Cisco VPN Client Privilege Escalation Vulnerability

GCIH Certified Incident Handler Practical Assignment
Version 3.0

Gary Dziak, CCNP

November 11 th, 2003

Table of Contents

Statement of Purpose

This GCIH Practical is about an exploit where a user can raise their Window's local system access privileges on a corporate desktop system, where the vulnerable VPN software is installed on. Typical user privileges are restricted to running what is already installed on their assigned laptop or desktop PC. They are unable to change any Windows system settings, registry settings desktop settings and/or environment settings. Because of these restrictions users are unable to install any software on their assigned PC.

These corporate "desktop images" are created, and consist of, approved and tested software deemed necessary, by the business, for users to perform their job function(s). This exploit will demonstrate how a user can either obtain local system administrative privileges or execute applications with local administrative system privileges. Once the local system access is exploited they could pursue other "black hat" activities. (As it will be seen these other activities helped identify this exploit.)

Cisco's VPN client is used to establish a private, end-to-end VPN, Virtual Private Network, communications tunnel between the end-users computer and a Cisco VPN concentrator end-device. At each end point the respective client or hardware device handles the encryption/decryption process. VPN tunnels are usually across a public, non-secure, networks. The Internet is one such network. VPN's give the ability to have end users access servers and services as if they were "local" to that network, no matter where they were geographically.

This exploit does not effect that process.

The Exploit

Name: Cisco VPN Client Privilege Escalation Vulnerability
http://www.securityfocus.com/bid/7599/info/

Bugtraq ID: 7599
Exploit type: Design error
Published May 14th 2003 and updated May 22nd 2003
Discovered by: Nick Staff Nick.Staff@FOX.com (Staff, Nick)

There are no CVE or candidate numbers or CERT numbers.

Operating System: The effected operating systems are as follows:

- Microsoft Windows XP
- Microsoft NT 4.0
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server

The above operating systems are effected regardless of Windows patch or hotfix levels.

Protocol / Service / Applications:
Protocol: No specific protocol is used for this exploit. However Windows Netlogon follows a set of rules. Netlogon verifies local authentication to the local SAM (System Account Manager) database for logging onto a Windows PC. This exploit allows the application to determine what gets used for authentication credentials when executing commands, instead of the operating system.

Service: This exploit alters the GinaDLL, Graphical Identification and Authentication (GINA) dynamic-link library (DLL), registry setting. Winlogon.exe, a part of the Windows boot process, reads these modified registry settings on a Windows startup. By changing these registry settings the exploit permits the VPN client to launch a separate authentication process.

Applications:
Cisco VPN Client 3.0 for Windows
Cisco VPN Client 3.0.5 for Windows
Cisco VPN Client 3.1 for Windows
Cisco VPN Client 3.5.1 C for Windows
Cisco VPN Client 3.5.1 for Windows
Cisco VPN Client 3.5.2 B for Windows
Cisco VPN Client 3.5.2 for Windows
Cisco VPN Client 3.5.4 for Windows
Cisco VPN Client 3.6 (Rel) for Windows
Cisco VPN Client 3.6 for Windows
Cisco VPN Client 3.6.1 for Windows

Variants: http://www.securityfocus.com/bid/7665/info/

Variant Name: Cisco VPN Client Privilege Escalation Variant Vulnerability
Bugtraq ID: 7665
Exploit type: Design error
Published May 22nd 2003 and updated May 23rd 2003

Discovered by: Nick Staff Nick.Staff@FOX.com (Staff, Nick)

There are no CVE or candidate numbers or CERT numbers.

Variant Operating System: The effected operating systems are as follows:

- Microsoft Windows XP
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server

The above operating systems are effected regardless of Windows patch or hotfix levels.

Variant Protocol / Service / Applications:
Variant Protocol: No specific protocol is used for this exploit. However Windows Netlogon follows a set of rules. Netlogon verifies local authentication to the local SAM (System Account Manager) database for logging onto a Windows PC. This exploit allows the application to determine what gets used for authentication credentials when executing commands, instead of the users.

Service: This exploit alters the GinaDLL, Graphical Identification and Authentication (GINA) dynamic-link library (DLL), registry settings in the system's registry. Winlogin.exe, a part of the Windows boot process, reads these modified registry settings on a Windows startup. By changing these registry settings the exploit permits the VPN client to launch separate authentication processes.

Variant Applications:
Cisco VPN Client 3.0 for Windows
Cisco VPN Client 3.0.5 for Windows
Cisco VPN Client 3.1 for Windows
Cisco VPN Client 3.5.1 C for Windows
Cisco VPN Client 3.5.1 for Windows
Cisco VPN Client 3.5.2 B for Windows
Cisco VPN Client 3.5.2 for Windows
Cisco VPN Client 3.5.4 for Windows
Cisco VPN Client 3.6 (Rel) for Windows
Cisco VPN Client 3.6 for Windows
Cisco VPN Client 3.6.1 for Windows

Variant Brief Description: If application access is restricted, via the application program/GUI interface, users could modify the VPN binary files directly and enable the execution of programs with elevated system administrator rights.

As a workaround, administrators should modify access permissions on the vpnclient.ini file and remove write permissions for all users other than administrators. The same should also be done for executable files in the VPN client program folder. Also associated with each connection Profile is a created text file with the same name given to the defined connection. Parameters are held here and read by the VPN client. Access to these files should also be restricted to read only, for the typical end user. The preferred method, to prevent this exploit, would to update the VPN client to a non-vulnerable version. Cisco recommends updating the VPN client to version 4.0(1).

A Cisco announcement about the bug:

> "*Cisco has confirmed the issue and announced that a fix is under development. Cisco bug CSCeb12179 has been assigned to this issue. This BID will be updated when a fix becomes available.*"
> (Security Focus, bugtraq id 7665)

See the next variant below.

Variant #2:
http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb12179
(Requires Cisco Login)

Variant #2 Name:
Cisco Bugtraq give the following definition:

> Cisco CSCeb12179 Bug Details
> Headline: improve checking by GINA
> Product: universal-vpn-client
> Component: win-vpn-client
>
> Issue: GINA allows launching of any application named ipsecdialer.exe pretending to be the VPN Client ipsecdialer.
> (Cisco, bugid=CSCeb12179)

Variant #2 Operating System: The effected operating systems are as follows:

- Microsoft NT 4.0
- Microsoft Windows XP
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows 2000Advanced Server
- Microsoft Windows 2000 Datacenter Server

The above operating systems are effected regardless of Windows patch or hotfix levels.

Variant #2 Protocol / Service / Applications:
Variant #2 Protocol: No specific protocol is used for this exploit. However Windows Netlogon follows a set of rules. Netlogon verifies local authentication to the local SAM (System Account Manager) database for logging onto a Windows

PC. This exploit allows the application to determine what gets used for authentication credentials when executing commands, instead of the users.

Variant #2 Service: This exploit alters the GinaDLL, Graphical Identification and Authentication (GINA) dynamic-link library (DLL), registry settings in the system's registry.

Variant #2 Application:
Cisco VPN Client 4.0(1) for Windows

Variant #2 Brief Description: Security mechanisms in this version of the VPN client only allowed the launching of the executable ipsecdialer.exe. The exploit is to change the name of any executable to that of ipsecdialer.exe. No further checking was done other than name. This variant allowed a user to disguise any executable, of their choosing, to the name ipsecdialer.exe.

As a workaround, administrators should modify access permissions on all VPN client executables. Changing access to read only would be one method. The preferred method would to upgrade the client to 3.6(5)REL, 4.0(1)A or 4.0(2)REL and above.

Exploit Description: Users have the ability to escalate their own Windows user privilege level to that of local system administrator by "utilizing" a feature within the vulnerable Cisco's VPN client software. By the selection of a feature called, Enable start before logon, within the VPN client dialog box called, Windows Logon Properties, the normal Windows Logon process is interrupted. This process is interrupted when the end user specifies the VPN client to be started before logon. The VPN client calls a separate Windows Logon process that the VPN application uses. This application's Windows Logon process uses the rights and privileges of the local system administrator.

End users can also launch applications that are executed with local system administrative privileges. When selected, the option within the Windows Logon Properties dialog box called, Application Launcher, Third party dial-up application, allows the VPN application to launch executables. The launched application or program would be run with local system administrative privileges and access rights. This was primarily meant for starting a remote ISP dial-up connection. The launched executable could alter system variables or even start installing non-standard, non-approved corporate software.

What makes this exploit possible is the way the software vendor designed the VPN application. They were providing a convince/feature, for their customers to use, as stated above. Most typical VPN connections are made away from their normal environments/networks. User's, and their PC's, rely on services, systems and connections to their corporate network(s) to run efficiently. Typically PC's, upon bootup/logon make references to these services, mapped drives, for instance is one such service. But in order to use these services, the PC has to be connected to that network. When on the road, at home, or elsewhere other than the configured network, a PC starts up and has no initial access to these services. (One symptom of this are long boot up times. As these service connections need to time out before continuing on with the boot/login process.) My thinking, as well as the vulnerability discoverer, thought that the vendor was trying to be helpful. Hence the classification as a design error. Before the PC's Windows login service began, the VPN application would make a dial-up connection that would connect the remote PC to the network. Thus when the user logged onto the PC, the services would be available to the PC and user upon startup.

By using these VPN client launch features end users can circumvent their designated users privileges assigned to them by their Windows Network Logon ID. Any Windows system that would have the vulnerable VPN client software installed, and the end user had logon access too, would be vulnerable. This could be their own desktop/laptop PC, a shared PC, a corporate walk-up PC, a server or a fellow employee's computer.

