GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Auditing with BindView bv-Control® for Windows® and enum

GSNA Practical Version 4.0 – Option 1

Author: Kris Monroe
Date: March 13, 2005

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Document Conventions 4

Introduction 5

Task 1 – Identification 6
- Identify the System to be Audited 6
  - Characteristics of the Device 7
  - The System's Role in the Organization 8

Risk #1 Risk of System Becoming Compromised 8
- 1.1 Threats and their capacity to inflict damage 8
- 1.2 Vulnerability and Impact for Risk 9
- 1.3 Impact of Vulnerability 9
- 1.4 Primary vulnerabilities that could lead to the impact 9
- 1.5 Scenario of exposure 10
- Testing for Item #1 11
  - Pass/Fail Criteria 11
  - Steps to conduct patch assessment 11
- Audit Results 15
  - Patch Assessment Audit Results 15
- Analyze the results 16
  - Audit Exceptions 16
  - Remediation 16

Risk #2 Risk of Information Disclosure 17
- 2.1 Threats and their capacity to inflict damage 17
- 2.2 Vulnerability and Impact for Risk 17
- 2.3 Impact of Vulnerability 18
- 2.4 Primary vulnerabilities that could lead to the impact 18
- 2.5 Scenario of exposure 18
- Testing for Item #2 19
  - Pass/Fail Criteria 20
  - Steps to conduct anonymous enumeration audit 20
- Audit results 20
  - Anonymous Enumeration Audit Results 20
- Analyze the results 22
  - Audit Exception 22
  - Remediation 22

Risk #3 – Risk of a Denial Of Service Attack 22
- 3.1 Threats and their Capacity to Inflict Damage 22
- 3.2 Vulnerability and Impact for Risk 23
- 3.3 Impact of Vulnerability 23
- 3.4 Primary vulnerabilities that could lead to the impact 23
- 3.5 Scenario of Exposure 24

© SANS Institute 2000 - 2005 Author retains full rights.

Testing for Item# 3 25
Pass/Fail Criteria 25
Steps to conduct running services audit 25
Audit Results 29
Running Services Audit 29
Analyze the results 30
Audit Exceptions 30
Remediation 31

References 32

Table of Figures

Figure 1 - Simplified Network Diagram 5
Figure 2 - BindView RMS Screenshot 12
Figure 3 – Query Builder – Patch Assessment Query 13
Figure 4 – Patch Assessment Scope Options 14
Figure 5 – Query Options dialogue box 14
Figure 6 - BindView RMS Screenshot 26
Figure 7 – Query Builder dialogue box – Field Specification 27
Figure 8 – Query Builder dialogue box – Scope 28
Figure 9 – Query Options dialogue box 29

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Abstract

This is a report on one of three machines that are part of a Microsoft Terminal Services solution which provides access to an application we will call TALLY. The terminal servers were audited using a variety of tools and methods. These tools included host based compliance scanning tools and external security scanning tools.

This document outlines three risks associated with the system identified. One audit point is selected from each of the three risks discussed. Each audit point identifies potential risk for the system. Primary vulnerabilities are discussed and a scenario of exposure is presented by using at last one of these vulnerabilities. The testing section follows a repeatable step-by-step testing procedure to audit for these risks including what results constitute pass and failure (exception). These testing procedures are presented in detail so that others may use them to repeat this audit or to conduct an audit of their own. Next the audit is conducted using these step-by-step testing procedures and the audit results are presented. Finally the findings are analyzed; exceptions are identified and remediation is recommended based on best practice, policy or procedure.

Document Conventions

When you read this practical assignment, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

`command`	Operating system commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell.
`filename`	Filenames, paths, and directory names are represented in this style.
`computer output`	The results of a command and other computer output are in this style
URL	Web URL's are shown in this style.
Quotation	A citation or quotation from a book or web site is in this style.

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction

I am a Senior IS Security Compliance Analyst for a Large Internet Protocol (IP)-based Telecommunications Carrier (LIPTC). The internal network is extremely large and spans numerous continents, countries and major cities. Thousands of workstations and servers with a variety of operating systems exist on this network. Due to the vastness and complexity of the network I will not be providing a detailed network diagram. Instead I will provide a simplified diagram showing only some of the devices related to the audit and the scenarios of exposure.

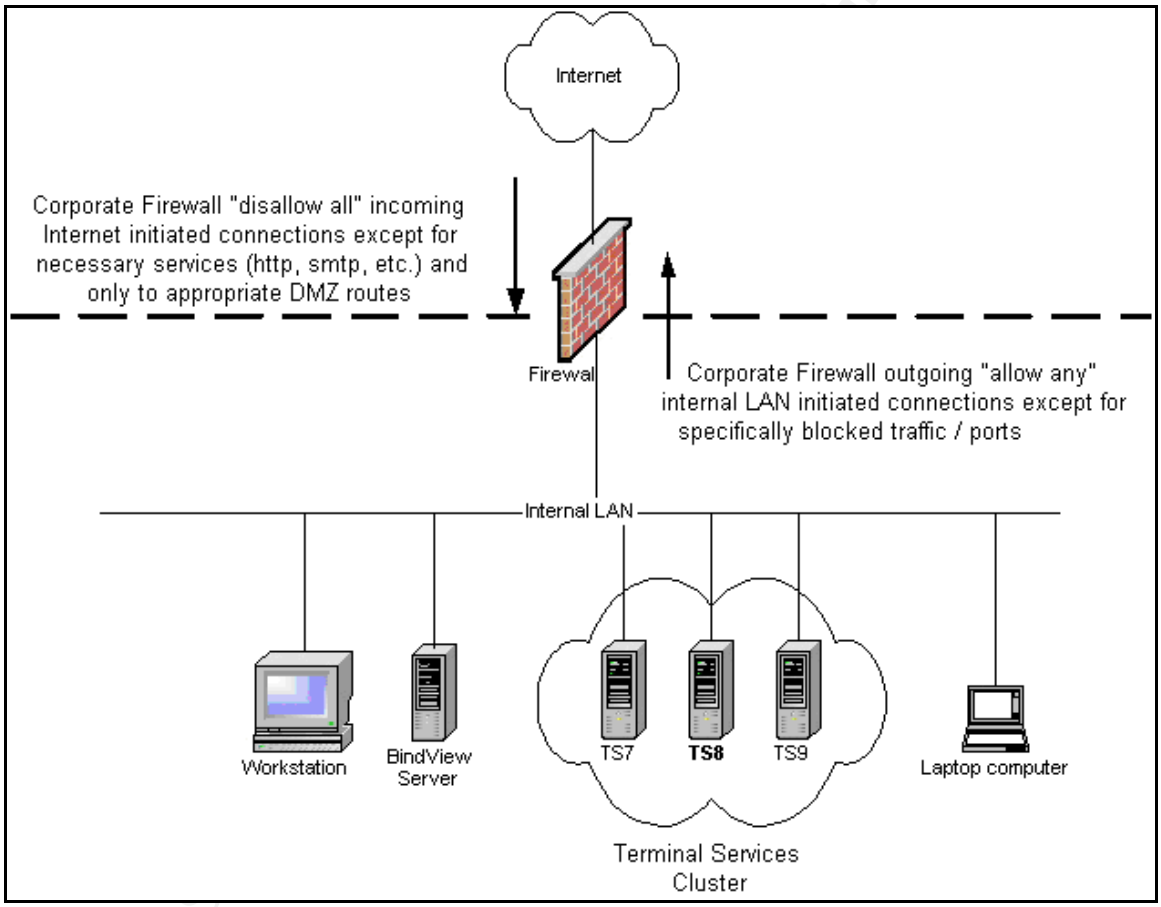

Figure 1 - Simplified Network Diagram

The network spans many countries and cities and sits behind a series of firewalls, proxies and many other network/security devices. While the use of firewalls helps reduce the immediacy for patching, firewalls should not be considered a cure-all. As shown in Figure 1 our firewall rules disallow all incoming Internet initiated connections except for necessary services. Our outgoing rules basically “allow any” internal LAN initiated connections except for some specifically blocked traffic /ports (e.g. NetBIOS traffic). Risk of compromise exists as long as there is a connection between the internal network and the Internet.

© SANS Institute 2000 - 2005
Author retains full rights.

To help address this risk our company has created a Vulnerability Management group, similar to the Patch and Vulnerability Group (PVG) outlined in the NIST Special Publication 800-40 "Procedures for Handling Security Patches".[1]

The stated mission of Vulnerability Management is as follows:

> To provide a forum for the implementation of the standard procedure for the deployment of operating system, application and firmware patches required to protect LIPTC's information system infrastructure from internal and external security threats and exposures.

