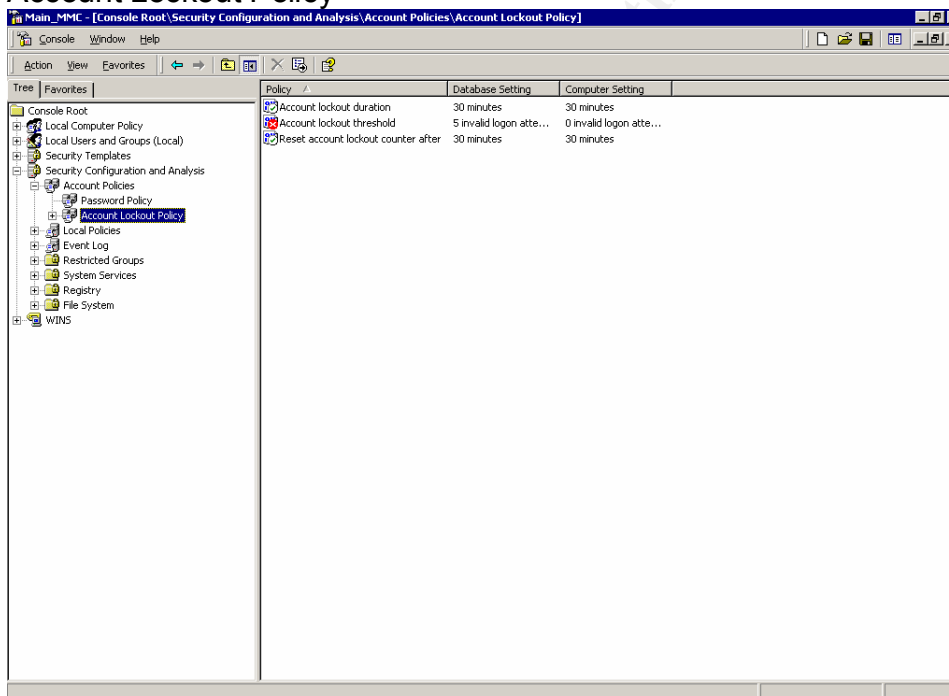
C:\WINNT\system32\cmd.exe
C:\>passprop
Passwords may be simple
The Administrator account may be locked out except for interactive logons
on a domain controller.
C:\>_

```

## Password Policies



## Account Lockout Policy



## Protected Utilities

Red = Failed

Note: Where there is nothing listed under the filename, which indicates that the respective file is not installed.

caccls c:\winnt\RegEdit.exe

c:\winnt\regedit.exe BUILTIN\Users:R

BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F

cacls c:\winnt\system32\append.exe  
c:\winnt\system32\append.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\attrib.exe  
c:\winnt\system32\attrib.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\cacls.exe  
c:\winnt\system32\CACLS.EXE BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\change.exe  
c:\winnt\system32\change.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\chcp.com  
c:\winnt\system32\chcp.com BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\chglogon.exe  
c:\winnt\system32\chglogon.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\chgport.exe  
c:\winnt\system32\chgport.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

```
cacls c:\winnt\system32\chgusr.exe
c:\winnt\system32\chgusr.exe BUILTIN\Users:R
                        BUILTIN\Power Users:R
                        BUILTIN\Administrators:F
                        NT AUTHORITY\SYSTEM:F
                        Everyone:R
```

```
cacls c:\winnt\system32\chkdsk.exe
c:\winnt\system32\CHKDSK.EXE BUILTIN\Users:R
                        BUILTIN\Power Users:R
                        BUILTIN\Administrators:F
                        NT AUTHORITY\SYSTEM:F
                        Everyone:R
```

```
cacls c:\winnt\system32\chkntfs.exe
c:\winnt\system32\CHKNTFS.EXE BUILTIN\Users:R
                        BUILTIN\Power Users:R
                        BUILTIN\Administrators:F
                        NT AUTHORITY\SYSTEM:F
                        Everyone:R
```

```
cacls c:\winnt\system32\cipher.exe
c:\winnt\system32\cipher.exe BUILTIN\Users:R
                        BUILTIN\Power Users:R
                        BUILTIN\Administrators:F
                        NT AUTHORITY\SYSTEM:F
                        Everyone:R
```

```
cacls c:\winnt\system32\cluster.exe
c:\winnt\system32\CLUSTER.EXE BUILTIN\Users:R
                        BUILTIN\Power Users:R
                        BUILTIN\Administrators:F
                        NT AUTHORITY\SYSTEM:F
                        Everyone:R
```

```
cacls c:\winnt\system32\cmd.exe
c:\winnt\system32\CMD.EXE BUILTIN\Users:R
                        BUILTIN\Power Users:R
                        BUILTIN\Administrators:F
                        NT AUTHORITY\SYSTEM:F
                        Everyone:R
```

```
cacls c:\winnt\system32\command.com
c:\winnt\system32\command.com BUILTIN\Users:R
                        BUILTIN\Power Users:R
                        BUILTIN\Administrators:F
                        NT AUTHORITY\SYSTEM:F
                        Everyone:R
```

```
cacls c:\winnt\system32\compact.exe
c:\winnt\system32\compact.exe BUILTIN\Users:R
                        BUILTIN\Power Users:R
                        BUILTIN\Administrators:F
                        NT AUTHORITY\SYSTEM:F
```

Everyone:R

```
cacls c:\winnt\system32\convert.exe
c:\winnt\system32\CONVERT.EXE BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\cscript.exe
c:\winnt\system32\cscript.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\dcpromo.exe
c:\winnt\system32\dcpromo.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\debug.exe
c:\winnt\system32\debug.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\dfscmd.exe
c:\winnt\system32\dfscmd.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\diskcomp.com
c:\winnt\system32\DISKCOMP.COM BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\diskcopy.com
c:\winnt\system32\DISKCOPY.COM BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\doskey.exe
c:\winnt\system32\doskey.exe BUILTIN\Users:R
```