This attack is a local system attack. (Note: It is not necessary to be connected to a network in order to exploit this vulnerability.) A user, at their leisure and privacy, could execute the exploit on a local machine, particularly if the computer was a laptop. The end user could work in privacy away from work. Once the laptop was exploited they could quietly reconnect the PC to the network.

Service Description: The service that the exploitable VPN client takes advantage of is a part of the Windows boot process. Part of the Windows boot process (described in more detail below) is the execution of Smss.exe. A function of Smss.exe is to call the Win32 subsystem Winlogin.exe executable. This executable reads data from the current system registry. By using the VPN client options, or by directly modifying the files the registry setting refers too, the VPN application executes normally as defined by Cisco, albeit at the expense of surpassing the operating system security rights the end user has.

How the Exploit works: In order to understand this exploit one must look at how the operating system, in this case a Windows 32 bit system, starts upon boot up. A Windows 32 bit operating system goes through 6 major levels on boot up:

1.) POST – Power on Self Test
2.) Operating System Loader
3.) Kernel Load
4.) Kernel Initialization
5.) Services Load
6.) Logon

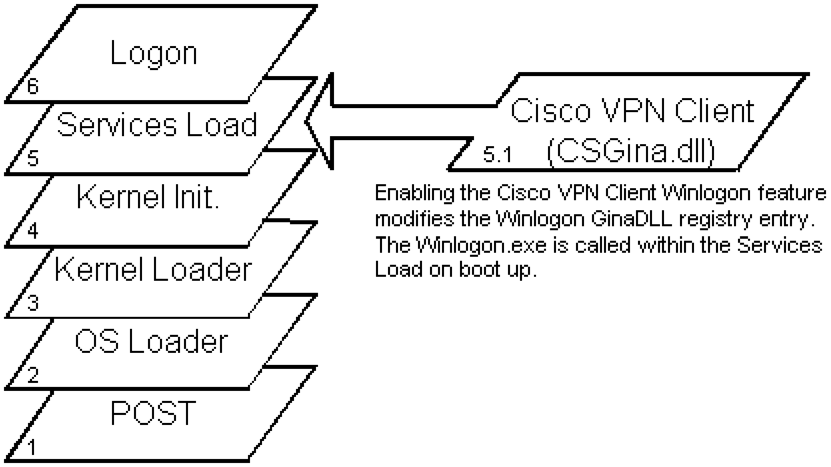

Logon
6
Services Load
5
Kernel Init.
4
Kernel Loader
3
OS Loader
2
POST
1
Cisco VPN Client
5.1
(CSGina.dll)
Enabling the Cisco VPN Client Winlogon feature modifies the Winlogon GinaDLL registry entry. The Winlogon.exe is called within the Services Load on boot up.

Image #1: Diagram of Windows boot in relation to the Cisco VPN Client Winlogon feature.

1: POST - Power on Self Test: After power is applied to the system the hardware performs self tests and verifies the existence of necessary hardware components (keyboard, mouse, SCSI cards, etc.). These devices in turn may also perform POST tests on themselves.

2: Operating System Loader: Starts the file system and starts to read files from the disk. (Note: you can press the F8 key here to load the LastKnownGood control set if the system is not booting properly.)

3: Kernel Loader: Continues to load all the appropriate files into memory.

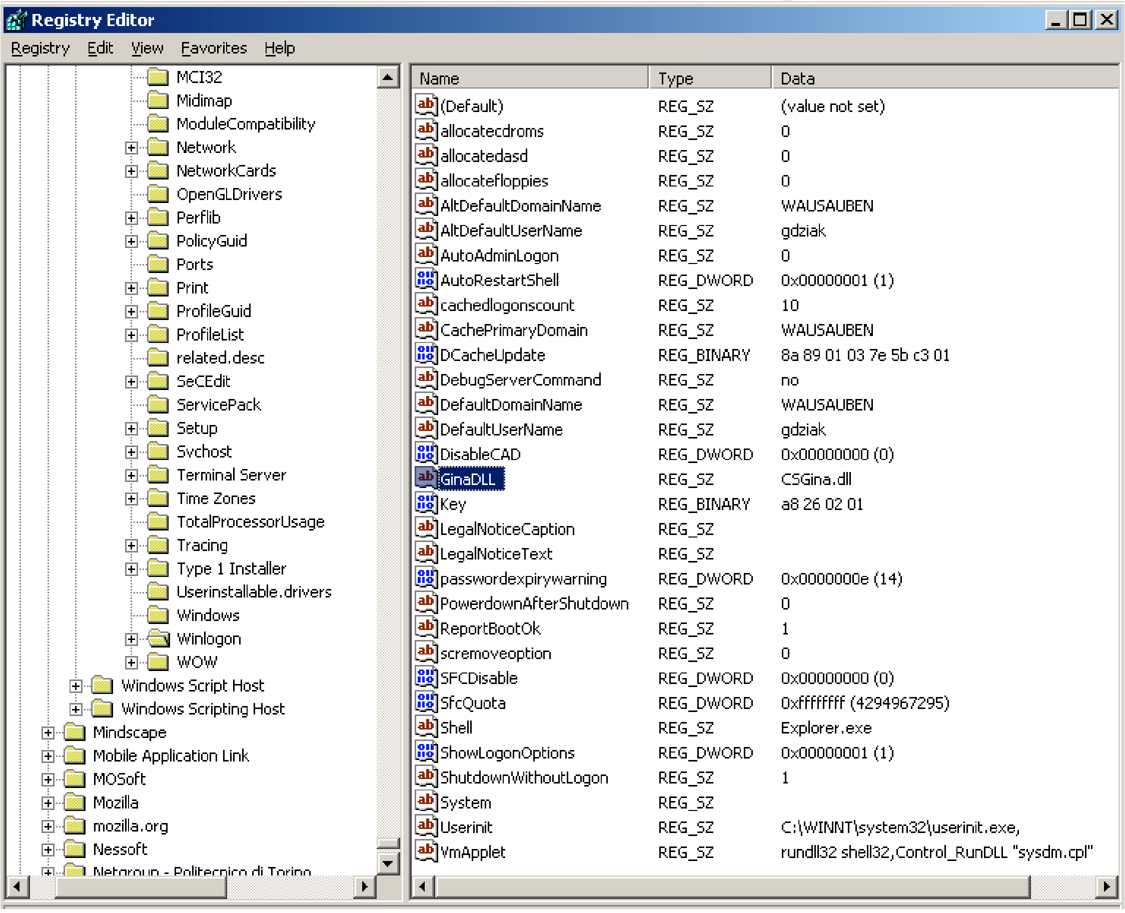
4: Kernel Initialization: Creates registry entries for the previously recognized hardware and loads device drivers read from the system registry. These services have a Windows registry value of 0x1. This process creates a Clone control set, by coping the current control set, and creates the Hardware registry key.

5: Services Load: The session manager, smss.exe, is started and begins to load all applications specified in the BootExecute Registry Entry. It also loads any required subsystems. One of these subsystems is the Winlogon.exe, which starts the Local Security Administration, lsass.exe executable that loads the Ctrl-Alt-Delete Logon Dialog Box. Next the Service Controller, screg.exe, reads the current system registry and starts services with the value of 0x2. (Note services with a value of 0x3 have to be started manually and services with a value of 0x4 are disabled.)

6: Logon: After a successful login the Clone control set, from the Kernel Initialization step, is copied and saved as the LastKnownGood control set.

Before the above six steps can start various required files are needed before a Windows machine can start. These files must be present and not corrupted or modified. They are also required to be in predefined system directories.

For this exploit we will examine the Services Load process and how Cisco's VPN client affects the Win32 subsystem Winlogon.exe process.
If the user selects the option, Enable start before logon, (see Image #8, page 18), the VPN client software changes a registry setting under the Winlogon registry setting. It replaces the registry setting, GinaDLL, Graphical Identification and Authentication (GINA) dynamic-link library (DLL), with the VPN client dll, CSGina.dll. The previous, and default, Windows operating system file was MSGina.dll.



MCI32
Midimap
ModuleCompatibility
Network
NetworkCards
OpenGLDrivers
Perflib
PolicyGuid
Ports
Print
ProfileGuid
ProfileList
related.desc
SeCEdit
ServicePack
Setup
Svchost
Terminal Server
Time Zones
TotalProcessorUsage
Tracing
Type 1 Installer
Userinstallable.drivers
Windows
Winlogon
WOW
Windows Script Host
Windows Scripting Host
Mindscape
Mobile Application Link
MOSoft
Mozilla
mozilla.org
Nessoft
Netgroup - Politecnico di Torino

Name	Type	Data
(Default)	REG_SZ	(value not set)
allocatecdroms	REG_SZ	0
allocatedasd	REG_SZ	0
allocatefloppies	REG_SZ	0
AltDefaultDomainName	REG_SZ	WAUSAUBEN
AltDefaultUserName	REG_SZ	gdziak
AutoAdminLogon	REG_SZ	0
AutoRestartShell	REG_DWORD	0x00000001 (1)
cachedlogonscount	REG_SZ	10
CachePrimaryDomain	REG_SZ	WAUSAUBEN
DCacheUpdate	REG_BINARY	8a 89 01 03 7e 5b c3 01
DebugServerCommand	REG_SZ	no
DefaultDomainName	REG_SZ	WAUSAUBEN
DefaultUserName	REG_SZ	gdziak
DisableCAD	REG_DWORD	0x00000000 (0)
GinaDLL	REG_SZ	CSGina.dll
Key	REG_BINARY	a8 26 02 01
LegalNoticeCaption	REG_SZ	
LegalNoticeText	REG_SZ	
passwordexpirywarning	REG_DWORD	0x0000000e (14)
PowerdownAfterShutdown	REG_SZ	0
ReportBootOk	REG_SZ	1
scremoveoption	REG_SZ	0
SFCDisable	REG_DWORD	0x00000000 (0)
SfcQuota	REG_DWORD	0xffffffff (4294967295)
Shell	REG_SZ	Explorer.exe
ShowLogonOptions	REG_DWORD	0x00000001 (1)
ShutdownWithoutLogon	REG_SZ	1
System	REG_SZ	
Userinit	REG_SZ	C:\WINNT\system32\userinit.exe,
VmApplet	REG_SZ	rundll32 shell32,Control_RunDLL "sysdm.cpl"

Image #2: Winlogon registry setting showing the GinaDLL modification.