Roles and Responsibilities of Vulnerability Management are:

- Receive and research notifications of vulnerabilities from various sources, including vendors, suppliers and communities of interest
- Filter notifications for those that apply to the LIPTC environment
- Provide expert advice on severity of announced vulnerabilities
- Provide expert advice on risk mitigation through patching and/or other methods
- Hold a weekly communication forum for all responsible internal parties to determine course of action

Security Compliance is also responsible for internal compliance audits. These audits are used to check for compliance to the patch management determined course of action as well as for conducting systems vulnerability assessments. These compliance audits are typically conducted using BindView bv-Control® for Windows®.

Task 1 – Identification

Identify the System to be Audited

As mentioned in the abstract above this information is in regards to an internal audit conducted against a set of terminal servers supporting the application I will refer to as TALLY. TALLY is not the actual name of our company's application. One reason why I chose to report on this system was due to a recent request for access to this application by another company acquiring part of our business. This request was being made by way of a list of services that they would require under a Transition of Services Agreement (TSA). During the term of this TSA some migration of our business to theirs would take place. Our company was being requested to provide support for equipment and software of LIPTC, including TALLY, the terminal servers and more. A migration team was being formed for the purpose of reviewing and migrating the business information systems and data to the customers' designed platforms. This migration team was also gathering information on TALLY and related systems to try and determine the best way to migrate these services to the customer. Long term

[1] NIST Special Publication 800-40

© SANS Institute 2000 - 2005 Author retains full rights.

external access to applications, including TALLY, was outlined as potentially being needed. While the details have not been fully determined at the time of this writing we may have to share access to TALLY with the hopes that access can somehow be separated. There is now the possibility that these terminal servers could be accessed from both outside our company by non-employees and internally from within our local area network. An audit was conducted to determine the security posture of the LIPTC systems used to access these applications our customer was requesting. The scope of the audit for this paper is limited to one of the three terminal servers supporting the TALLY application. The actual LIPTC audit was conducted against all three terminal servers.

Characteristics of the Device

Computer Model, Operating System and Software Version

As outlined in the NIST Special Publication 800-40 it is important to have an inventory of hardware and software. It is equally important that the information remain current so that it may be referenced when determining whether a system is at risk to a particular vulnerability. Having such an inventory or database makes the job of LIPTC Vulnerability Management easier by not having to check against inappropriate or unused versions.

Our IS department had started a systems inventory prior to my arrival at the company, but sadly it has fallen behind in being updated. The following is information pulled from the LIPTC Asset Management Website showing the general characteristics of the device to be audited:

General

System Contact:	On-Call	Additional Documentation	
Status:	Production	Location:	[sanitized]
Host ID:		Serial Number:	[sanitized]
Manufacturer:	Compaq	Model:	Proliant DL360
Parent :	None		
OS:	Windows 2000TS	Maint Contract:	
CPU Description:	[2] Pentium III	Memory (MB)	2048
Notes:	Rack *x*		

Subordinate Hardware:

Services this host is associated with:
TALLY

The installed software page of the Asset Management Website resulted in no additional information on any other software installed on this server.

The Asset Management Website and manual examination outline the server to be audited is a Compaq Proliant DL360 with two Pentium III CPUs and 2048 MB of memory. The operating system installed is Windows 2000 Advanced Server Service Pack 4 with Terminal Services.

© SANS Institute 2000 - 2005 Author retains full rights.

To access the TALLY application one must login to the terminal server cluster. This cluster is comprised of three Windows 2000 terminal servers that are joined to a legacy NT4 domain. It is believed that these servers were not migrated to our newer Active Directory domain for application compatibility.

The System's Role in the Organization

The internal IS Customer Support TALLY homepage gives the following description of the TALLY system:

> TALLY is a trouble management system used by certain LIPTC employees. It consists of a Windows 2000 Terminal Server Cluster using approximately 10 different applications that access an oracle database. The TALLY applications provide functions as follows: trouble ticketing, order entry and review, monitoring, quoting, reporting, employee data, etc. TALLY was designed so that it could not be accessed directly from a user's desktop but rather accessed only through a terminal server.

While collecting information on TALLY and the systems that support the application we discovered that we have little documentation. Not much is known about the terminal servers and the application itself as most everything was setup by a former Intel Platform employee who was in a hurry to setup the system shortly after the attacks of September 11th (9/11/2001).

Risk #1 Risk of System Becoming Compromised

1.1 Threats and their capacity to inflict damage

- System: Terminal Servers
- Primary Vulnerabilities:
  - **Unpatched operating system vulnerabilities**
  - Unnecessary Operating System services running

- Likelihood of Exploitation: High
- Value of the Asset: High
- Potential Impact: High
  - Confidentiality – Unauthorized users that gain administrative or escalated privileges by leveraging vulnerabilities have unlimited access to the sensitive data stored on the server.
  - Integrity - Unauthorized and unrestrained changes could be made to the server. Sensitive data could be copied, changed or deleted.
  - Availability – By taking advantage of unpatched vulnerabilities or vulnerable services unauthorized users could interrupt necessary services or cause a denial of service causing the server and application to be unavailable.

© SANS Institute 2000 - 2005 Author retains full rights.

1.2 Vulnerability and Impact for Risk

Failure to patch vulnerable systems in a timely manner introduces significant business risk to the enterprise. There are continually growing numbers of attacks seeking to exploit unpatched operating system vulnerabilities. IS and Security departments should develop and document patch risk assessment and deployment procedures to better manage this risk.

1.3 Impact of Vulnerability

The impact of vulnerability is about loss. Losses due to breach of systems can result when unauthorized users gain administrative or escalated privileges by leveraging vulnerabilities. Once leveraged these vulnerabilities could allow unauthorized and unrestrained changes to the server. Sensitive data could be copied, changed or deleted. Interruption of necessary services or denial of service could occur causing the server and application to become unavailable. Compromise of unpatched operating system vulnerabilities can impact confidentiality, integrity and availability which could lead to the following loss:

- **Privacy loss** – Since TALLY contains customer information and employee data the user could suffer personally through loss of privacy, unauthorized use of his/her identity possibly leading to identity theft.

- **Loss of Public Confidence/Reputation** – If employee data or customer information was disclosed, damage to customer confidence, public image and even shareholder/supplier loyalty could be affected. If the customer relied upon application was interrupted their company could also result in loss of public confidence/reputation as well as LIPTC's.

In the past personal information belonging to LIPTC employees has actually been posted to a website by a disgruntled employee. Our company would obviously like to avoid another situation like this. I am sure our shareholders and customers would also like to avoid this.

1.4 Primary vulnerabilities that could lead to the impact

Unpatched operating system vulnerabilities - if a system is not fully patched it could be subject to RPC DCOM buffer overflow vulnerabilities or similar vulnerabilities that various malware writers are taking advantage of. Infection by a worm or bot due to these types of buffer overflows could easily result in unauthorized users gaining administrative or escalated privileges.

Unnecessary Operating System services running - if a system is running unnecessary services it may be vulnerable to targeted attempts to compromise the system.

1.5 Scenario of exposure

© SANS Institute 2000 - 2005 Author retains full rights.

In this scenario assume the patch for Microsoft Bulletin ID MS04-011, a Microsoft LSASS Buffer Overrun, was missing from the terminal server. By missing this patch the Windows 2000 Server would be vulnerable to several flaws, ranging from remote code execution to denial of service. Recent events have shown that a variant of the RBOT Trojan, commonly referred to as RXBOT, has the ability to scan for hosts that are affected by the MS04-011 Microsoft LSASS Buffer Overrun vulnerability. Also in this scenario we will assume a user brings in their personal laptop and connects it to the corporate network. This laptop is also unpatched, not running updated Antivirus software and is infected with RXBOT. The user logs in and unbeknownst to them the RXBOT goes to work scanning for other vulnerable machines. Once a vulnerable host is identified RXBOT can exploit those vulnerabilities to infect that host.

According to the Trend Micro website RXBOT includes the ability to:

- Create a Denial of Service condition by sending Ping, SYN or UDP packet floods.
- Capture video
- Send email via SMTP or POP
- Send and receive files via DCC
- Receive files via TFTP
- Install a key logger
- Start an HTTP web server
- Start an RLOGIN server
- Start an IDENT server
- Act as a Socks4 proxy server
- Start a port scan
- Manipulate files / directories of choice
- Keep a complete log of all activity

Besides MS04-011 RXBOT also has the ability to scan for hosts that are affected by the following vulnerabilities:

- MS01-059 Microsoft Unchecked Buffer in Universal Plug and Play
- MS03-001 Microsoft Unchecked Buffer in RPC
- MS03-007 Microsoft Unchecked Buffer in WebDAV
- MS03-026 Microsoft Buffer Overrun in RPC

Within a matter of minutes the vulnerable terminal server is infected with RXBOT. RXBOT calls out making use of the “allow any” nature of the outbound firewall rules and establishes an IRC connection “dialing home” to announce it is ready to receive files and allowing manipulation of files / directories of the hacker’s choice. LIPTC employee and customers’ data, the TALLY application and the terminal server itself are in the hands of a hacker.