```
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\edlin.exe
c:\winnt\system32\edlin.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\exe2bin.exe
c:\winnt\system32\exe2bin.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\expand.exe
c:\winnt\system32\expand.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\fc.exe
c:\winnt\system32\fc.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\find.exe
c:\winnt\system32\find.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\findstr.exe
c:\winnt\system32\findstr.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\finger.exe
c:\winnt\system32\finger.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\forcedos.exe
c:\winnt\system32\forcedos.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\format.com
c:\winnt\system32\FORMAT.COM BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\ftp.exe
c:\winnt\system32\FTP.EXE BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\hostname.exe
c:\winnt\system32\hostname.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\iisreset.exe
```

```
cacls c:\winnt\system32\ipconfig.exe
c:\winnt\system32\ipconfig.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\ipxroute.exe
c:\winnt\system32\ipxroute.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\label.exe
c:\winnt\system32\LABEL.EXE BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\logoff.exe
c:\winnt\system32\logoff.exe BUILTIN\Users:R
```

```
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\makecab.exe
c:\winnt\system32\makecab.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\mem.exe
c:\winnt\system32\mem.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\mmc.exe
c:\winnt\system32\mmc.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\mode.com
c:\winnt\system32\mode.com BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\more.com
c:\winnt\system32\more.com BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\mountvol.exe
c:\winnt\system32\mountvol.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\msg.exe
c:\winnt\system32\msg.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\nbtstat.exe
c:\winnt\system32\NBTSTAT.EXE BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\net.exe
c:\winnt\system32\net.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\net1.exe
c:\winnt\system32\net1.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\netsh.exe
c:\winnt\system32\netsh.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\netstat.exe
c:\winnt\system32\NETSTAT.EXE BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\nslookup.exe
c:\winnt\system32\NSLOOKUP.EXE BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\ntbackup.exe
c:\winnt\system32\NTBACKUP.EXE BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
caccls c:\winnt\system32\ntdsutil.exe
c:\winnt\system32\ntdsutil.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
```

NT AUTHORITY\SYSTEM:F  
Everyone:R

caccls c:\winnt\system32\ntsd.exe  
c:\winnt\system32\ntsd.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

caccls c:\winnt\system32\ls2.exe  
c:\winnt\system32\ls2.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

caccls c:\winnt\system32\passprop.exe  
c:\winnt\system32\Passprop.exe BUILTIN\Users:R  
BUILTIN\Power Users:C  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F

caccls c:\winnt\system32\pathping.exe  
c:\winnt\system32\pathping.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

caccls c:\winnt\system32\ping.exe  
c:\winnt\system32\ping.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

caccls c:\winnt\system32\posix.exe  
c:\winnt\system32\posix.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

caccls c:\winnt\system32\print.exe  
c:\winnt\system32\print.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

caccls c:\winnt\system32\query.exe  
c:\winnt\system32\query.exe BUILTIN\Users:R

BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\rasdiag.exe  
c:\winnt\system32\rasdiag.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\rpc.exe  
c:\winnt\system32\rpc.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\recover.exe  
c:\winnt\system32\RECOVER.EXE BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\regedt32.exe  
c:\winnt\system32\regedt32.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\regini.exe  
c:\winnt\system32\regini.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\register.exe  
c:\winnt\system32\register.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cacls c:\winnt\system32\regsvr32.exe  
c:\winnt\system32\REGSVR32.EXE BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

```
cacls c:\winnt\system32\replace.exe
c:\winnt\system32\replace.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\reset.exe
c:\winnt\system32\reset.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\rexec.exe
c:\winnt\system32\rexec.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\route.exe
c:\winnt\system32\route.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\routemon.exe
c:\winnt\system32\routemon.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\router.exe
c:\winnt\system32\router.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\rsh.exe
c:\winnt\system32\rsh.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\runas.exe
c:\winnt\system32\runas.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
```

NT AUTHORITY\SYSTEM:F  
Everyone:R

cac ls c:\winnt\system32\runonce.exe  
c:\winnt\system32\runonce.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cac ls c:\winnt\system32\secedit.exe  
c:\winnt\system32\secedit.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cac ls c:\winnt\system32\setpwd.exe  
c:\winnt\system32\setpwd.exe BUILTIN\Users:R  
BUILTIN\Power Users:C  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F

cac ls c:\winnt\system32\shadow.exe  
c:\winnt\system32\shadow.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cac ls c:\winnt\system32\share.exe  
c:\winnt\system32\share.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cac ls c:\winnt\system32\snmp.exe

cac ls c:\winnt\system32\snmptrap.exe

cac ls c:\winnt\system32\srvmgr.exe  
c:\winnt\system32\srvmgr.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R

cac ls c:\winnt\system32\subst.exe  
c:\winnt\system32\subst.exe BUILTIN\Users:R  
BUILTIN\Power Users:R  
BUILTIN\Administrators:F  
NT AUTHORITY\SYSTEM:F  
Everyone:R