A reboot is necessary for the operating system to re-read the registry for the change to take affect. After the reboot the boot process now calls the new GinaDLL registry entry. This new dll, CSGina.dll, executes its configuration. This is where an alternate Windows Logon process is started, when the user activates the VPN application, because of the selection, Enable start before logon (Image

#6). The alternate Windows Logon process uses the local system administrator to logon onto the system and uses the administrator rights to start the VPN client. Once that process is done the CSGina.dll hands off execution to the original GinaDLL, MSGina.dll. MSGina.dll operates and allows Windows to bring up the normal Ctrl-Alt-Del Windows logon box.

The variant exploit starts with the user selecting the option, Application Launcher, in the VPN client. The user then enters what executable they wish to have executed with local system administrator privileges.

Signature of the Attack: When a user selects the Winlogon and Application Launch options two files are changed. (Note users could also modify these files by "hand" since they are not locked to standard users by default.) The vpnclient.ini file and associated Profile files responsible for holding these settings are, by default, installed to a non-restricted access path. The default install path for the vpnclient.ini file is C:\Program Files\Cisco Systems\VPN Client\ and the default install path for the Profile is C:\Program Files\Cisco Systems\VPN Client\Profiles.

Shown below is what is modified in the vpnclient.ini file.

< vpnclient.ini file snippet >

```
[ApplicationLauncher]
Enable=1
Command=C:\WINNT\system32\explorer.exe
```

The setting, **Enable=1**, enables the application launch ability. A setting of **0** would disable the application launch ability. The **Command** setting tells what application or program the VPN client should launch upon startup. Default settings for these parameters are **Enable=0** and **Command=** (i.e. launch nothing)

A Profile file is created when you first configure the VPN client. The name a user gives for the Connection Entry creates an exact named text file for recording connections parameters. (See Image #7, page 18, for example. In that Image you see the Connection Entry, GCIH Practical. A Profile text file is created with the same name, GCIH Practical.txt.)

Shown below is what is modified in the GCIH Practical.txt file.

< CGIH Practical.txt file snippet >

```
EnableISPConnect=1
ISPConnectType=1
ISPConnect=Dial-up Connection
ISPCommand=explorer.exe
```

A setting of **EnableISPConnect=0** and **ISPConnectType=0** would disable third party dial-up.

Since these files are changed a host IDS application would be able to pick this modification up and alert an administrator. Even, as stated in covering their tracks, the user tried to change these settings back to the way they were. The file time stamps would be different from what would be recorded in the host IDS database.

Note: As mention in How the Exploit Works, the registry setting, HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows NT/Current Version/Winlogon/GinaDLL is changed when VPN application options are selected. If there are no company reasons to have these options used by the VPN client, this could be used as a signature for the exploit.

There are no other changes, for this exploit, to the system that create a signature. Of course changes to the system after the exploit can and do leave their own signatures.

The Platforms/Environments:

Victim's Platform: The targeted platform is the own users laptop. The initial exploit was conducted off the network and then re-attached to the corporate network. The exploit needs two pieces in order to work, the Windows operating system itself, and a vulnerable version of the VPN client. Once the laptop was exploited the user installed the Windows version of Nmap and the associated WinPcap files. Although these "tools" were not necessary for the exploit, they were the reason for discovering the privilege escalation exploit.

Operating system: Windows 2000 Professional with Service Pack 4 and all the latest Microsoft hot fixes and Patches installed for the operating system. (As of the date of this practical.) (Note: Internet Explorer 6.0 is also installed on the system. It too has all the latest released hot fixes and patches installed.) Norton AntiVirus Corporate Edition –Scan Engine 4.1.0.15 with the latest virus definition files installed (At the time of the exploit.)

Microsoft Office Suite 2000

Cisco Systems VPN Client: Version 3.5.2

Windows Nmap: Version 3.48

Nmap, Network Mapper, is an open source licensed tool for scanning networks for discovery and security auditing.

WinPcap Version 3.01

WinPcap is described as a Windows device driver that adds the ability to capture and send packets from a network card. Nmap requires these files for operation.

Source Network: Since this exploit is a local exploit, the source network could be defined as the PC itself. However once the exploit was conducted, the exploited laptop was reconnected back into the target network and began using services of the targeted network.

Target Network: The corporate network, and it services, contained the following:

The exploited laptop - As described in the previous section.

Server 1 & 2 – Windows 2000 Server. Service Pack 4 is installed with all the latest released patches and hot fixes for the operating system and Internet Explorer. Norton AntiVirus Corporate Edition –Scan Engine 4.1.0.15 with the latest virus definition files installed (At the time of the exploit.) These servers handled file, print, DHCP, DNS and IIS (Intranet) services for the target network. Other unused services have been disabled or turned off, although no specific security tools have been run against these servers to verify if all services have been identified.

Computers 1 & 2 – Fellow employee's Windows 2000 Professional PC's, Windows & network login restricts user access to the Windows system environment, the Windows registry settings and prevents modification of Windows Operating System files. Users were also unable to install software. Service Pack 4 is installed with all the latest released patches and hot fixes for the operating system and Internet Explorer. Norton AntiVirus Corporate Edition – Scan Engine 4.1.0.15 with the latest virus definition files installed (At the time of the exploit.). Microsoft Office Suite 2000

Network Monitoring Server – Linux, RedHat 8.0. Running Nagios, Snort 2.0, and IPTraf. Access is restricted by SSH and limited logon accounts to approved personal. VNC, version 3.3.3, is also enabled for remote administration of the server and tools.

Switches – Cisco 2924, Layer 2 switch, IOS version 12.0. Limited device access by SSH, by only selected individuals.

Router – Cisco 2610, IOS version 12.2. Limited access by SSH by only selected individuals. An access list on the firewall permits only a predefined list of internal IP address to have SSH access to the device.

Firewall – Cisco Pix: Access lists: Inside to Outside; All inside initiated traffic is allowed out. Outside to Inside; Only ports required are permitted to DMZ servers. (80-http, 443-https, 20/21-FTP). There is no direct access from the Outside (Internet) to the Inside Corporate infrastructure. Limited device access by SSH by only selected individuals

Network Diagram:

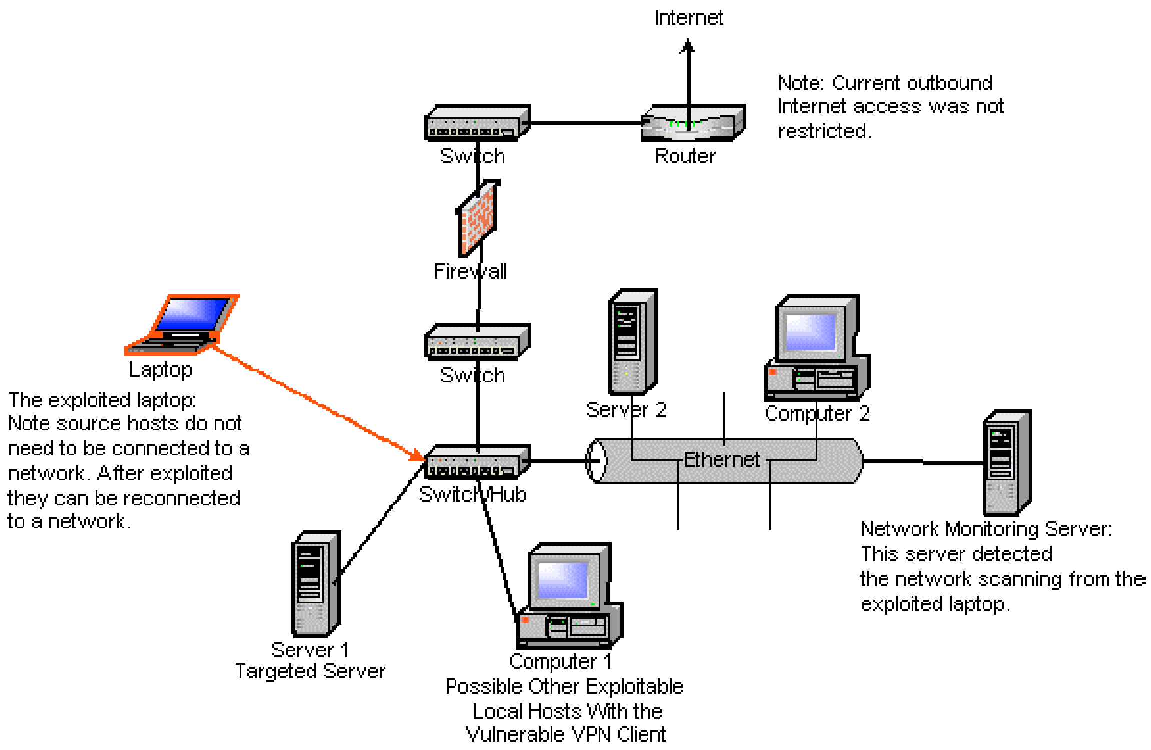

Internet
Note: Current outbound Internet access was not restricted.
Switch
Router
Firewall
Laptop
The exploited laptop: Note source hosts do not need to be connected to a network. After exploited they can be reconnected to a network.
Switch
Server 2
Computer 2
Switch/Hub
Ethernet
Network Monitoring Server: This server detected the network scanning from the exploited laptop.
Server 1
Targeted Server
Computer 1
Possible Other Exploitable Local Hosts With the Vulnerable VPN Client

Image #3: Network Diagram

Stages of the Attack:

Reconnaissance:

Initial reconnaissance was by happenstance. While debugging an unrelated Windows error I happened to run across this link, http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0305&L=ntbugtraq&F=P&S=&P=4117. (Staff, Nick: Reference #3, page 49) This posting had an exploit that pertained to a piece of software already loaded on my laptop. By following the steps, as described in the posting, and as I detailed below in, Exploiting the System, I was able to get local system administrator privileges.