Testing for Item #1

The LIPTC vulnerability management group assesses the risk of vulnerabilities to the company. Compliance reporting for patches of interest is done by way of

© SANS Institute 2000 - 2005 Author retains full rights.

a Weekly Security Metrics report. Patches of interest typically pertain to Critical and High risk assessments. Some Medium risk patches are reported on when they supersede a previous patch of interest. This is not to say that Medium or Low items should be ignored. Items rated as Medium are supposed to be applied within one month in order to reduce prolonged exposure and to mitigate risk. Items rated as low are supposed to be applied within one quarter to also reduce prolonged exposure and to mitigate risk.

Because the terminal servers have been in place for almost four years, testing for patches will be conducted for all Microsoft patches regardless of assessment. This is being done so that we might catch any prolonged exposure and mitigate the risk of that exposure.

Pass/Fail Criteria

Pass

The criteria for passing the Patch Assessment test would be when the particular Bulletin ID patch status is reported as Installed.

Fail

Failure to pass the test would be when the patch status is shown as Missing or Missing Service Pack.

Bulletin ID TOOL03-039 should be excluded from the pass/fail criteria. This item is simply a tool used to remove Blaster worm and Nachi worm infections from computers that are infected. This item is reported on when all patch assessments are chosen. This item's status should be considered informational only and is not required on LIPTC servers.

In BindView patch assessment reason codes are given when a patch is not installed. This field will not be shown in test results due to the amount of space available on a page. Below is an example of a reason code where the version 5.2.3735.1 of file hhctrl.ocx is older than the patched version of 5.2.3790.233. In this case the Status field for this bulletin would show Missing.

File \\HOSTNAME\C$\WINNT\system32\hhctrl.ocx has a file version [5.2.3735.1] that is less than what is expected [5.2.3790.233].

Steps to conduct patch assessment

Use BindView bv-Control® for Windows® patch assessment

Launch BindView RMS Console from the Start menu

Start • BindView RMS • BindView RMS Console

Select New Query from the toolbar.

© SANS Institute 2000 - 2005 Author retains full rights.

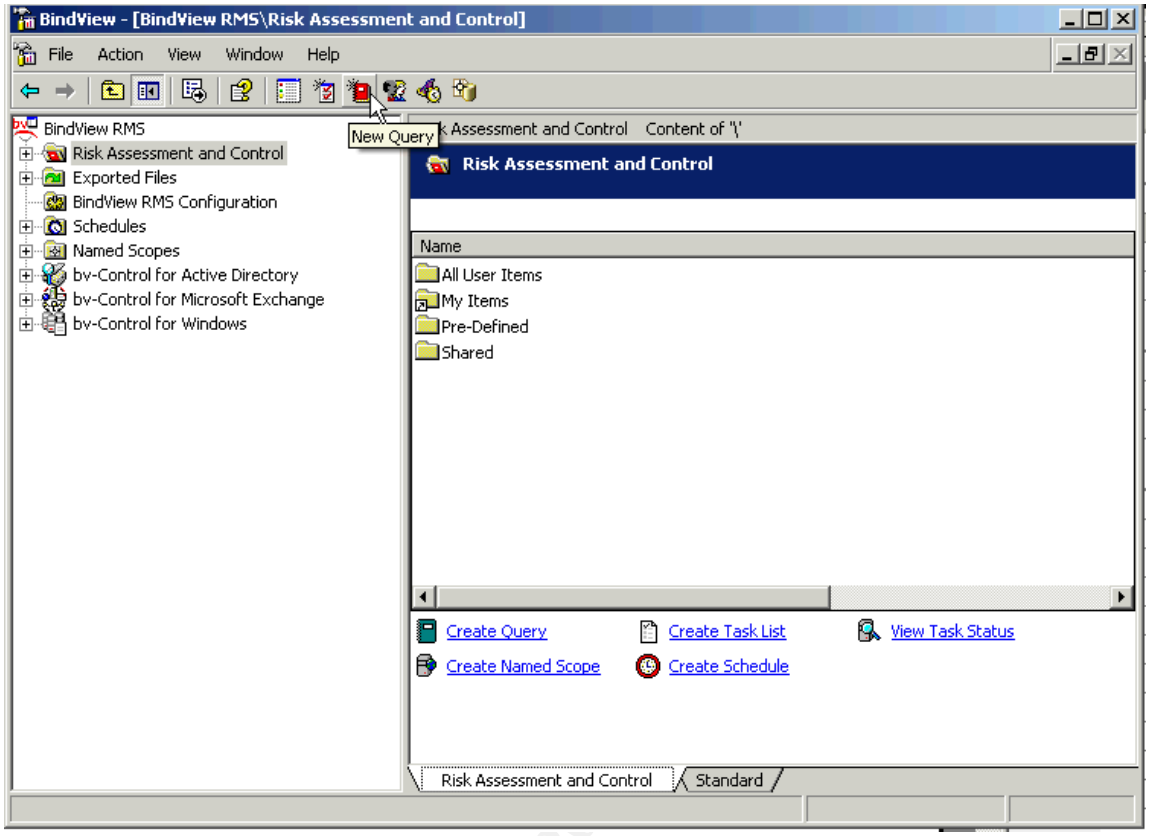

Figure 2 - BindView RMS Screenshot

Double-click **bv-Control for Windows** to expand data sources.

Select **Patch Assessment** by double-clicking it.

© SANS Institute 2000 - 2005
Author retains full rights.