```
cacls c:\winnt\system32\sysedit.exe
c:\winnt\system32\sysedit.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\syskey.exe
c:\winnt\system32\syskey.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\taskmgr.exe
c:\winnt\system32\TASKMGR.EXE BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\telnet.exe
c:\winnt\system32\telnet.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\termsrv.exe
c:\winnt\system32\termsrv.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\ftp.exe
c:\winnt\system32\ftp.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\tntadmn.exe
c:\winnt\system32\tntadmn.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\tntsess.exe
c:\winnt\system32\tntsess.exe BUILTIN\Users:R
BUILTIN\Power Users:R
```

BUILTINAdministrators:F  
NT AUTHORITYSYSTEM:F  
Everyone:R

cacls c:\winnt\system32\lntsrv.exe

cacls c:\winnt\system32\tracert.exe  
c:\winnt\system32\tracert.exe BUILTINUsers:R  
BUILTINPower Users:R  
BUILTINAdministrators:F  
NT AUTHORITYSYSTEM:F  
Everyone:R

cacls c:\winnt\system32\tree.com  
c:\winnt\system32\tree.com BUILTINUsers:R  
BUILTINPower Users:R  
BUILTINAdministrators:F  
NT AUTHORITYSYSTEM:F  
Everyone:R

cacls c:\winnt\system32\tsadmin.exe  
c:\winnt\system32\tsadmin.exe BUILTINUsers:R  
BUILTINPower Users:R  
BUILTINAdministrators:F  
NT AUTHORITYSYSTEM:F  
Everyone:R

cacls c:\winnt\system32\tscon.exe  
c:\winnt\system32\tscon.exe BUILTINUsers:R  
BUILTINPower Users:R  
BUILTINAdministrators:F  
NT AUTHORITYSYSTEM:F  
Everyone:R

cacls c:\winnt\system32\tsdiscon.exe  
c:\winnt\system32\tsdiscon.exe BUILTINUsers:R  
BUILTINPower Users:R  
BUILTINAdministrators:F  
NT AUTHORITYSYSTEM:F  
Everyone:R

cacls c:\winnt\system32\tskill.exe  
c:\winnt\system32\tskill.exe BUILTINUsers:R  
BUILTINPower Users:R  
BUILTINAdministrators:F  
NT AUTHORITYSYSTEM:F  
Everyone:R

cacls c:\winnt\system32\tsprof.exe  
c:\winnt\system32\tsprof.exe BUILTINUsers:R  
BUILTINPower Users:R  
BUILTINAdministrators:F  
NT AUTHORITYSYSTEM:F  
Everyone:R

```
cacls c:\winnt\system32\tssshutdn.exe
c:\winnt\system32\tssshutdn.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\usmgr.exe
c:\winnt\system32\usmgr.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\winmsd.exe
c:\winnt\system32\winmsd.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\winver.exe
c:\winnt\system32\winver.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\wmimgmt.msc
c:\winnt\system32\wmimgmt.msc BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

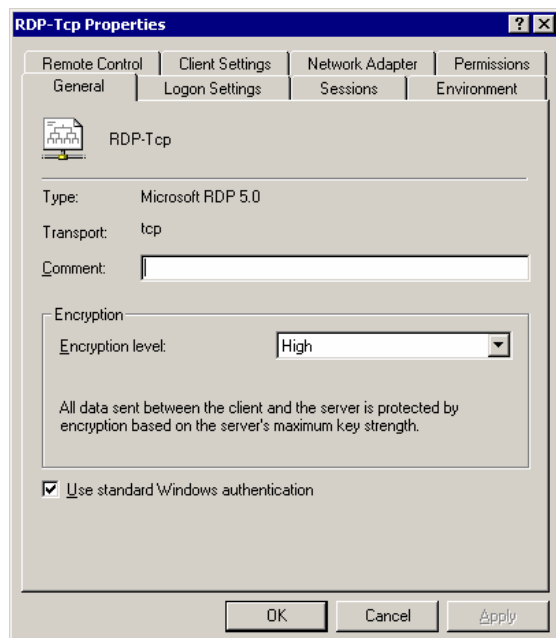
```
cacls c:\winnt\system32\wscript.exe
c:\winnt\system32\wscript.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