The VPN client software was already apart of the standard corporate desktop "images" of approved applications. These images are created for users or a subset of defined users or groups. In our environment, and as in this "test" environment, the laptop "software image" included a vulnerable version of VPN client.

Other reconnaissance would be necessary if the user was not part of a group or did not have the VPN software. Such reconnaissance can begin with a quite walk around the company. This walk is to locate and examine machines that may become potential targets. While taking the "survey" they would note the target host location, in relation to other people, and be aware when access to the target host is used and not used. Inside knowledge is helpful in zeroing in on machines that are likely to be vulnerable. In this case knowing that laptops carry VPN software, and assessing that VPN software is normally installed on systems that are designed to be easily removable from the network, i.e. laptops, would help narrow down the search. Another option while doing their reconnaissance would be noting how fellow employees leave their laptop/desktop systems when they are unattended and away from them. Perfect times would be at lunch hour and after normal work hours. Depending on one's role within the corporation this may seem as "normal" job activity for the user to be doing.

*Note: Corporate Desktop images: A common practice with corporations is to have several standard desktop configurations. These configurations have a list of corporate approve software to be installed on machines. These "saved" desktop images reduce the amount of time necessary to bring PC's into production.

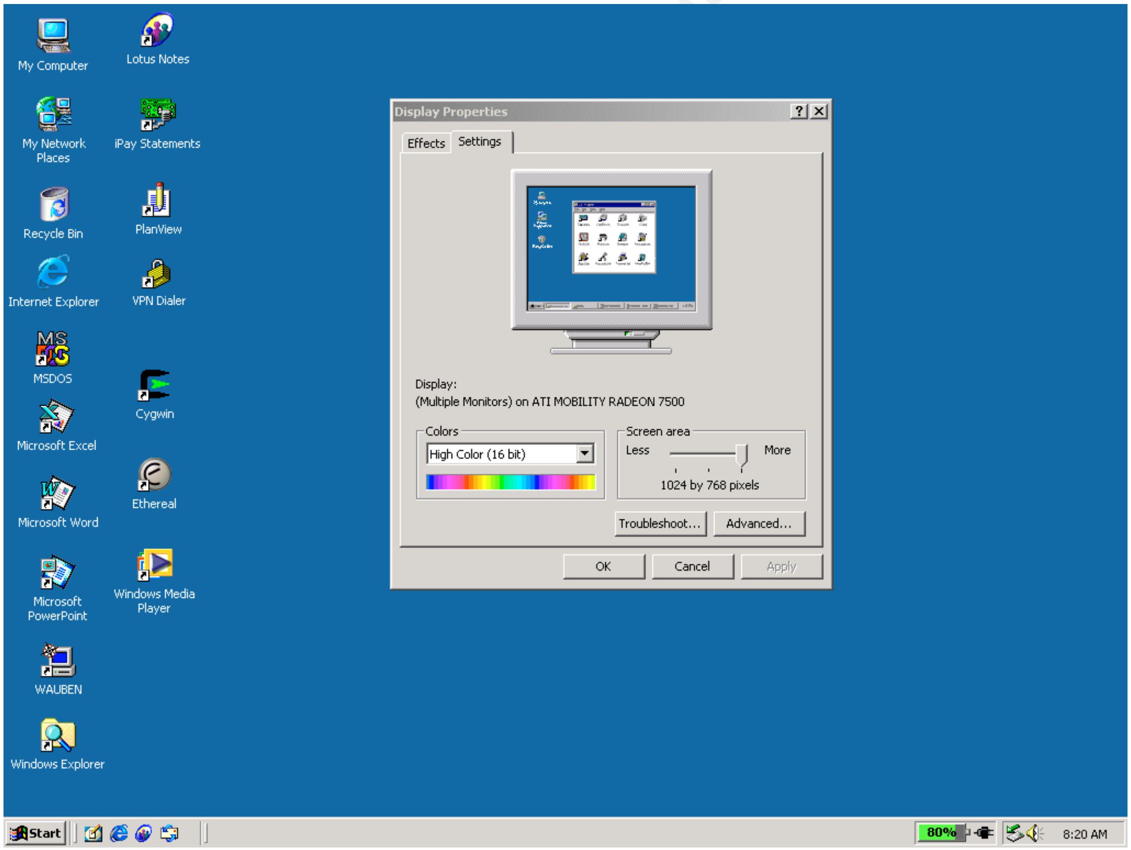
Another reconnaissance point that the end users can take advantage of is what is available on the corporate Intranet. In some instances a listing of approved software is defined. This gives an easy reference list to search the Internet, and other sources, for known vulnerabilities. In this case the end user could verify if the vulnerable VPN client is listed for corporate approved software. (A listing of specific corporate approved software, that is made generally available, would not be recommended due to this type of tactic.)

Scanning: The previous reconnaissance, i.e. eyes, ears and feet, have located a desired target. In this case it was the users own laptop. If the targeted PC happened not to be their laptop and was some other system, the next step would be determining their login access, operating system version and VPN client version on the targeted host. What type of logon process presented to the user can help determine the operating system. This exploit requires the operating system to be Windows 2000. One way to determine the operating system is by looking at the login process presented to the user, on Windows it's the Ctrl-Alt-Delete dialog box. Another process for identifying the Operating Systems would be examining what Windows Networking displays. By opening up Windows explorer, on the laptop, and selecting Microsoft Windows Network, under My Network Places the user then selects their corporate domain. After that selection a listing of systems are shown participating in the domain. By right clicking on a selected system, and selecting the properties option, you can see what type of operating system is participating in the Windows domain.

Once a target is located, and verified, a more adept hacker would try to determine what type of monitoring is being done to the selected host. Possible techniques would be telneting to the machine to determine if and how logs, to that host, are being monitored. (Of course this would be done from another machine that would not be directly associated with him or her.) A more drastic example may to "accidentally" pull the network connection to the targeted host and see how soon the machine is discovered off the network.

<u>Exploiting the System:</u>

The below diagram shows what a typical "restricted" user has access too, based off of their security policies rights from their Windows network logon ID. Once they have discovered a machine with the vulnerable VPN client they can begin exploiting it. In this instance it is their laptop.



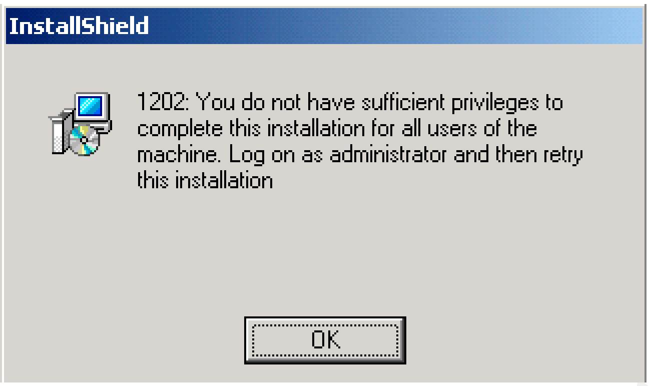
Display:
(Multiple Monitors) on ATI MOBILITY RADEON 7500

Colors: High Color (16 bit)

Screen area: 1024 by 768 pixels

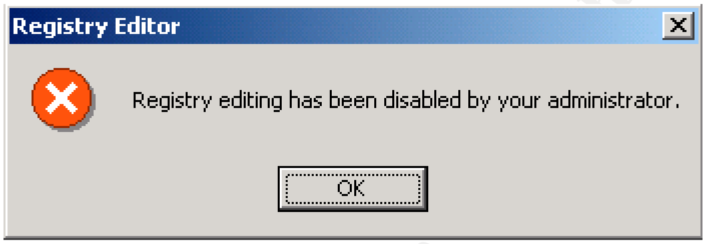
<u>Image #4: Demonstration of users desktop privileges before exploit</u>

As shown in the above picture (Image #4) access to alter their desktop settings is not available. (The above dialog box is gotten by right clicking on the desktop and selecting Properties.) The user is also not able to install software onto the device. Current access to the Internet is not restricted from our corporate network. If I go out, to the Internet, and download a program, for instance Nmap, and try to install the application, due to my current system privileges, the PC would deny the install due to my Windows/PC account ID privileges. I could download all I want but would not be able to do anything with those downloads. Access to the system registry is also restricted. If I hit the Start button, on the Windows task bar and select the Run option and type the command regedit, execution is denied. The following screen captures illustrates these attempts:


InstallShield

1202: You do not have sufficient privileges to complete this installation for all users of the machine. Log on as administrator and then retry this installation