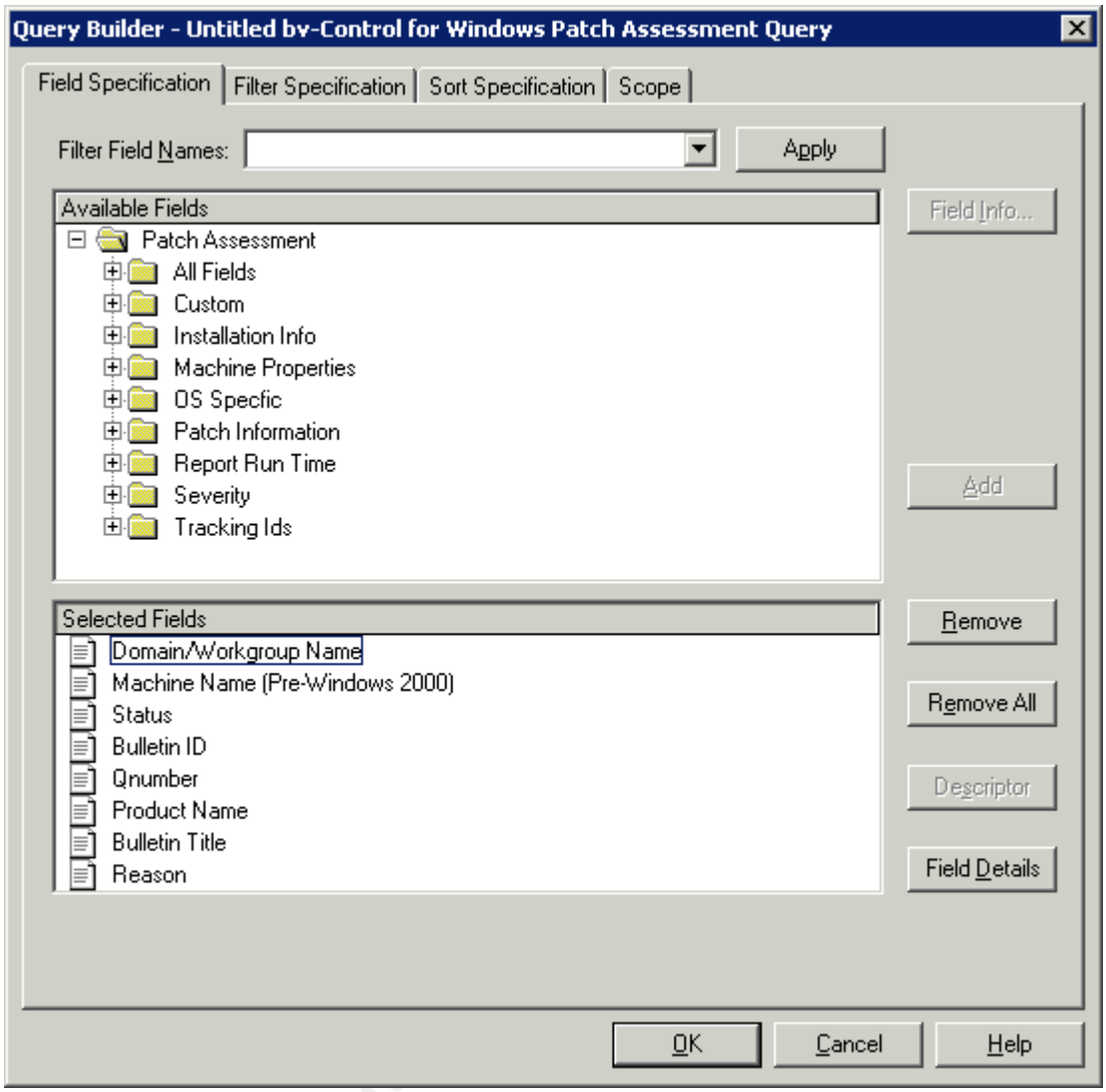

Figure 3 – Query Builder – Patch Assessment Query

Next, select the **Scope** tab
Expand **Microsoft Windows Network**
Expand the Domain – expand **Server (From Browser)**
Select the server to be audited and click **Add Scope**
In Record Status Filtering section clear the check boxes for Show Warnings, Show Informational Messages, Show Notes and Show Effectively Installed Patches. Ensure that Show Missing Patches, Show Missing Service Packs and Show Installed Patches are checked.
Under Patch Filtering Options ensure that Check for all Patches for all Products radio button is selected.

Your selections should look like those in Figure 4.

© SANS Institute 2000 - 2005
Author retains full rights.

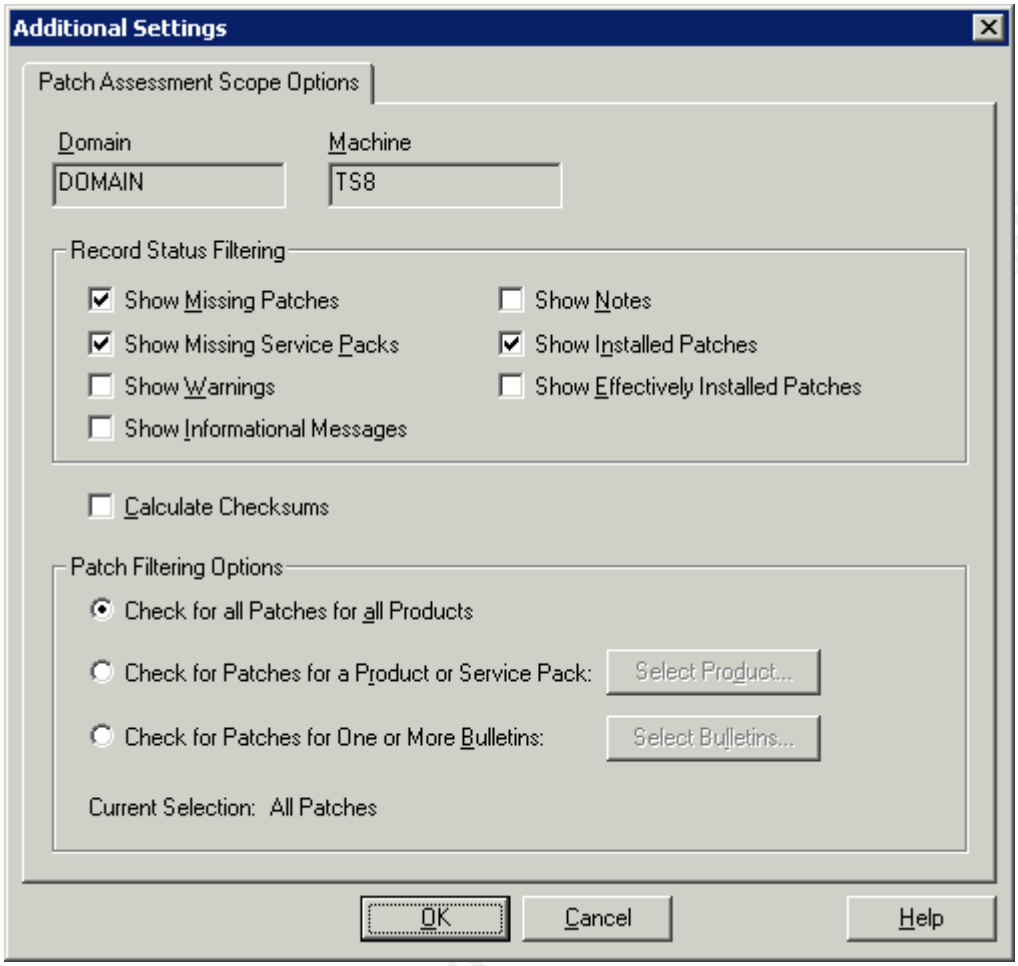

Figure 4 – Patch Assessment Scope Options

Click **OK**
Ensure View As Grid is selected as shown in Figure 5.

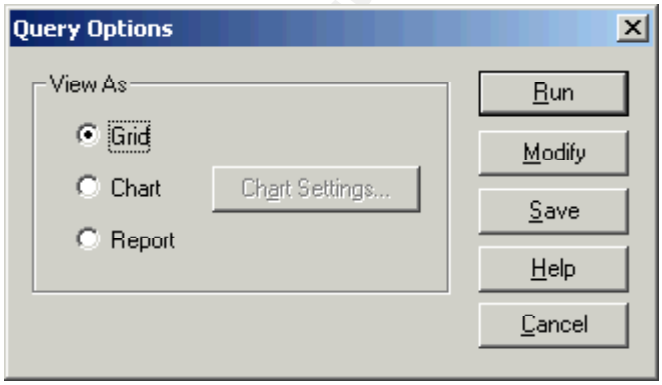

Figure 5 – Query Options dialogue box

Click **Run**
Once the query is complete a grid is returned with the results.

© SANS Institute 2000 - 2005
Author retains full rights.

Audit Results

Patch Assessment Audit Results

Domain Name	Machine Name	Status	Bulletin ID	Qnumber	Product Name
DOMAIN	TS8	Missing Service Pack	[None]	[None]	Office 2000
DOMAIN	TS8	Missing	MS00-015	Q256167	Office 2000
DOMAIN	TS8	Installed	MS02-050	Q329115	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS03-008	Q814078	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS03-023	Q823559	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS03-026	Q823980	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS03-034	Q824105	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS03-037	Q822150	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS03-039	Q824146	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS03-040	Q828026	Windows Media Player 6.4 for Windows 2000
DOMAIN	TS8	Installed	MS03-041	Q823182	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS03-042	Q826232	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS03-043	Q828035	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS03-044	Q825119	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS03-045	Q824141	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS03-049	Q828749	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS04-003	Q832483	MDAC 2.5
DOMAIN	TS8	Installed	MS04-004	Q832894	Internet Explorer 6
DOMAIN	TS8	Installed	MS04-007	Q828028	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS04-011	Q835732	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS04-012	Q828741	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS04-013	Q837009	Internet Explorer 6
DOMAIN	TS8	Installed	MS04-014	Q837001	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS04-018	Q823353	Internet Explorer 6
DOMAIN	TS8	Installed	MS04-019	Q842526	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS04-020	Q841872	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS04-022	Q841873	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS04-023	Q840315	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS04-024	Q839645	Windows 2000 Advanced Server
DOMAIN	TS8	Installed	MS04-025	Q867801	Internet Explorer 6
DOMAIN	TS8	Missing	MS04-028	Q833989	Internet Explorer 6
DOMAIN	TS8	Missing	MS04-031	Q841533	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS04-032	Q840987	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS04-037	Q841356	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS04-041	Q885836	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS04-043	Q873339	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS04-044	Q885835	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS05-001	Q890175	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS05-002	Q891711	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS05-003	Q871250	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS05-008	Q890047	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS05-010	Q885834	Windows 2000 Advanced Server

© SANS Institute 2000 - 2005 Author retains full rights.

DOMAIN	TS8	Missing	MS05-011	Q885250	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS05-012	Q873333	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS05-013	Q891781	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS05-014	Q867282	Internet Explorer 6
DOMAIN	TS8	Missing	MS05-015	Q888113	Windows 2000 Advanced Server
DOMAIN	TS8	Missing	MS99-044	Q241901	Excel 2000
DOMAIN	TS8	Missing	TOOL03-039	Q833330	Windows 2000 Advanced Server

Analyze the results

Audit Exceptions

Twenty-two patches are identified as missing. These items are highlighted in yellow in the Patch Assessment Audit Results above with the exclusion of ID TOOL03-039. As mentioned in the criteria above bulletin ID TOOL03-039 is simply a worm removal tool and not a required patch.

The Bulletin IDs and Qnumbers are listed for all items but one and is the first patch identified as missing. This first exception correlates to the Office 2000 product. While not shown in the audit results above, the reason code outlines the following information:

> The latest service pack for this product is not installed. Currently Gold is installed. The latest service pack is SP3.