```
cacls c:\winnt\system32\xcopy.exe
c:\winnt\system32\xcopy.exe BUILTIN\Users:R
BUILTIN\Power Users:R
BUILTIN\Administrators:F
NT AUTHORITY\SYSTEM:F
Everyone:R
```

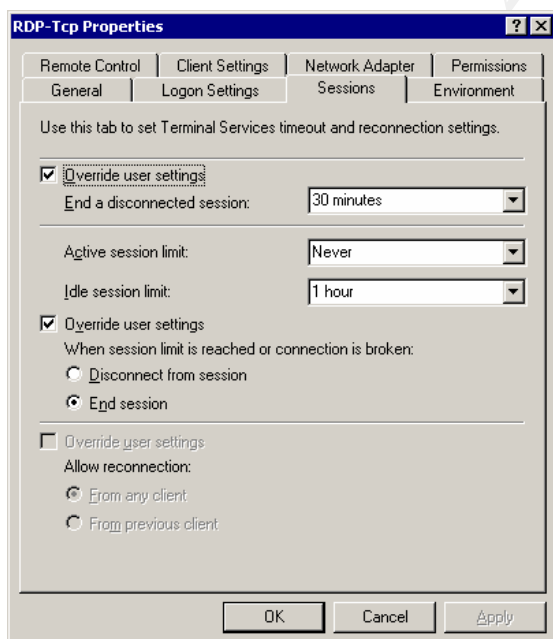
### 3.2.8. Item SH8: Results - Terminal Server Specific

Findings	All checks PASSED
----------	-------------------

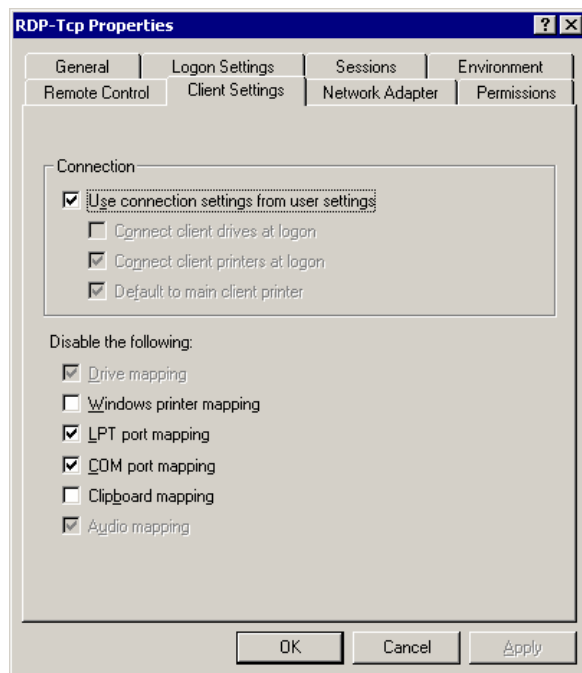
RDP set to High Encryption – PASSED



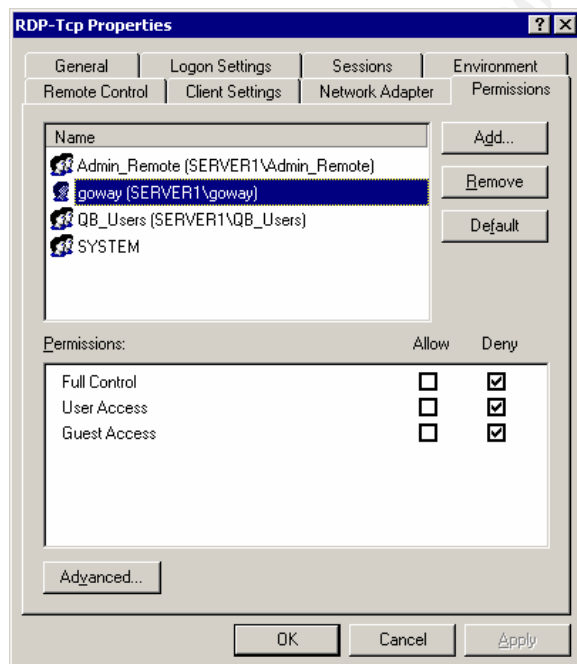
Sessions Tab – PASSED



## Client Settings Tab – PASSED



## Permissions – PASSED



### 3.3. Internal Scan for Open Ports and Services

#### 3.3.1. Item IPS1: Results - Internal Nessus Scan

Findings	Normal open ports for Microsoft where found. No unexpected services where identified with the port scan.
----------	---

Scan results showed normal internal Microsoft ports all with a LOW severity. External scan indicated that these ports **ARE being blocked** by the firewall from being reached externally. EGRESS scan could not be performed due to client request not to perform Egress scans.

A recommendation to place this server on an isolated DMZ will be made to address possible issues presented from the backend network and the hosting facilities Web Server. These devices/networks where not scanned under the restrictions of the scope of work.

The only port exposed to the Internet is Port 3389 for the RDP connection. This will be addressed in the external scan results.

#### NESSUS SECURITY SCAN REPORT

Session Name : XY Scan Internal

Open ports:

Service: domain (53/tcp)

Severity: Low

A DNS server is running on this port. If you do not use it, disable it.

Risk factor : Low

Service: domain (53/udp)

Severity: Low

A DNS server is running on this port. If you do not use it, disable it.

Risk factor : Low

Service: domain (53/udp)

Severity: Low

Risk factor : Low

Service: cap (1026/tcp)

Severity: Low

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Solution : filter incoming traffic to this port.

Risk factor : Low

Service: epmap (135/tcp)

Severity: Low

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Solution : filter incoming traffic to this port.

Risk factor : Low

Service: general/icmp

Severity: Low

Service: ms-wbt-server (3389/tcp)

Severity: Low

The Terminal Services are enabled on the remote host.

Terminal Services allow a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, he may be able to use this service to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution : Disable the Terminal Services if you do not use them, and do not allow this service to run across the internet

Risk factor : Medium

CVE : CVE-2001-0540

BID : 3099, 7258

Service: netbios-ns (137/udp)

Severity: Low

Severity: Low

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host.

Solution : filter incoming traffic to this port.



Risk factor : Low

Service: tip2 (3372/tcp)

Severity: Low

A MSDTC server is running on this port

Service: unknown (1034/tcp)

Severity: Low

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host.

Solution : filter incoming traffic to this port.

Risk factor : Low

### **3.4. External (Internet based) Scan for Open Ports and Services**

#### ***3.4.1. Item EPS1: Results - External Nessus Scan***

External scan identified the services running on the FTP server and also appears to have fingered the Web Server Operating system. This server was outside of the scope of this audit and is not owned/operated by XY CPA.

I noticed that the NetGear FVS-318 did respond to a number of the scan tests. Auditing the FVS-318 was not part of the Audit, but this may indicate that the Firewall needs to receive an updated firmware version and tighten down some of its configuration. I removed the results detailing “holes” attributable to the non-audited devices

The one Item for Port 3389 for the RDP (Terminal Services) connection. I will recommend that the VPN capabilities of the FVS-318 be used to mitigate the “Man-in-the-Middle” vulnerability.

Session Name : XY External Scan

Service: ms-wbt-server (3389/tcp)

Severity: Low

The Terminal Services are enabled on the remote host.

Terminal Services allow a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, he may be able to use this service to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimates users by impersonating the

Windows server.

Solution : Disable the Terminal Services if you do not use them, and do not allow this service to run across the internet

Risk factor : Medium

CVE : CVE-2001-0540

BID : 3099, 7258

## Section 4: Risk Assessment

### *Executive Summary*

XY CPA requested a baseline security assessment of the XY CPA Terminal Server. The purpose of the assessment was to determine the current level of security of the server. The assessment results include both the areas that met the best practices recommendations and areas that can be modified to improve the security level of the server. The assessment has taken into account the level of risk that any deficiency presents to the server. This report will allow XY CPA to determine what modifications are deemed of highest priority in order to meet its customer's security concerns.

The assessment found that the XY CPA contracted computer consultant had taken reasonable steps to secure the server from Internet based attacks. However, there are many areas where improvements can be made. Most of the recommended modifications are designed to protect the server from the least considered threat, the end users themselves.