Image #5: Insufficent install privileges

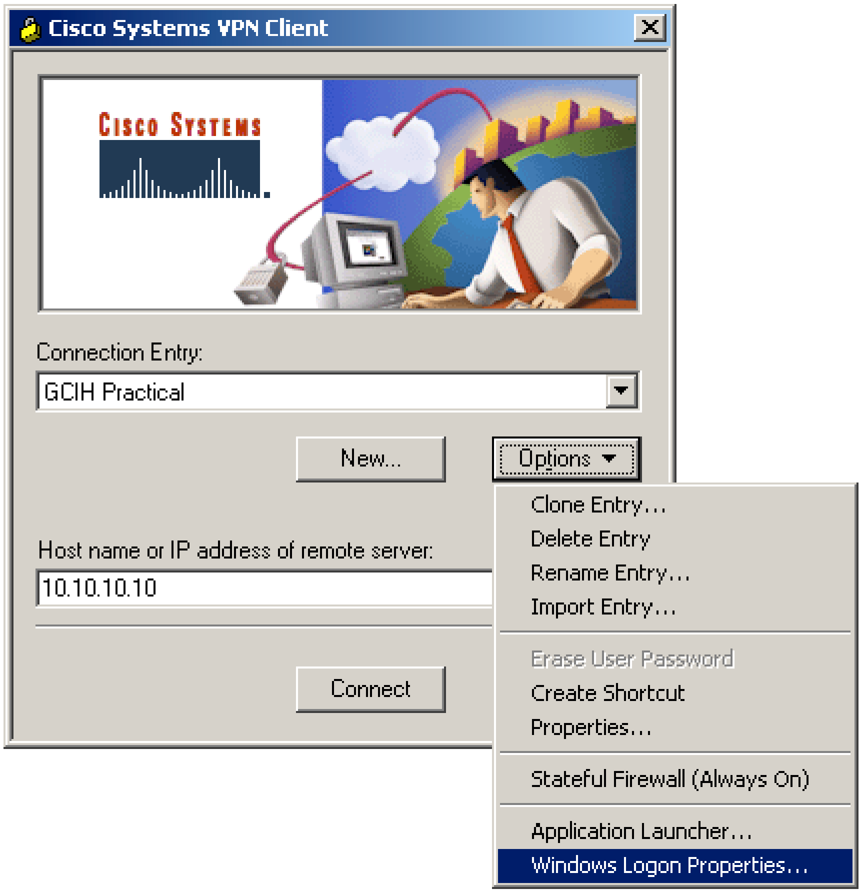

Registry Editor

Registry editing has been disabled by your administrator.

Image #6: Disabled registry editing

*Note: Usually the Windows Registry is locked down preventing installation of software. However most software that does not modify the registry can be installed when this method is used to prevent software installs.

To alter my security rights, and begin the exploit, on the laptop I would now enable the Application Window Logon features of the vulnerable Cisco VPN client. (Image #7 and Image #8, page 18 below)

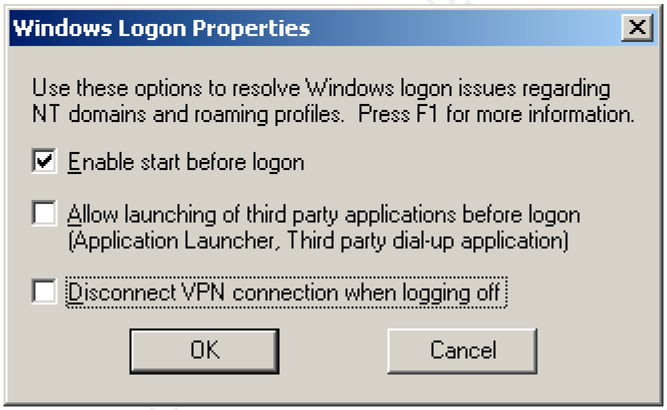


Cisco Systems VPN Client

Connection Entry: GCIH Practical

Host name or IP address of remote server: 10.10.10.10

Image #7: Vulnerable Cisco VPN Client Options



Windows Logon Properties

Use these options to resolve Windows logon issues regarding NT domains and roaming profiles. Press F1 for more information.

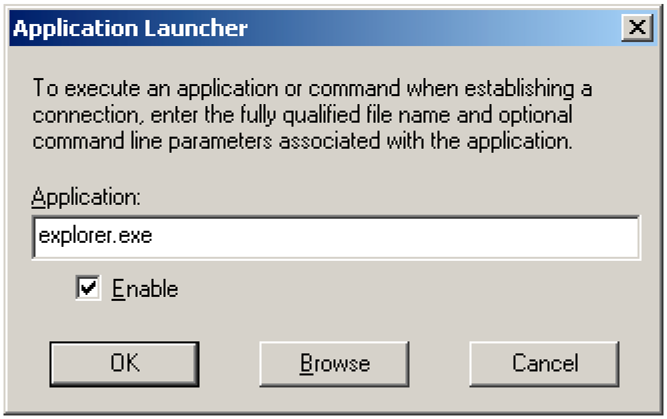
☑ Enable start before logon

□ Allow launching of third party applications before logon (Application Launcher, Third party dial-up application)

□ Disconnect VPN connection when logging off

Image #8: Vulnerable Cisco VPN client Windows Logon Properties dialog box

Select the Enable start before logon option and enter an application to be launched.



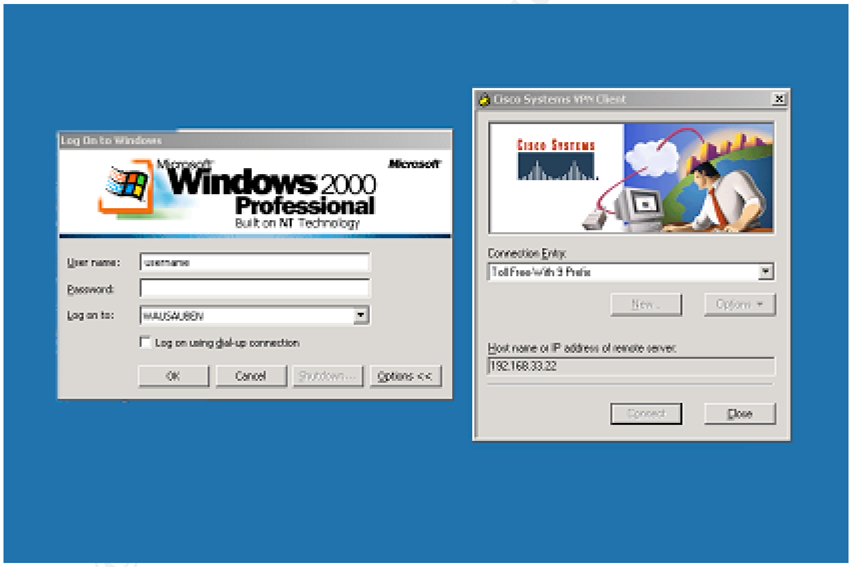
To execute an application or command when establishing a connection, enter the fully qualified file name and optional command line parameters associated with the application.

Application: explorer.exe

☑ Enable

Image #9: Vulnerable Cisco VPN client Application Launcher dialog box

The above diagram (Image #9) shows the launching of explorer.exe. Any executable entered here for launching will exhibit the same behavior as the demonstrated explorer.exe does. After those features are turned on, a checkmark is shown after selecting. A reboot is now necessary to take advantage of either of those modifications. After the reboot procedure the system now reacts quite differently on how it starts up. The following screen capture illustrates this.



User name: username

Password:

Log on to: WAUSAUBEN

☐ Log on using dial-up connection

Connection Entry: Toll Free-With 9 Prefix

Host name or IP address of remote server: 192.168.33.22

Image #10: Windows Logon dialog box after exploit.

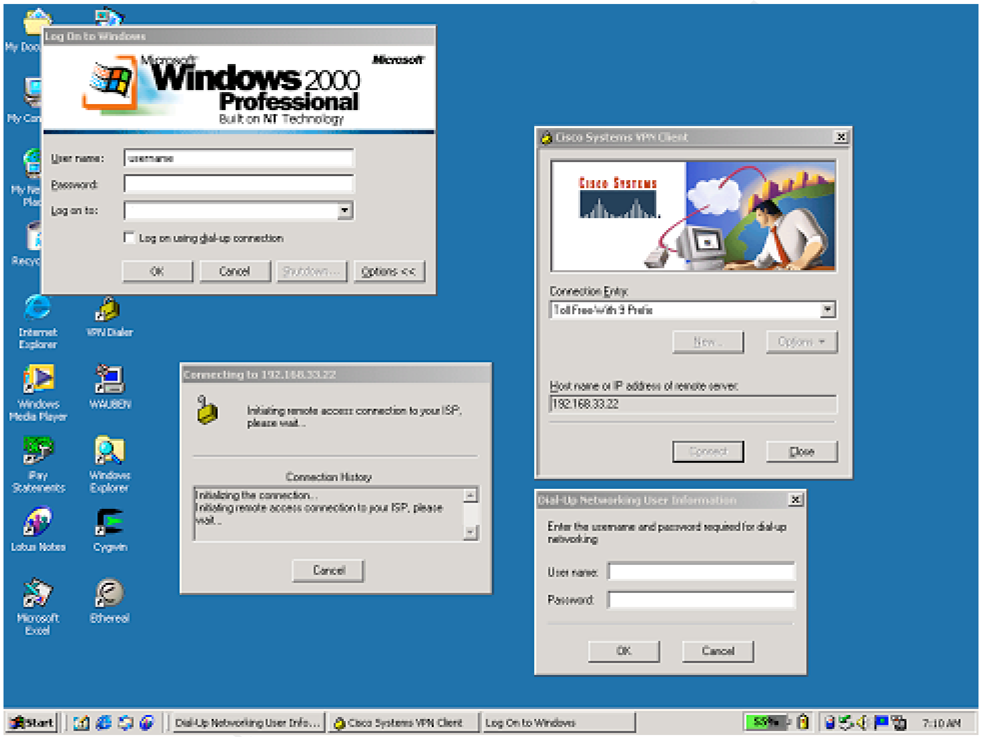
*Note: The reboot is necessary because registry changes are being made. The PC must be rebooted to read those affected changes as explained in the section, How the Exploit works.