Remediation

In order to reduce prolonged exposure and to mitigate risk it is recommended to apply patches for all the exceptions identified in the Patch Assessment Audit Results including applying Office 2000 Service Pack 3.

Risk #2 Risk of Information Disclosure

2.1 Threats and their capacity to inflict damage

- System: Terminal Servers
- Primary Vulnerabilities:
  - **Anonymous Access – Null Session**
  - Weak passwords
  - Shares without proper permissions set
  - SNMP using the default “public” string

- Likelihood of Exploitation: High
- Value of the Asset: High
- Potential Impact: High
  - Confidentiality – sensitive account information and server settings could be enumerated anonymously. Customer and/or employee

© SANS Institute 2000 - 2005 Author retains full rights.

data could be released by leveraging additional vulnerabilities.
  - Integrity – by leveraging additional vulnerabilities unauthorized changes could be made to the server. Sensitive data could be copied, changed or deleted.

2.2 Vulnerability and Impact for Risk

About four years ago the FBI teamed up with industry security experts to put together a list of the twenty most important Internet security vulnerabilities. Information leakage via null session connections was identified as one of the top ten Windows vulnerabilities in that list. As of the writing of this document the SANS Top 20 Vulnerabilities[2] ranks Windows Remote Access Services, which includes Anonymous Logon, as the number three top vulnerability in Windows systems.

By default Windows 2000 allows anonymous users to perform activities such as enumerating users, groups, shares and password policies via anonymous logon. This anonymous access is referred to as Null Sessions. Null Sessions can be used to gather more information about the computer. This information can then be used to formulate continued attacks against the system. This being the default setting is one reason why anonymous access is outlined so high as a dangerous vulnerability to have.

IS and Security departments should develop system baselines and deployment procedures to better manage this risk. Period baseline checks should be conducted to check for compliance to these baselines.

2.3 Impact of Vulnerability

The impact of vulnerability is about loss. Losses due to breach of systems can result when unauthorized users gain anonymous or unauthorized access to data by leveraging weaknesses. Sensitive data could be copied, changed or deleted. Anonymous or unauthorized access to data can impact confidentiality and integrity which could lead to the following loss:

- **Privacy loss** – Since TALLY contains customer information and employee data the user could suffer personally through loss of privacy, unauthorized use of his/her identity possibly leading to identity theft.

- **Loss of Public Confidence/Reputation** – If employee data or customer information was disclosed, damage to customer confidence, public image and even shareholder/supplier loyalty could be affected.

2.4 Primary vulnerabilities that could lead to the impact

Anonymous Access – Null Session - unauthorized users gain anonymous or unauthorized access to data that aids in continued focused attacks.

[2] SANS Top 20 Vulnerabilities http://www.sans.org/top20/

© SANS Institute 2000 - 2005 Author retains full rights.

Weak passwords – with a list of account names and groups gathered from null sessions weak passwords are easily brute forced allowing unauthorized use of a valid account.

Shares without proper permissions set – shares with improper permissions set may allow anonymous or unauthorized access to data. By default new Windows 2000 shares have permissions set to Everyone – Full Access.

SNMP using the default "public" string - SNMP, is a commonly used service that provides network management and monitoring capabilities. Unauthorized users may gain information about a device using the default "public" read community string aiding in continued focused attacks.

2.5 Scenario of exposure

For this scenario assume the terminal server has the default configuration allowing null sessions. A hacker may use system information returned from a null session to target the terminal servers for further exploitation. Access to such information greatly simplifies a brute force password attack against those user accounts identified. Brute force password attacks will be more successful if weak passwords exist for those accounts identified.

A few years ago a worm called W32/Lioten, commonly referred to as IraqiWorm, was discovered to have the ability to scan for hosts with anonymous access allowed. In this scenario we will assume a user brings in their personal laptop and connects it to the corporate network. This laptop also has a default configuration allowing null sessions, is not running updated Antivirus software and is infected with W32/Lioten or a variant thereof. The user logs in and unbeknownst to them the W32/Lioten goes to work scanning for other vulnerable machines. Once a vulnerable host is identified W32/Lioten can exploit those vulnerabilities to infect that host.

According to the Trend Micro website W32/Lioten includes the ability to:

- Spread to and run on systems running Windows 2000/XP/.NET
- Connect to random IP addresses and access a remote network share
- Schedule itself to execute after 1 to 2 minutes has elapsed on the infected system.

The worm propagates by the generating of a pseudo-random IP address and exploits hosts which have the following weak security configuration:

- Anonymous null sessions fully enabled
- Weak (or null) passwords on privileged user accounts

Once the worm has a list of valid user accounts from the Null Session, it attempts basic brute forcing of the passwords using a list of passwords

© SANS Institute 2000 - 2005 Author retains full rights.

(dictionary attack) against those user accounts. If weak passwords exist on the Terminal Server alongside anonymous null sessions then W32/Lioten could crack the passwords and infect the server.

Testing for Item #2

One of the best ways to audit for anonymous enumeration is to actually attempt to get information via a remote null session. One way to do this is to manually attempt to establish a null session with the use of the `net use` command. My preferred audit method is to use a tool named enum to enumerate using null sessions. Enum was written by Jordan Ritter and is available for download from BindView at the URL given here:

http://www.bindview.com/Resources/RAZOR/Files/enum.tar.gz

Running enum without any switches provides the following usage information:

```
>enum
usage: enum [switches] [hostname|ip]
 -U: get userlist
 -M: get machine list
 -N: get namelist dump (different from -U|-M)
 -S: get sharelist
 -P: get password policy information
 -G: get group and member list
 -L: get LSA policy information
 -D: dictionary crack, needs -u and -f
 -d: be detailed, applies to -U and -S
 -c: don't cancel sessions
 -u: specify username to use (default "")
 -p: specify password to use (default "")
 -f: specify dictfile to use (wants -D)
```

In our audit we will run enum at the command prompt to attempt to get userlist, machine list, namelist dump, sharelist, password policy information, group and member list and finally the LSA policy information and to report in detail (verbose) where applicable. This is done using the following switches -U -M -N -S -P -G -L –d.

By not setting a username and password enum uses the default of “”, or anonymous/null session.

Pass/Fail Criteria

Pass

If enum returns the following information then anonymous or null session access is prevented:

```
server: [host name]
setting up session... fail.
return 5, Access is denied.
```


© SANS Institute 2000 - 2005 Author retains full rights.

Fail
If enum returns `setting up session... success` and then any information on the lists and policy information we were checking for then null sessions are allowed.

Steps to conduct anonymous enumeration audit

From the Start menu select Run
Start • Run…
Enter `cmd` in the Open: text box and click **OK**.
In the command window change directories to where you have enum installed, in this example C:\DL\Enum, then press the enter key.

```
cd \DL\Enum
```

Enter the following in the command window and press the enter key:
```
enum -U -M -N -S -P -G -L -d [hostname or IP]
```

Audit results

Anonymous Enumeration Audit Results

```
>enum -U -M -N -S -P -G -L -d TS8

server: TS8
setting up session... success.
password policy:
 min length: none
 min age: none
 max age: 365 days
 lockout threshold: none
 lockout duration: 30 mins
 lockout reset: 30 mins
opening lsa policy... success.
server role: 3 [primary (unknown)]
names:
 netbios: TS8
 domain: DOMAIN
quota:
 paged pool limit: 33554432
 non paged pool limit: 1048576
 min work set size: 65536
 max work set size: 251658240
 pagefile limit: 0
 time limit: 0
trusted domains:
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
 indeterminate
netlogon done by a PDC server
enumerating names (pass 1)... got 3 accounts, 0 left:
admin: Administrator
 comment: Built-in account for administering the
computer/domain
 login: Thu Nov 04 13:42:46 2004
 good logins: 91
guest: Guest
 comment: Built-in account for guest access to the
computer/domain
guest: TsInternetUser (TsInternetUser)
 comment: This user account is used by Terminal
Services.
getting user list (pass 1, index 0)... success, got 3.
 Administrator (Built-in account for administering the
computer/domain)
 attributes:
 Guest (Built-in account for guest access to the
computer/domain)
 attributes: disabled no_passwd
 TsInternetUser (This user account is used by Terminal
Services.)
 attributes: no_passwd
enumerating shares (pass 1)... got 7 shares, 0 left:
 fs: E$ ()
 fs: Support ()
 ipc: IPC$ (Remote IPC)
 fs: D$ (Default share)
 fs: A$ ()
 fs: ADMIN$ (Remote Admin)
 fs: C$ (Default share)
getting machine list (pass 1, index 0)... success, got
0.
Group: Administrators
TS8\Administrator
DOMAIN\Domain Admins
DOMAIN\LAN Admins
Group: Backup Operators
Group: Guests
TS8\Guest
TS8\TsInternetUser
Group: Power Users
Group: Replicator
Group: Users
NT AUTHORITY\INTERACTIVE
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
NT AUTHORITY\Authenticated Users
DOMAIN\Domain Users
cleaning up... success.
```

Analyze the results

Audit Exception

Anonymous access via null sessions was fully allowed. The server is unnecessarily allowing anonymous access to data that could aid in continued focused attacks.