We will detail the findings in the following sections as well as recommended modifications.

### *Assessment Findings*

We will begin by reviewing the items rated as high risk as these items should be at the top of the list to correct. High-risk items should be addressed first and as funding allows items of lesser risk should be addressed in order.

#### HIGH RISK ITEMS

##### **COMPUTER CONFIGURATION – REGISTRY SETTINGS**

Microsoft (Microsoft, 2003) has made recommendations to change many registry settings and access permissions in order to protect the server from the users themselves. During the assessment, these registry items were assessed in comparison to the Microsoft recommendations, as detailed in the Microsoft Windows 2000 Server Hardening Guide. Many of the registry changes are designed to protect the server for inadvertent user actions that can cause damage to the servers' operating system and potentially threaten other users' ability to use the system.

##### **PASSWORD POLICIES**

The assessment discovered that the servers' security policies allow the users to have a zero length password. In other words, this policy allows a user to have no password whatsoever. An attacker that obtained the users account name could login and change the users' files and accounting information. This risk is quite serious to the XY CPA firm in the event a client using the terminal server has their accounting data changed, deleted or stolen.

## **PROTECTED UTILITIES**

The Microsoft Windows 2000 operating system, by default, allows users to access many programs and utilities that can pose a serious threat to the server. Users can access programs that allow them to transfer files to the server, replace permissions on files, or run applications that could be used to gather information about the network and other users. Corp-Sec (Corp-Sec, 2004), an independent organization of systems administrators focused on security, has compiled a list of utilities that should be secured to prevent undesired activities by the users of your system. Each of these utilities was checked to determine if a user could execute them. The default permissions were still in effect on these files thus still allowing users to execute nearly every utility checked.

## **FILE ACCESS CONTROL LIST**

Corp-Sec has identified various files and directories that are not utilities, but are critical to the core operation of the server. Many of these control how the server boots, saves restore information, and security databases. The assessment checked these files to determine if the permissions on these files met the recommended settings. Many of the files checked allowed regular users to access these files or directories. Access to these items could allow a user to obtain sensitive information about the server. In the event the permissions allow the user to modify the files, server failure could result if the user changes or deletes these files.

## **MEDIUM RISK ITEMS**

### **UNNEEDED WINDOWS COMPONENTS**

In keeping with the recommendations of Microsoft (Microsoft, 2003) and Corp-Sec (Corp-Sec, 2004), the assessment reviewed what additional accessories and utilities were installed on the server. None of the commonly installed applications that normally pose a risk to the server were installed. The assessment did identify that two services were installed that did not appear to be necessary for supporting the XY CPA clients. Domain Name Services (DNS) and Windows Internet Naming Service (WINS) have been installed. It was confirmed during the external security scan that neither of these services can be reached from the Internet. A user on the server could use these services to gain knowledge of and access to other servers, workstations, and services on the internal DMZ network.

### **EXTERNAL SECURITY SCAN**

TCP ports 21, 80, and 3389 were identified during the external Nessus scan. The Web Server located on the same DMZ as the terminal server services ports 21 and 80. That server is out of the scope of this assessment. Port 3389 is the common TCP Microsoft Terminal Server RDP port. Earlier verification of the RDP configuration showed that this service is properly setup for normal user access. The Terminal Services RDP protocol is that it is vulnerable to the "Man-in-the-Middle" attack.

To summarize, this attack requires an attacker to hijack the DNS address of the server and redirect normal users to a system that masquerades as the real server. A user will logon to the masquerading server and then the masquerading server will use those users'

credentials to access the real server, thus acting as a Middle-Man in the user's sessions. An attacker can capture all information being passed between the user and the server.

In order to address client concerns of security from the internet, XY CPA should strongly consider implementing a VPN and eliminate direct access to the Terminal Server from the internet.

## **PHYSICAL**

We arranged to visit the computer facilities housing the server. Overall security of the facility was good. Backup electrical power is currently provided by a dedicated 1500 Watt UPS and a manually connected electrical generator for facility wide emergency power. The computer consultant must manually connect and start the generator if power is lost to the facility for more than 1 hr. This will not pose much of a problem during the summer months, but severe winter storms could prevent the consultant from reaching the facility before the UPS system fails. Total loss of access to the server would result for however long the facility is without power.