Not only is the user prompted for Windows logon but the Cisco VPN client is also displayed. This is because of our settings we enabled in the VPN client in the previous steps.

The next step is to “establish” a VPN connection.

*Note this exploit does not require an actual connection to a VPN end device. Just the activation of the VPN client is enough for the exploit to work. This execution of the VPN client, which in turn launches the executable explorer.exe, starts the alternate Windows Logon process. The first Windows Logon process is still there, I just choose to not activate that process.

The user now ignores the Ctrl-Alt-Del Windows logon dialog box and hits the Connect button on the VPN client displayed. As described previously, in How the Exploit Works, the VPN software client executes explorer.exe with local system administration rights. This is what is presented to the user after activation:



Log On to Windows

User name: username

Password:

Log on to:

□ Log on using dial-up connection

Connecting to 192.168.33.22

Initiating remote access connection to your ISP, please wait...

Connection History

Initializing the connection...
Initiating remote access connection to your ISP, please wait...

Cisco Systems VPN Client

Connection Entry: Toll Free With 9 Prefix

Host name or IP address of remote server: 192.168.33.22

Dial-Up Networking User Information

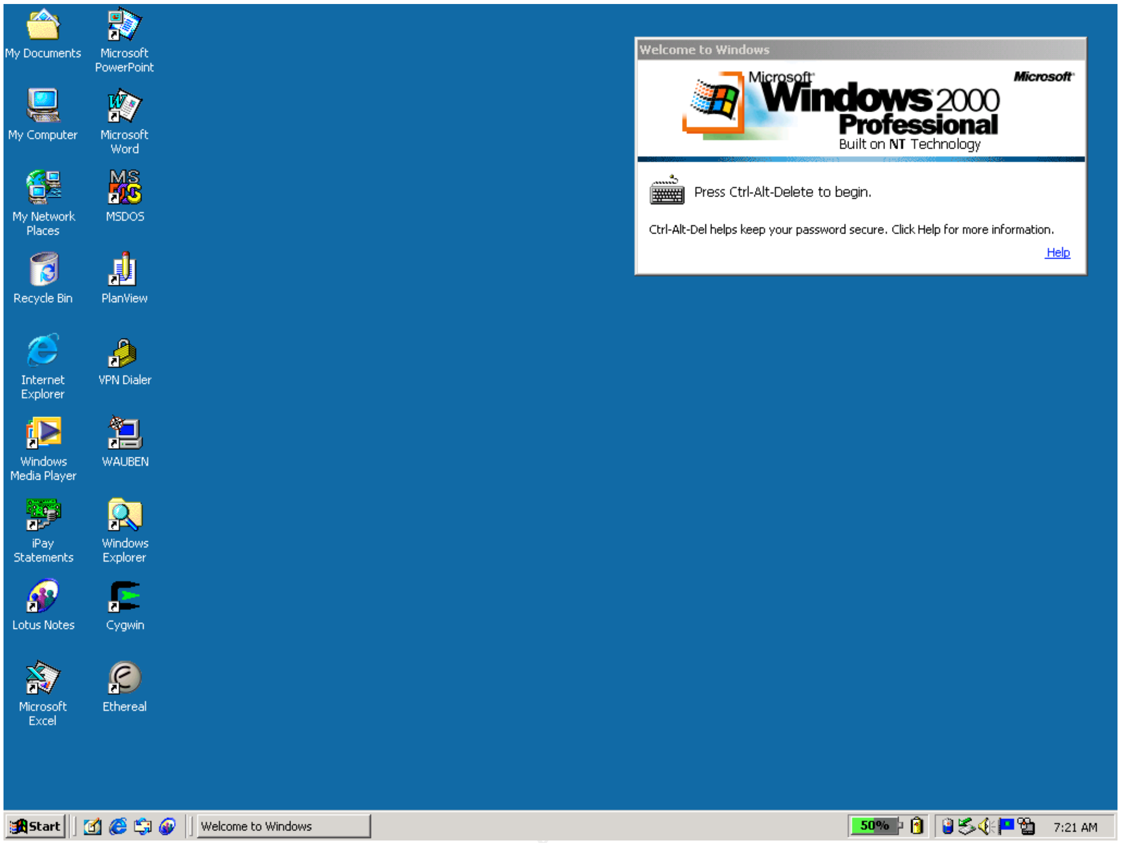
Enter the username and password required for dial-up networking

User name:

Password:

Image #11: Desktop after initating exploit.

Notice that no username or password is used, or given, in either the VPN application or Windows logon process, or a VPN connection established. Now the user just needs to close the various VPN client windows. A requirement for the Cisco VPN client is to have a host name or IP address to connect too. However this IP address or host name can be bogus. No real end device is needed at the configured Remote Server Dialog Box Location. After closing the various VPN dialog boxes the user is left with this: (Image #12, page 21)



Press Ctrl-Alt-Delete to begin.

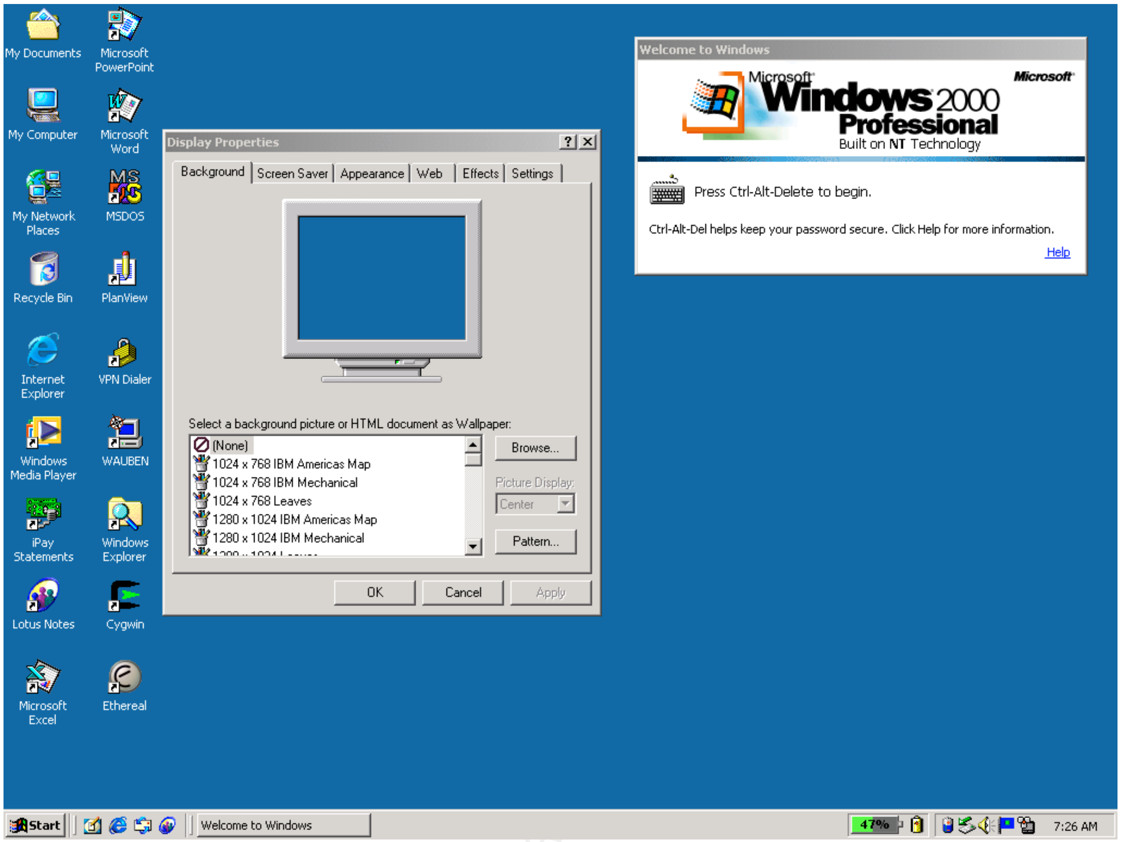
Ctrl-Alt-Del helps keep your password secure. Click Help for more information.

Image #12: Cleared desktop with unused Windows Logon dialog box.

The end user is now logged in as a local system administrator. In the upper right corner you see the first Windows login the end user was presented. That process did not get executed. Instead the activation of the Cisco VPN client executed a separate Windows log in process, which in turn logged in as the local system administrator.

Note: If the end user were to execute the remaining login window, by hitting Ctrl-Alt-Del, it would log out the system administrator and use the credentials the end user imputed for login.