Remediation

It is recommended to disable NetBIOS Null Sessions.
To do this manually one would perform the following steps:
Start • Programs • Administrative Tools • Local Security Settings • Local Policies • Security Options

Select "Additional restrictions of anonymous connections" in the Policy pane on the right.

Local policy setting from the pull down menu labeled "Local policy setting" can be set to “None. Rely on default permissions”, “Do not allow enumeration of SAM accounts or shares”, or “No access without explicit anonymous permissions”. It is recommended this be set to the last choice to protect the server from access by the null user account.

Risk #3 – Risk of a Denial of Service Attack

3.1 Threats and their Capacity to Inflict Damage

- System: terminal servers
- Vulnerability:
    - **Services that run on the server unnecessarily or unchecked**
    - Poorly configured networking settings leaving system exposed to DoS

- Likelihood of Exploitation –High
- Value of the asset – High
- Potential Impact – High
    - Integrity – if servers crash or become unavailable to process legitimate requests users and more importantly customers can lose confidence in LIPTC.
    - Availability – Some malware causes Denial of Service attacks on the network either on purpose or as they propagate, causing servers to crash or become unavailable to process legitimate

© SANS Institute 2000 - 2005 Author retains full rights.

requests.

3.2 Vulnerability and Impact for Risk

Windows services perform useful and valuable tasks, but there are risks associated with unnecessary services. Those Windows services that are running by default offer opportunities of attack. For example, services often listen on ports that might provide an avenue for an attacker to access the system, or the service may contain a vulnerability that can be exploited by hackers or malware. Security best practices advise that only those services required for the operation of a server be enabled. IS and Security departments should establish a baseline indicating what services should be disabled. Periodic auditing of servers should be conducted to check for unnecessary Windows services.

3.3 Impact of Vulnerability

Again, the impact of vulnerability is about loss. Losses due to interruption of necessary services can result when unauthorized users or malware cause the server and application to be unavailable. Denial of service attacks can impact integrity and availability which could lead to the following loss:

- **Loss of Public Confidence/Reputation** –If the terminal servers the customer relied upon for its business were unavailable due to denial of service attack loss confidence in, and the reputation of, LIPTC could result. The customers' company could also result in loss of public confidence/reputation if they were not able to conduct business because of the denial of service attack.
- **Loss of Revenue/Business** – If public confidence/reputation was affected companies looking for an IP-based Telecommunications Carrier might dismiss LIPTC as a viable candidate. If service level agreements (SLAs) were not met due to a denial of service attack LIPTC might have to refund money to the customer or the customer may be able to contractually end our business relationship.

3.4 Primary vulnerabilities that could lead to the impact

Unnecessary Operating System services running

Microsoft Windows 2000 has a large number of unnecessary services installed and running by default. Many of these services are frequently the target of attempts to compromise the system and/or deny service to the machine.

Default or poorly configured networking settings leaving system exposed to Denial of Service attacks (DoS)

By default Windows 2000 Server is more exposed to DoS attacks than is desirable. To help reduce the exposure to DoS attacks one should add or edit some Tcpip parameter values in the Windows registry. See the section "Registry Settings for Maximum Protection from Network Attack" outlined in the Microsoft

© SANS Institute 2000 - 2005 Author retains full rights.

kb article Security Considerations for Network Attacks[3]. These settings are intended to help defend against Denial of Service attacks.

3.5 Scenario of Exposure

In this scenario assume a default and unnecessary installation of Internet Information Server (IIS) 5.0 was allowed on the terminal server in the haste to get the server up and running. Due to time constraints security best practices, such as running the IIS lockdown tool and patching, were not conducted.

According to Microsoft Security Bulletin MS03-007 [4] Internet Information Server (IIS) 5.0;

- Is installed by default on all server versions of Windows 2000
- Runs by default
- WebDAV is enabled by default

In this scenario a malicious internal user scans the local area network with network mapping software and discovers port 80 open on the terminal server. Next the attacker uses a readily available exploit tool called the Metasploit Framework[5]. While the Metasploit Project website outlines the tool is *"provided for legal penetration testing and research purposes only*", nothing prevents an attacker from using this tool. Using this tool the attacker selects the "IIS 5.0 WebDAV ntdll.dll Overflow" and enters the IP address of the terminal server as the target. The attacker then uses this tool to exploit the vulnerability and send a payload to the terminal server. This payload can include a single remote command, a remote shell allowing multiple commands to be run, or even injecting remote control software (VNC) onto the server, allowing full remote control of the local console.

So in this scenario with the vulnerable World Wide Web Publishing Service running on the Terminal Server an attacker could exploit this vulnerability to take complete control of the system. Complete control would include the ability to shutdown necessary services rendering the system inaccessible for its intended use resulting in denial of service.

Testing for Item# 3

For this audit of running services we will refer to the Center for Internet Security "Windows 2000 Server Operating System Level 2 Benchmark Consensus Baseline Security Settings (Stand-alone and Member Servers)".[6] Section 4.1 Outlines what services the benchmark suggests be disabled. The following is a summary of this section outlining sixteen services that should be disabled.

---

[3] Security Considerations for Network Attacks
[4] Microsoft Security Bulletin MS03-007
[5] Metasploit Framework
[6] Windows 2000 Server Operating System Level 2 Benchmark.

© SANS Institute 2000 - 2005 Author retains full rights.

Alerter – Disabled
Clipbook – Disabled
Computer Browser – Disabled
Fax Service – Disabled
FTP Publishing Service – Disabled
IIS Admin Service – Disabled
Internet Connection Sharing – Disabled
Messenger – Disabled
NetMeeting Remote Desktop Sharing – Disabled
Remote Registry Service – Disabled
Routing and Remote Access – Disabled
Simple Mail Transfer Protocol (SMTP) – Disabled
Simple Network Management Protocol (SNMP) Service – Disabled
Simple Network Management Protocol (SNMP) Trap – Disabled
Telnet – Disabled
World Wide Web Publishing Services – Disabled

Pass/Fail Criteria

Pass

If the service listed is disabled or does not show in the audit because it was uninstalled/removed then that is a pass.

Fail

If the service listed is enabled then that is a failure or audit exemption.

Steps to conduct running services audit

Use BindView bv-Control® for Windows® Services Query

Launch BindView RMS Console from the Start menu

Start • BindView RMS • BindView RMS Console

Select New Query from the toolbar.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