### **LOW RISK ITEMS**

## **PHYSICAL – ACCESS CONTROLS**

The computer facility has relatively good access controls. Items that were noted to be missing were no guards for controlling access to the building, no visitors log documenting who visited the facility and when, and lack of a video surveillance system.

With no active response security, such as a guard, an intruder could obtain access to the computer room and steal the hardware before local law enforcement could arrive.

Access logs are necessary for auditing and security review. This also forces additional verification of a visitor's purpose for accessing the facility.

## **INTERNAL SECURITY SCAN**

The internal Nessus scans did not reveal any unexpected services running on the server. The firewall appears to be properly blocking access to the more sensitive Microsoft services from the Internet. However, many of these services are not necessarily needed for the proper operation of the server and do pose a slight threat to the internal DMZ if a user of the terminal server has the knowledge to access the service to obtain information about the internal network.

### *Assessment Recommendations*

The greatest threat to the XY CPA Terminal Server is from the end users or clients. The majority of these threats are easily mitigated through various file and registry changes to the server in order to reduce the vulnerabilities.

We have already provided the required script files and Regedit files to implement all the registry values and file changes recommended to the XY CPA Computer consultant. This was done to reduce time to implement and to provide the XY CPA computer consultant a

means to re-verify the settings against the recommended settings. Additional changes to the registry permissions have also been detailed for the computer consultant to implement once XY CPA management gives authorization to do so.

## HIGH RISK ITEMS

### **COMPUTER CONFIGURATION – REGISTRY SETTINGS**

Changing the registry setting to the recommended values requires no funding other than labor. The majority of these changes can be automated and be applied in relatively short order. The only risk to applying these changes is possible conflicts with the QuickBooks application. Some testing must be performed to insure no adverse effects to the applications operations results.

### **PASSWORD POLICIES**

Changing the password policy to require at least an 8-character length password is a simple administrative task that task only a few seconds of time. Customer support to existing clients currently using passwords of less than eight characters may be needed. For those clients using no password XY CPA will need to conduct training to instruct those users of the dangers posed by having no password. Funding for this item will be labor only.

### **PROTECTED UTILITIES**

Locking down access to sensitive utilities is mandatory to prevent the clients from threatening the operating system. Inadvertent modifications to the server's configuration can result in loss of service. These utilities can be locked down via the means of a simple script that the computer consultant can run.

### **FILE ACCESS CONTROL LIST**

Again, this is a simple and relatively low risk item to mitigate. Setting the access permissions to allow only administrators of the server to make changes will reduce the server's vulnerability to an end user from making changes to sensitive system level files. A script can be run to set the correct Access Control List properties of the files.

## MEDIUM RISK ITEMS

### **UNNEEDED WINDOWS COMPONENTS**

Removal of the Windows Internet Name service and Domain Name Service is highly recommended. The presence of these services does not necessarily pose a threat to the server as much as it poses a threat to the remaining systems on the DMZ. There is requirement for these services to be running for proper operation of the QuickBooks application and therefore should be removed at the earliest opportunity.

If there is business need for these services within the DMZ or internal backend network, a separate server running these services needs to be deployed.

### **EXTERNAL ACCESS**

We recommend moving all XY CPA clients to use the VPN to connect to the terminal server and removing access to the Terminal server directly from the internet. This

solution eliminates the vulnerability of a “Man-in-the-Middle” attack and further secures the clients data. This may require XY CPA to absorb the cost of deploying the NetGear VPN software to the client.

## **PHYSICAL**

XY CPA needs to work with the hosting facility to provide a more reliable means of emergency power. Local building regulations may restrict deployment of an emergency electrical generator to provide power in the event of an extended outage. XY CPA and the hosting facility should research options for providing extended emergency power to the facility and/or obtain insurance to mitigate the costs of an extended electrical power outage. This item will pose the most significant cost if implemented.

## **LOW RISK ITEMS**

### **PHYSICAL – ACCESS CONTROLS**

XY CPA and the host facility will need to agree on the need to provide an access log to document visitors to the computer floor.

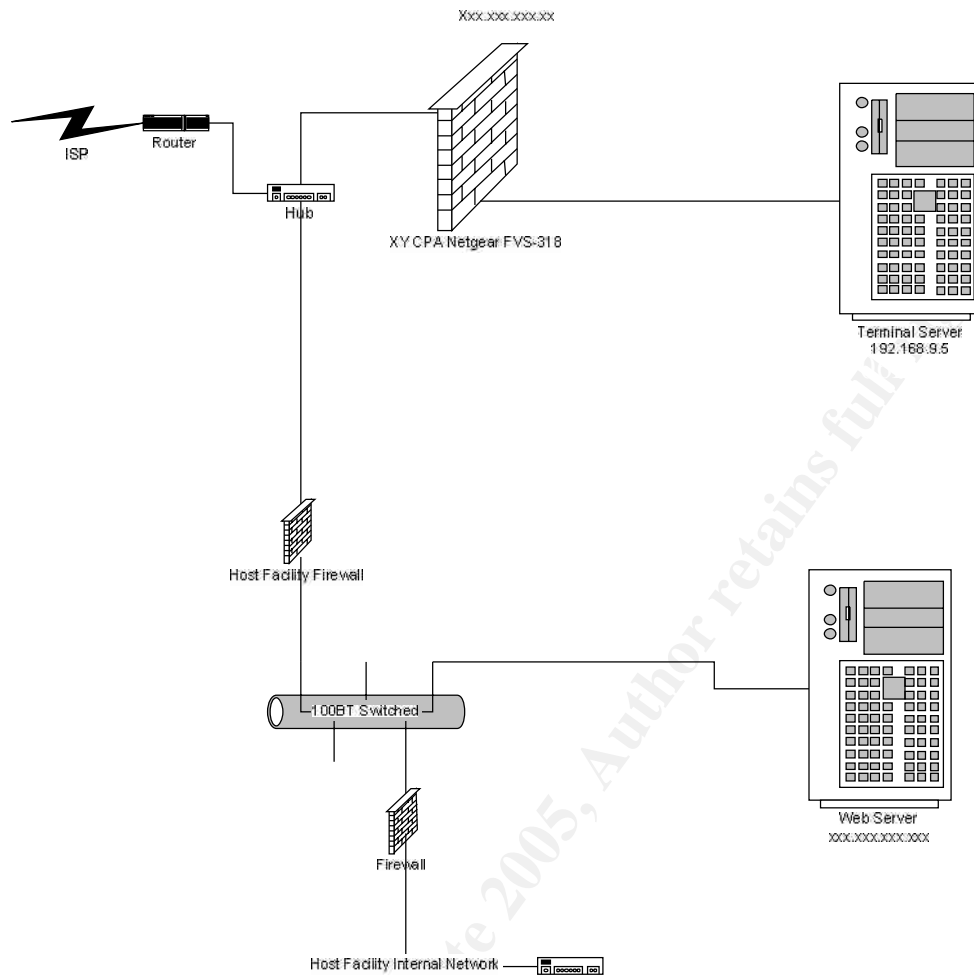