The user now has full local system access rights. This can be demonstrated by comparing to the previous diagram of Properties of the Desktop to this, Properties of the Desktop. (Image #13, page 22)



Select a background picture or HTML document as Wallpaper:

(None)
1024 x 768 IBM Americas Map
1024 x 768 IBM Mechanical
1024 x 768 Leaves
1280 x 1024 IBM Americas Map
1280 x 1024 IBM Mechanical
1280 x 1024 Leaves

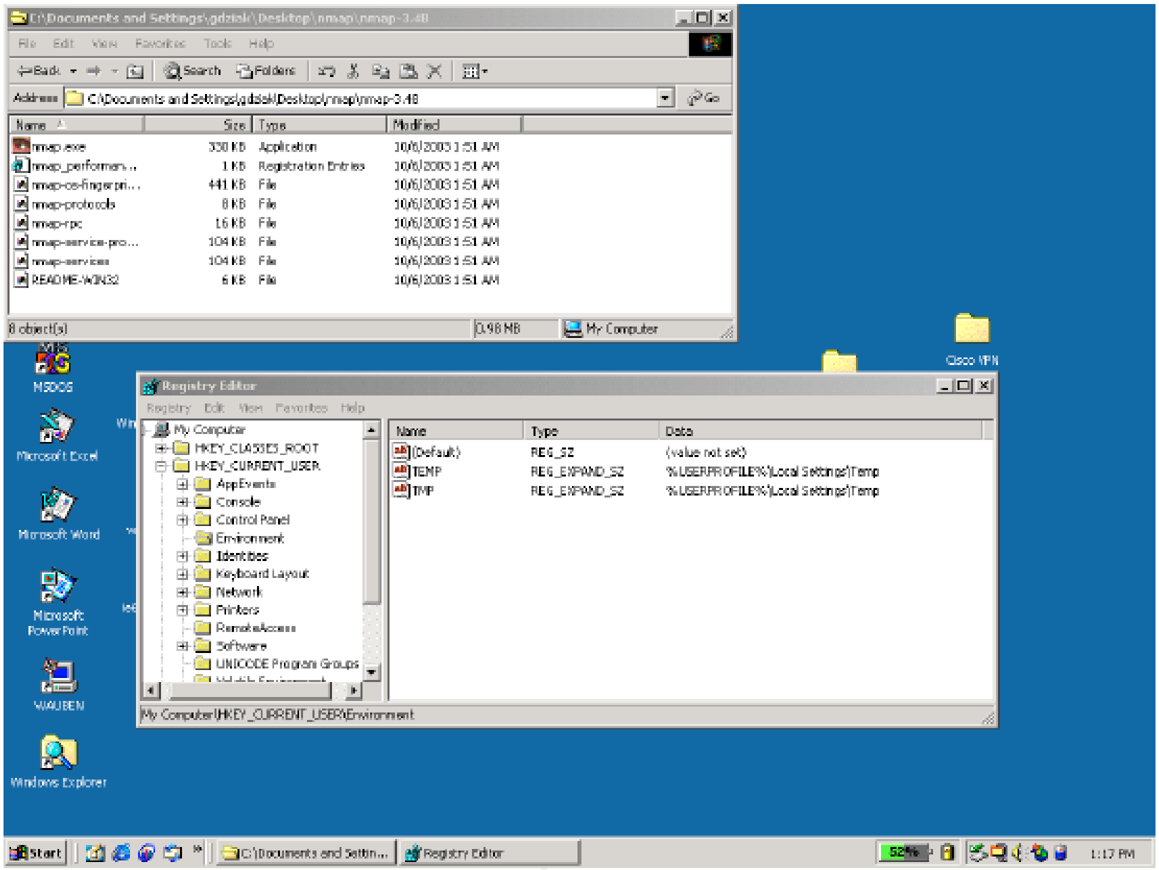
Press Ctrl-Alt-Delete to begin.

Ctrl-Alt-Del helps keep your password secure. Click Help for more information.

Image #13: Demonstration of users desktop privileges after exploit.

The user now has access to resources they didn't have before, as shown in the above picture. In this case the user now had the ability to install any type of software they choose. Now what to do with this new power? I know, install Nmap and see what else in running on the network. Off too http://winpcap.polito.it to get the WinPcap files; WinPcap_3_0.exe and then too http://www.insecure.org/nmap for the latest version of Nmap; nmap-3.48-win32.zip.

Here is another screen capture demonstrating these new powers and abilities the user did not have, until they exploited the vulnerability in the VPN client. Shown is the installation of Nmap and having the ability to run the Windows registry editor. (Image #14, page 23)



C:\Documents and Settings\gdzialx\Desktop\nmap\nmap-3.48

Address C:\Documents and Settings\gdzialx\Desktop\nmap\nmap-3.48

Name	Size	Type	Modified
nmap.exe	330 KB	Application	10/6/2003 1:51 AM
nmap_performan...	1 KB	Registration Entries	10/6/2003 1:51 AM
nmap-os-fingerpri...	441 KB	File	10/6/2003 1:51 AM
nmap-protocols	8 KB	File	10/6/2003 1:51 AM
nmap-rpc	16 KB	File	10/6/2003 1:51 AM
nmap-service-pro...	104 KB	File	10/6/2003 1:51 AM
nmap-services	104 KB	File	10/6/2003 1:51 AM
README-WIN32	6 KB	File	10/6/2003 1:51 AM

8 object(s) 0.98 MB My Computer

Registry Editor

Name	Type	Data
(Default)	REG_SZ	(value not set)
TEMP	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\Temp
TMP	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\Temp

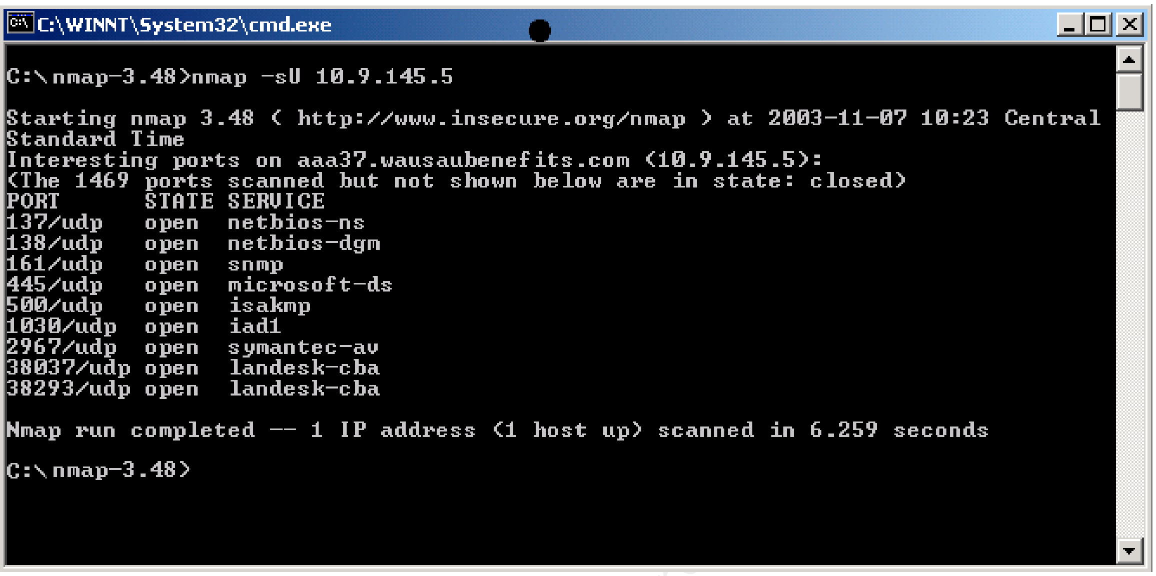
My Computer\HKEY_CURRENT_USER\Environment

Image #14: New powers

The actual exploit ends here. Users inevitably have some reasons for pursuing such exploits, hence if the user just stopped here, and not use their new abilities, there would not be much purpose in pursuing the exploit to begin with. Unless of course you are a "White hat" and want to inform and provide education to the Security community.

Up until now detection was not possible. The exploited laptop was not connected to the corporate network. However once the laptop was reconnected to the corporate network detection would be possible if certain methods are employed. Direct detection of the exploit can only happen after a reconnection to the network.

Let's see what I can glen off of the network…For reference here are the commands for conducting a Nmap scan. The command syntax is: nmap –*flags* "*target ip address".* In the example given below,
Nmap –sU 10.9.145.5, the flag values of –sU are used to conduct a UDP (User Datagram Protocol) port scan.

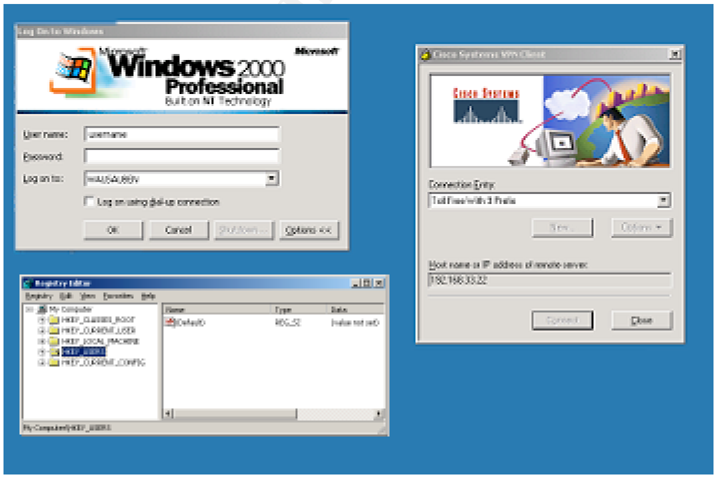


```
C:\nmap-3.48>nmap -sU 10.9.145.5

Starting nmap 3.48 ( http://www.insecure.org/nmap ) at 2003-11-07 10:23 Central
Standard Time
Interesting ports on aaa37.wausaubenefits.com (10.9.145.5):
(The 1469 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
137/udp   open  netbios-ns
138/udp   open  netbios-dgm
161/udp   open  snmp
445/udp   open  microsoft-ds
500/udp   open  isakmp
1030/udp  open  iad1
2967/udp  open  symantec-av
38037/udp open  landesk-cba
38293/udp open  landesk-cba

Nmap run completed -- 1 IP address (1 host up) scanned in 6.259 seconds

C:\nmap-3.48>
```

Image #15: Nmap usage.

Variant Option Exploit:

With the option Application Launcher, (Image #8, page 18) Third party dial-up application, selected, and the option Enable start before logon selected, (You would have to enable both of these options), the user is presented with the same Windows startup screen as seen in Image #10, page 19. The Windows Logon dialog box after exploit and the VPN client, but the application runs differently when the user hits connect. The VPN client starts the preset command the user previously entered in the VPN client. In this example the user placed the command regedit.exe. The user now has the ability, that they did not have before, to change registry settings.