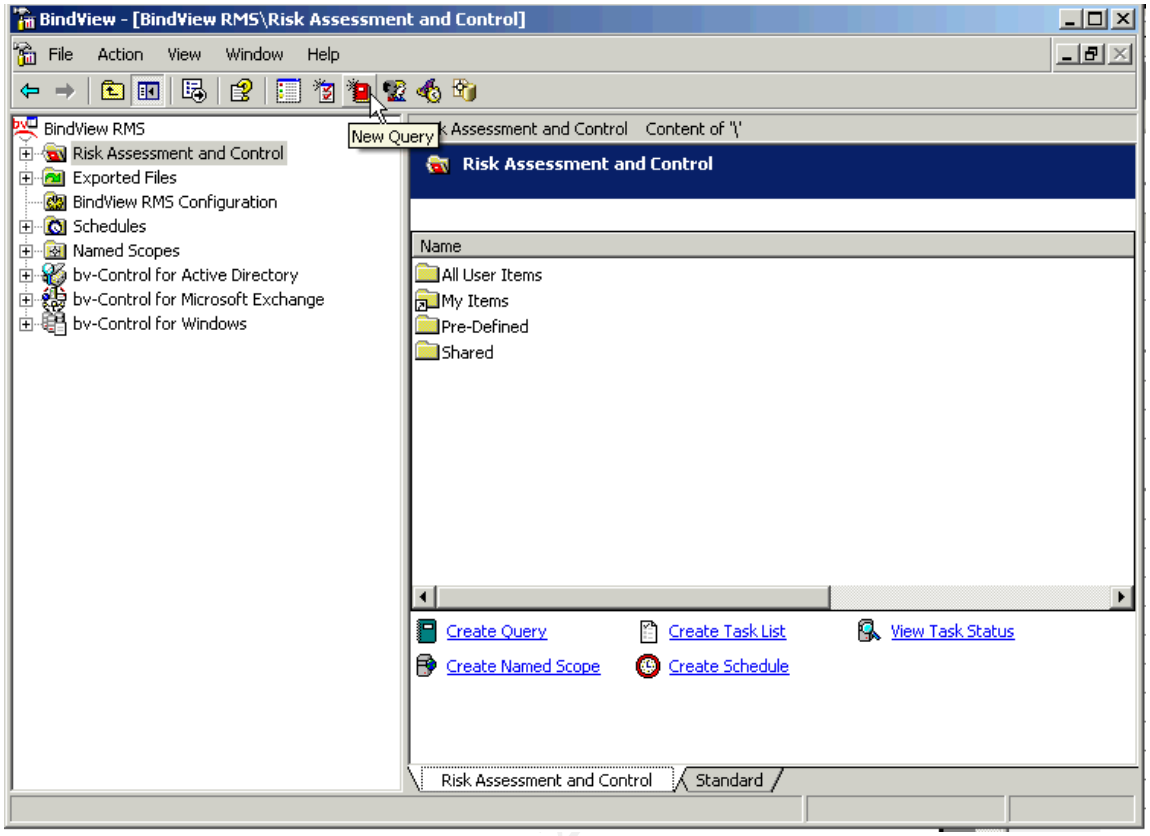

Figure 6 - BindView RMS Screenshot

Double-click **bv-Control for Windows** to expand data sources.

Select **Services** by double-clicking it.

In available fields expand **Service Configuration**

Select **Status** and click **Add**.

Your query builder dialogue box should look the one in Figure 7.

© SANS Institute 2000 - 2005
Author retains full rights.

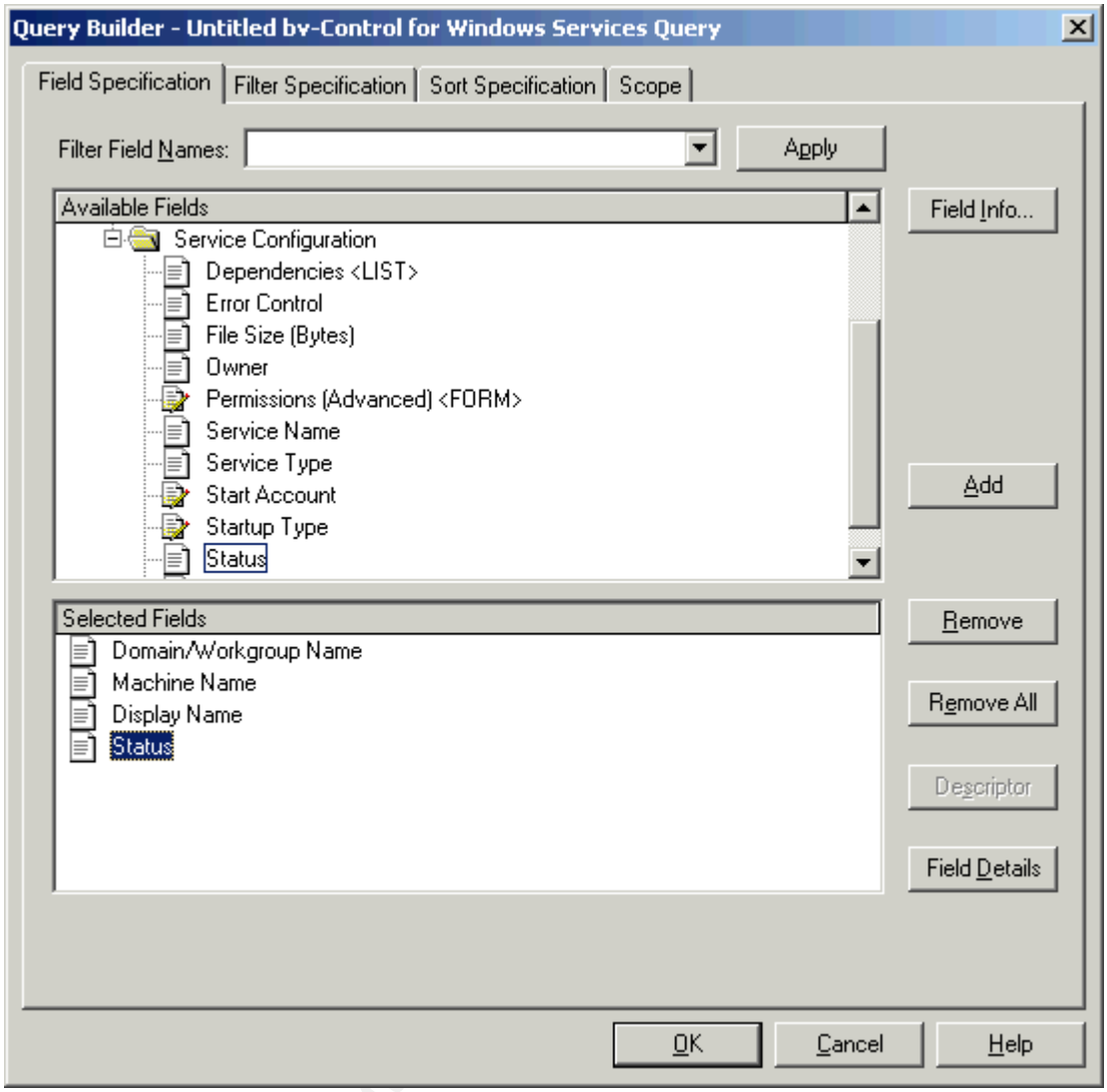

Figure 7 – Query Builder dialogue box – Field Specification

Next, select the **Scope** tab

Expand **Microsoft Windows Network**

Expand the Domain – expand **Server (From Browser)**

Select the server to be audited and click **Add Scope**

Your query builder dialogue box should look the one in Figure 8.

© SANS Institute 2000 - 2005
Author retains full rights.

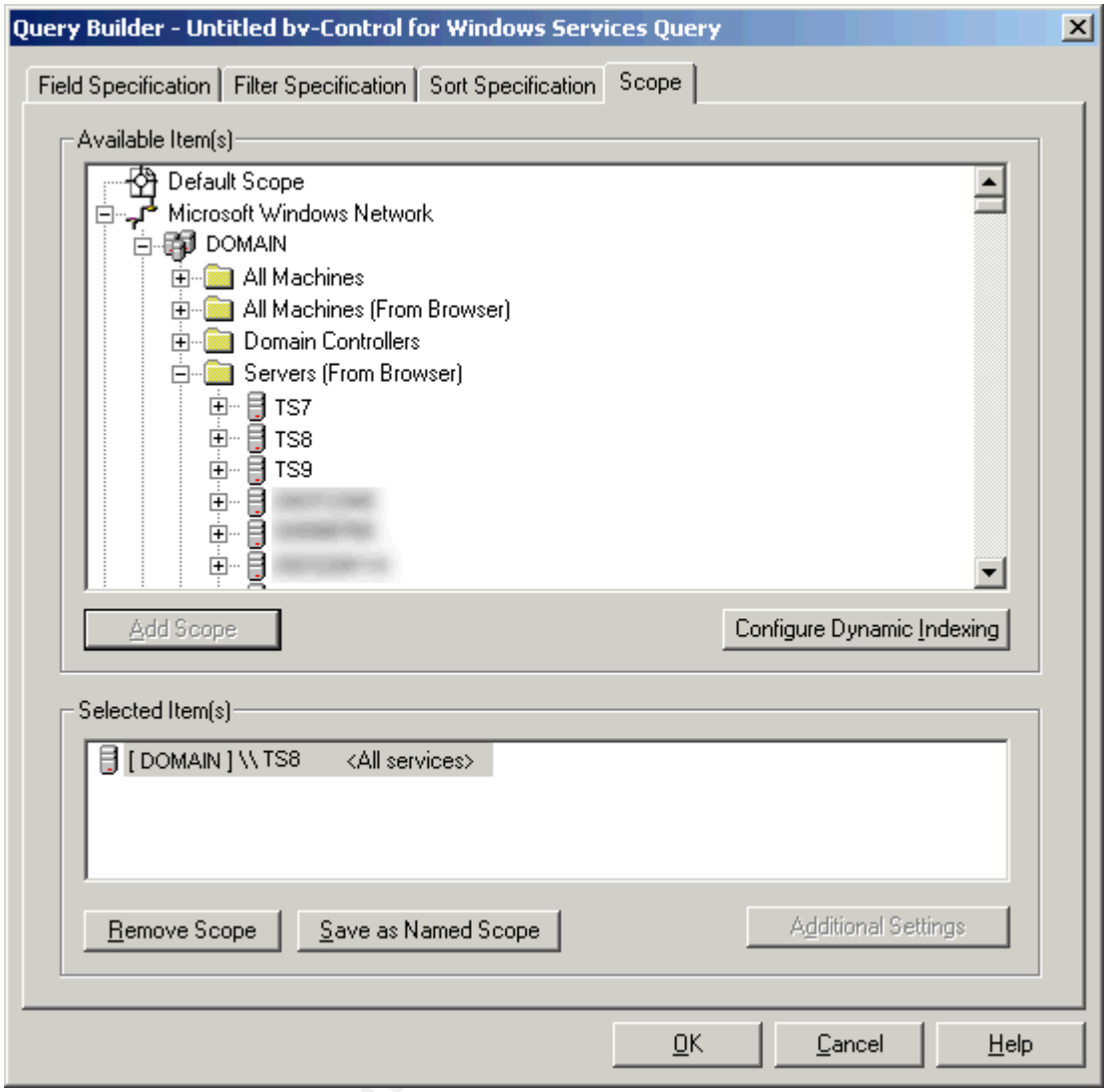

Figure 8 – Query Builder dialogue box – Scope

Note: Do not expand the services under the Server as we are looking to report on all services.