### **INTERNAL DMZ**

We recommend that XY CPA take advantage of the VPN capabilities of the existing NetGear FVS-318 Firewall. However, due to the way the NetGear OEM implements its VPN, additional network changes will need to be implemented. This firewall is designed for Small Office/Home Office (SOHO) use. Interviews (XY CPA Interviews, 2004) with XY CPA and the computer consultant indicated that this was not an issue for them and they were satisfied with staying with the NetGear product.

We are recommending that the Terminal Server be placed on a separate DMZ from the rest of the server farm located in the hosting facility. This is to reduce the threat from other systems on the DMZ that may be compromised and used to attack the XY CPA Server, reduce the threat to VPN clients connected to the Terminal Servers DMZ, and to reduce the possible threat and liability of XY CPA in the event that the Terminal Server is ever compromised and is used as an internal attack point against other systems residing on a shared DMZ.

Isolating the Terminal Server will also mitigate threats to/from the internal network and other devices on the shared DMZ.

**Figure 2. Recommended Network Configuration**



#### ADDITIONAL RECOMMENDATIONS

While the following items were not in the original scope of work, we feel the following points need to be addressed.

Documentation of the Terminal Servers configuration is not maintained in hard copy. The computer consultant has notes, system information printouts, and remembered steps to rely on to rebuild the server in the event of a failure. Full system configuration documentation must be created and maintained in the event the server fails and especially if the computer consultant is no longer available to rebuild the server.

Egress filter testing needs to be performed to determine if any outbound filtering is needed. Egress filtering was requested not to be performed during this audit.



Security audit of the NetGear FVS-318 should be conducted to determine the current security posture of the device and possible changes to improve any deficiencies.

Backups need to be tested to insure that the end users data can be reliably restored in a reasonable period of time.

A disaster recovery plan needs to be created and tested. The hosting facility had no disaster recovery plan for the XY CPA Terminal Server when asked. Current support is limited to hosting the server on the DMZ.

The NetGear FVS-318 Firewall is owned by XY CPA. However, the hosting facility appears to be using the firewall to provide services to other customers. XY CPA will need to revisit the terms of its hosting agreement to allow the firewall to provide a dedicated DMZ to the Terminal Server. It should be noted that the computer consultant has raised this issue with the hosting facility before with no resolution. As we detailed earlier, the shared DMZ poses a threat to the XY CPA terminal server from other systems residing on the DMZ and from the back-end internal network.

### *Summary*

XY CPA can significantly improve the security posture of the terminal server by implementing the above recommendations. The majority of our recommendations can be rapidly implemented at little to no cost.

By doing so, XY CPA can address their clients security concerns and provide a secure environment to the client no matter where they require access from.

Review of the current hosting configuration will also improve the security of the Terminal server if a separate DMZ can be created that isolates the XY CPA Terminal Server from the rest of the hosting facilities networks.

XY CPA should conduct regular security audits of the systems to evaluate and respond to new threats to the systems. Security is a continuing issue that XY CPA needs to balance against its normal operations in order to provide its customers with the most secure environment possible.

## References

Microsoft Corp. "Windows 2000 Security Hardening Guide." Version 1.3. May 15, 2003  
URL:

<http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&displaylang=en>

Corp-Net. "Practical Security for the Corporate World" URL:

[http://www.corp-sec.net/Hardening/win2k\\_h.html](http://www.corp-sec.net/Hardening/win2k_h.html)

Robert J. Shimonski. "Windows 2000 and 2003 Server Physical/Logical Security Primer" July 20, 2004 URL:

<http://www.windowsecurity.com/articles/Windows-2000-2003-Server-Physical-Security-Part1.html>

US Department of Justice. "Security Disciplines for Objective 1: Support" Version 2.0 March 2004 URL: <http://it.ojp.gov/documents/asp/ApplyingSecurityPractices.pdf>

The SANS Institute. "The SANS Security Policy Project" URL:

<http://www.sans.org/resources/policies/>

Nessus Security Scanner URL: <http://www.nessus.org>

Vakharia, Sunil. "Nessus scanning on Windows Domain" November 4, 2003 URL:

[http://www.nessus.org/doc/nessus\\_windows\\_scanning.pdf](http://www.nessus.org/doc/nessus_windows_scanning.pdf)

The Sans Institute. "SANS Glossary of Terms Used in Security and Intrusion Detection"

May 2003 URL: <http://www.sans.org/resources/glossary.php>

Mclure, Scambray, Kurtz. "Hacking Exposed: Fourth Edition" 2003 ISBN: 0-07-222742-7

Owner, XY CPA, LLC. Interview. August 14, 2004

Owner and IT Team, XY CPA, LLC. Interview. August 28, 2004

IT Consultant, XY CPA, LLC. Interview. September 4, 2004

## Appendixes

### Appendix A – Checking File Permissions for SH2 and SH7

Batch file used to check permissions for certain sensitive files

Save these entries to a file (ex: check\_files.cmd) and run the script

Redirect the output to a file for document the results. (i.e.: check\_files.cmd > file\_check.txt)

Cacls is part of the default Windows Operating system.

---