Click **OK**

Ensure View As Grid is selected as shown in Figure 9.

© SANS Institute 2000 - 2005
Author retains full rights.

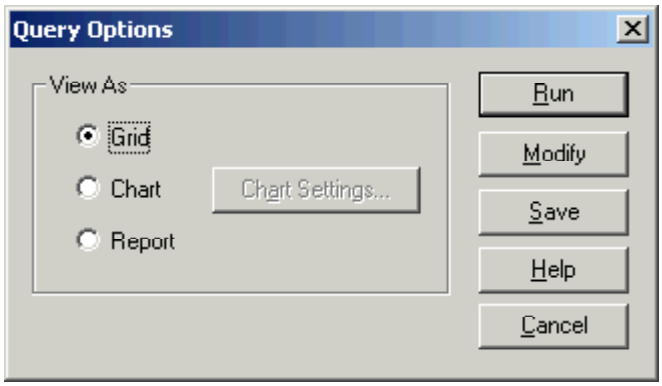

Figure 9 – Query Options dialogue box

Click **Run**

Once the query is complete a grid is returned with the results.
Compare the grid results with the sixteen services that should be disabled.

Audit Results

Running Services Audit

Domain	Name	Service Name	Display Name	Status	Startup Type
DOMAIN	TS8	Alerter	Alerter	Started	Automatic
DOMAIN	TS8	AppMgmt	Application Management	Started	Manual
DOMAIN	TS8	wuauserv	Automatic Updates	Started	Automatic
DOMAIN	TS8	EventSystem	COM+ Event System	Started	Manual
DOMAIN	TS8	CqMgHost	Compaq Foundation Agents	Started	Automatic
DOMAIN	TS8	CPQNicMgmt	Compaq NIC Agents	Started	Automatic
DOMAIN	TS8	CpqRcmc	Compaq Remote Monitor Service	Started	Automatic
DOMAIN	TS8	CqMgServ	Compaq Server Agents	Started	Automatic
DOMAIN	TS8	CqMgStor	Compaq Storage Agents	Started	Automatic
DOMAIN	TS8	sysdown	Compaq System Shutdown Service	Started	Automatic
DOMAIN	TS8	Browser	Computer Browser	Started	Automatic
DOMAIN	TS8	Dhcp	DHCP Client	Started	Automatic
DOMAIN	TS8	Dfs	Distributed File System	Started	Automatic
DOMAIN	TS8	TrkWks	Distributed Link Tracking Client	Started	Automatic
DOMAIN	TS8	MSDTC	Distributed Transaction Coordinator	Started	Automatic
DOMAIN	TS8	Dnscache	DNS Client	Started	Automatic
DOMAIN	TS8	Eventlog	Event Log	Started	Automatic
DOMAIN	TS8	MSFTPSVC	FTP Publishing Service	Started	Automatic
DOMAIN	TS8	IISADMIN	IIS Admin Service	Started	Automatic
DOMAIN	TS8	PolicyAgent	IPSEC Policy Agent	Started	Automatic
DOMAIN	TS8	LicenseService	License Logging Service	Started	Automatic
DOMAIN	TS8	dmserver	Logical Disk Manager	Started	Automatic
DOMAIN	TS8	Messenger	Messenger	Started	Automatic
DOMAIN	TS8	Netlogon	Net Logon	Started	Automatic

© SANS Institute 2000 - 2005
Author retains full rights.

DOMAIN	TS8	NetIQccm	NetIQ AppManager Client Communication Manager	Started	Automatic
DOMAIN	TS8	NetIQmc	NetIQ AppManager Client Resource Monitor	Started	Automatic
DOMAIN	TS8	NSClient	NetSaint NT agent	Started	Automatic
DOMAIN	TS8	Netman	Network Connections	Started	Manual
DOMAIN	TS8	PlugPlay	Plug and Play	Started	Automatic
DOMAIN	TS8	Spooler	Print Spooler	Started	Automatic
DOMAIN	TS8	ProtectedStorage	Protected Storage	Started	Automatic
DOMAIN	TS8	RasMan	Remote Access Connection Manager	Started	Manual
DOMAIN	TS8	RpcSs	Remote Procedure Call (RPC)	Started	Automatic
DOMAIN	TS8	RemoteRegistry	Remote Registry Service	Started	Automatic
DOMAIN	TS8	NtmsSvc	Removable Storage	Started	Automatic
DOMAIN	TS8	seclogon	RunAs Service	Started	Automatic
DOMAIN	TS8	SamSs	Security Accounts Manager	Started	Automatic
DOMAIN	TS8	lanmanserver	Server	Started	Automatic
DOMAIN	TS8	SNMP	SNMP Service	Started	Automatic
DOMAIN	TS8	Surveyor	Surveyor	Started	Automatic
DOMAIN	TS8	SENS	System Event Notification	Started	Automatic
DOMAIN	TS8	Schedule	Task Scheduler	Started	Automatic
DOMAIN	TS8	LmHosts	TCP/IP NetBIOS Helper Service	Started	Automatic
DOMAIN	TS8	TapiSrv	Telephony	Started	Manual
DOMAIN	TS8	TermService	Terminal Services	Started	Automatic
DOMAIN	TS8	SpntSvc	Trend ServerProtect	Started	Automatic
DOMAIN	TS8	WinMgmt	Windows Management Instrumentation	Started	Automatic
DOMAIN	TS8	Wmi	Windows Management Instrumentation Driver Extensions	Started	Manual
DOMAIN	TS8	W32Time	Windows Time	Started	Automatic
DOMAIN	TS8	lanmanworkstation	Workstation	Started	Automatic
DOMAIN	TS8	W3SVC	World Wide Web Publishing Service	Started	Automatic

Analyze the results

Audit Exceptions

Of the sixteen services that should be disabled the following eight were enabled:

Alerter – Enabled
Computer Browser – Enabled
FTP Publishing Service – Enabled
IIS Admin Service – Enabled
Messenger – Enabled
Remote Registry Service – Enabled
Simple Network Management Protocol (SNMP) Service – Enabled
World Wide Web Publishing Services – Enabled

Also of note, the audit results show other non-standard services and/or third

© SANS Institute 2000 - 2005 Author retains full rights.

party services installed and running.

Remediation

To protect against denial of service one should configure applications, services, and operating systems with denial of service attacks in mind.

For the eight exemptions in the audit above, action should be taken to remove/disable the unnecessary and potentially dangerous operating system services. Additional investigation is recommended for the third party services such as Compaq Remote Monitor Service and Compaq Server Agents. There are known vulnerabilities in certain versions of Compaq Management agents that could be exploited by malicious people to compromise a system.

As mentioned throughout this document one should stay current with patches and security updates.

It is also suggested to harden the TCP/IP stack against denial of service particularly by configuring registry settings for maximum protection from network attack.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

References

1. Mell, Peter. Tracy, Miles C. "Procedures for Handling Security Patches". NIST Special Publication 800-40. August 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf

2. SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus". Version 5.0. October 8, 2004. URL: http://www.sans.org/top20/

3. Microsoft kb Article – Security Considerations for Network Attacks. URL: http://www.microsoft.com/technet/security/topics/networksecurity/secdeny.mspx

4. Microsoft Security Bulletin MS03-007 "Unchecked Buffer In Windows Component Could Cause Server Compromise (815021)". URL: http://www.microsoft.com/technet/security/bulletin/MS03-007.mspx

5. Metasploit Framework. URL: http://www.metasploit.com/projects/Framework/

6. The Center for Internet Security. "Windows 2000 Server Operating System Level 2 Benchmark Consensus Baseline Security Settings (Stand-alone and Member Servers)" Version 2.2.1. November 15, 2004. URL: http://www.cisecurity.org/bench_win2000.html

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005
Author retains full rights.