```
cacls c:\
cacls c:\boot.ini
cacls c:\ntldr
cacls c:\ntdetect.com
cacls c:\winnt\repair
cacls c:\winnt\security
cacls c:\winnt\system32\config
cacls c:\winnt\system32\dlldata
cacls c:\winnt\system32\logfiles
cacls c:\winnt\RegEdit.exe
cacls c:\winnt\system32\append.exe
cacls c:\winnt\system32\attrib.exe
cacls c:\winnt\system32\cacls.exe
cacls c:\winnt\system32\change.exe
cacls c:\winnt\system32\chcp.com
cacls c:\winnt\system32\chglogon.exe
cacls c:\winnt\system32\chgport.exe
cacls c:\winnt\system32\chgusr.exe
cacls c:\winnt\system32\chkdsk.exe
cacls c:\winnt\system32\chkntfs.exe
cacls c:\winnt\system32\cipher.exe
cacls c:\winnt\system32\cluster.exe
cacls c:\winnt\system32\cmd.exe
cacls c:\winnt\system32\command.com
cacls c:\winnt\system32\compact.exe
cacls c:\winnt\system32\convert.exe
cacls c:\winnt\system32\cscript.exe
cacls c:\winnt\system32\dcpromo.exe
cacls c:\winnt\system32\debug.exe
cacls c:\winnt\system32\dfscmd.exe
cacls c:\winnt\system32\diskcomp.com
cacls c:\winnt\system32\diskcopy.com
cacls c:\winnt\system32\doskey.exe
cacls c:\winnt\system32\edlin.exe
cacls c:\winnt\system32\exe2bin.exe
cacls c:\winnt\system32\expand.exe
cacls c:\winnt\system32\fc.exe
cacls c:\winnt\system32\find.exe
cacls c:\winnt\system32\findstr.exe
cacls c:\winnt\system32\finger.exe
cacls c:\winnt\system32\forcedos.exe
cacls c:\winnt\system32\format.com
cacls c:\winnt\system32\ftp.exe
cacls c:\winnt\system32\hostname.exe
cacls c:\winnt\system32\iisreset.exe
cacls c:\winnt\system32\ipconfig.exe
cacls c:\winnt\system32\ipxroute.exe
cacls c:\winnt\system32\label.exe
cacls c:\winnt\system32\logoff.exe
cacls c:\winnt\system32\makecab.exe
```

cacIs c:\winnt\system32\mem.exe  
cacIs c:\winnt\system32\mmc.exe  
cacIs c:\winnt\system32\mode.com  
cacIs c:\winnt\system32\more.com  
cacIs c:\winnt\system32\mountvol.exe  
cacIs c:\winnt\system32\msg.exe  
cacIs c:\winnt\system32\nbtstat.exe  
cacIs c:\winnt\system32\net.exe  
cacIs c:\winnt\system32\net1.exe  
cacIs c:\winnt\system32\netsh.exe  
cacIs c:\winnt\system32\netstat.exe  
cacIs c:\winnt\system32\nslookup.exe  
cacIs c:\winnt\system32\ntbackup.exe  
cacIs c:\winnt\system32\ntdsutil.exe  
cacIs c:\winnt\system32\ntsd.exe  
cacIs c:\winnt\system32\os2.exe  
cacIs c:\winnt\system32\passprop.exe  
cacIs c:\winnt\system32\pathping.exe  
cacIs c:\winnt\system32\ping.exe  
cacIs c:\winnt\system32\posix.exe  
cacIs c:\winnt\system32\print.exe  
cacIs c:\winnt\system32\query.exe  
cacIs c:\winnt\system32\rasdiag.exe  
cacIs c:\winnt\system32\rccp.exe  
cacIs c:\winnt\system32\recover.exe  
cacIs c:\winnt\system32\regedt32.exe  
cacIs c:\winnt\system32\regini.exe  
cacIs c:\winnt\system32\register.exe  
cacIs c:\winnt\system32\regsvr32.exe  
cacIs c:\winnt\system32\replace.exe  
cacIs c:\winnt\system32\reset.exe  
cacIs c:\winnt\system32\rexc.exe  
cacIs c:\winnt\system32\route.exe  
cacIs c:\winnt\system32\routeMon.exe  
cacIs c:\winnt\system32\routerv.exe  
cacIs c:\winnt\system32\rsh.exe  
cacIs c:\winnt\system32\runas.exe  
cacIs c:\winnt\system32\rnonce.exe  
cacIs c:\winnt\system32\seccedit.exe  
cacIs c:\winnt\system32\setpwd.exe  
cacIs c:\winnt\system32\shadow.exe  
cacIs c:\winnt\system32\share.exe  
cacIs c:\winnt\system32\snmp.exe  
cacIs c:\winnt\system32\snmptrap.exe  
cacIs c:\winnt\system32\svrMgr.exe  
cacIs c:\winnt\system32\subst.exe  
cacIs c:\winnt\system32\sysedit.exe  
cacIs c:\winnt\system32\syskey.exe  
cacIs c:\winnt\system32\taskmgr.exe  
cacIs c:\winnt\system32\telnet.exe  
cacIs c:\winnt\system32\termsrv.exe  
cacIs c:\winnt\system32\ftp.exe  
cacIs c:\winnt\system32\tlntadmn.exe  
cacIs c:\winnt\system32\tlntsess.exe  
cacIs c:\winnt\system32\tlntsrv.exe  
cacIs c:\winnt\system32\ttracert.exe  
cacIs c:\winnt\system32\tree.com  
cacIs c:\winnt\system32\tadmin.exe  
cacIs c:\winnt\system32\tcon.exe  
cacIs c:\winnt\system32\tldiscon.exe  
cacIs c:\winnt\system32\tskill.exe

```
cacis c:\winnt\system32\tspref.exe  
cacis c:\winnt\system32\tsshutdn.exe  
cacis c:\winnt\system32\usmgr.exe  
cacis c:\winnt\system32\winmsd.exe  
cacis c:\winnt\system32\winver.exe  
cacis c:\winnt\system32\wmimgmt.msc  
cacis c:\winnt\system32\wscript.exe  
cacis c:\winnt\system32\xcopy.exe
```

© SANS Institute 2005, Author retains full rights.