User name: username

Password:

Log on to: WAUSAUBEN

☐ Log on using dial-up connection

Connection Entry: Toll Free with 3 Prefix

Host name or IP address of remote server: 192.168.33.22

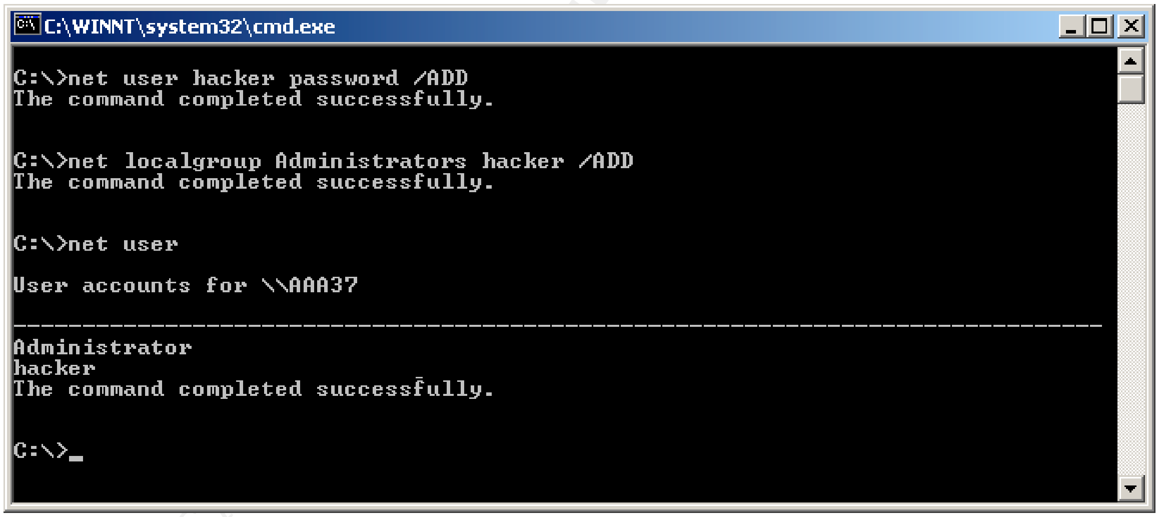
Image #16: Variant Exploit Startup Screen.

Any executable entered in the dialog box (Image #9, page 19) would be run with local system administrator privileges.

Keeping Access:

Once they have system administrator rights they can pursue any other "black hat" activities. They now have the ability to install sniffers, key loggers, scanners, games, etc… They now can achieve elevated privileges any time they activate the VPN client features and simply reboot. Once common practice is to create alternate logins, with local administrative rights, that look like legitimate logins. A user would create false names that match corporate standards. For example, first initial and last name, jsmith, of a bogus person. Administrators could have a hard time picking out these false login names, as compared to false names like l33t_haxz0r. Once created they can log onto the targeted host with anonymity. Once the privilege escalation is accomplished the commands to create these alternate log in are as follows.

At the DOS command prompt of the Windows machine the syntax of the command is this: C:\ **net user "*username*" "*password*" /ADD**. Once the user is created the next step would be to add that username to the PC's local administrators group by using this syntax: C:\**net localgroup Administrators "*username*" /ADD.** See Image #17 below for an example.



```
C:\>net user hacker password /ADD
The command completed successfully.


C:\>net localgroup Administrators hacker /ADD
The command completed successfully.


C:\>net user

User accounts for \\AAA37

-------------------------------------------------------------------------------
Administrator
hacker
The command completed successfully.


C:\>_
```

Image #17: net user command.

Covering their Tracks:

If the Cisco VPN client software is a corporate approve application it may be difficult to discover this type of exploit. With this type of software the person can be not as paranoid about having non-corporate approved software noticed/discovered as with other types of software exploits. As explained in Keeping Access, that after gaining administrator rights and creating false logins, with those same administrator rights, users can "go back" and remove those settings on the VPN client that gave them their initial elevated rights. The VPN application would look as it did before the exploit. Without a host IDS, Intrusion Detection System, or some other monitoring tool, this would be very difficult to discover.

The Incident Handling Process

Preparation: The company had begun to realize the importance of security and had implemented security systems at the perimeter of the network, but had not yet addressed the interior of the network. Several areas of security had been started but were in various stages of implementation.

- Policies and procedures were in the process of being done, but nothing was completed. Some areas were more complete than others, in this case the company had concentrated on exterior threats and not interior based threats.
- No predefined incident handling polices were in place for this type of incident.
- No security “jump-kit” had been gathered.
- The company had no dedicated Security officer or incident handling team.
- Tools were in place to help identify and notify system administrators, but like the policies it was not in a completed state and was not monitored sufficiently.
- Adequate training and time with the security tools were not sufficient.
- System administrators for the infrastructure: Database, Network, Server, Desktop handled and conducted their own, as needed, security procedures, including monitoring, patching, updating and documentation. Adequate communications between the departments was not efficient. No centralize procedures were in place.
- Network baselines of “normal” network traffic were not known. It was unclear that network activity seen was normal or some type of suspicious behavior.

The company had issued a Computer Security Policy for all employees, but just having a policy is not enough. Here are some excerpts, relevant to this exploit, from that policy:

- “To use Company computer systems (hardware, software and data) all Corporation employees (“You or Users”) must comply with our Company’s Computer Security Policy.”
- “Use of company resources for illegal activity is grounds for immediate termination. The Company will cooperate with any legitimate law enforcement efforts.”
- “Ownership: All information accessed, retrieved or used through the Internet into the company network is the sole property of the Company, including any downloaded software or files.”
- “Access Review: The company has software and systems in place that can monitor and record usage. The Company reserves the right to

inspect any and all files stored in private areas of our networks and equipment in order to assure compliance with policy."

- "Intentional Acts: You may not use company facilities knowingly to download or distribute pirated software or data."
- "Downloads: You may not download executable software to Company owned equipment unless explicit permission has been granted."

The above corporate policy states that employees shall use company resources for the sole purpose of doing their stated job(s). This policy was/is communicated and explained to the employee base, and each employee has signed. With this type of appropriate use policy, it may help deter this type of activity. At the lease it provides the company with legal recourses.

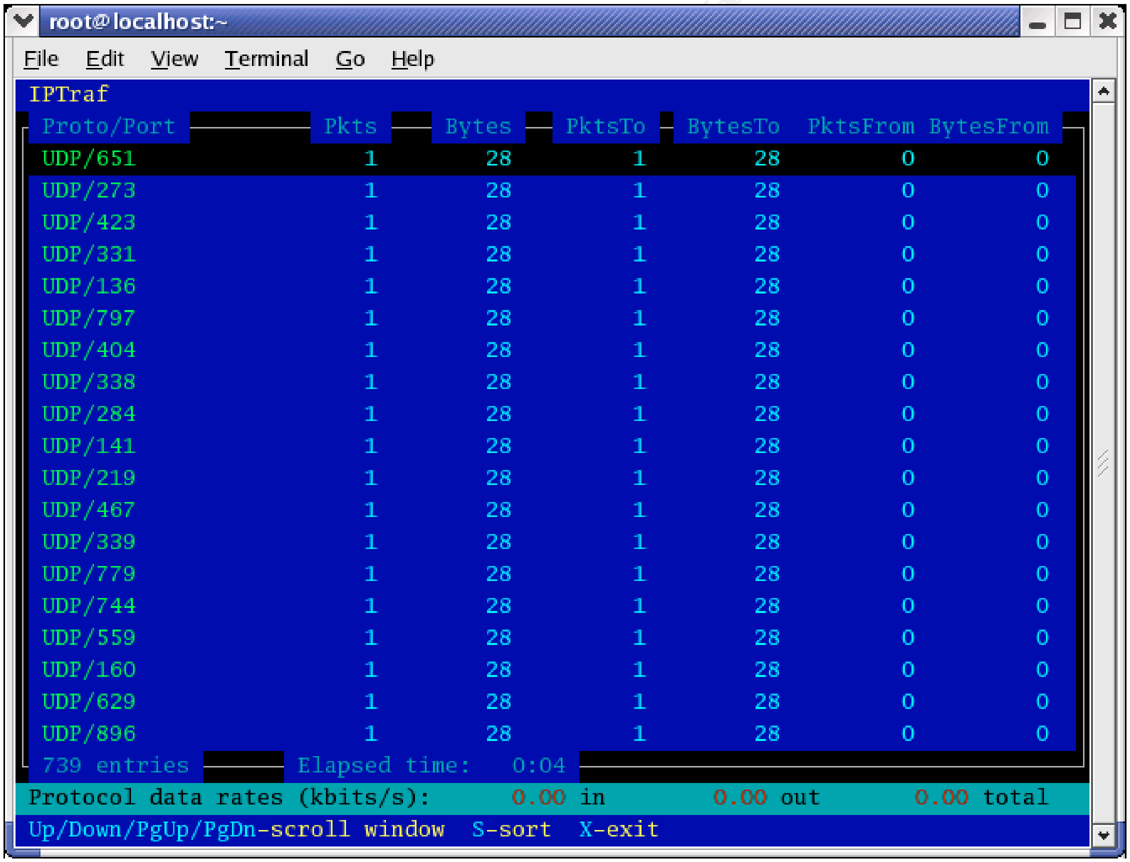
After the incident we began to document and define our internal policies and procedures. We asked ourselves some basic questions and applied what we learned from this incident, along with what we had for our external policies. We addressed the following items to define internal incident handling procedures.
-Guidelines: Step-by-step approach on how to handle and incident.
-Classification types: High, Medium, Low.
-Assignments: Who does what and when.
-Checklists: To be used along with guidelines, insuring steps get completed and documented.
-Questions sheets: What to ask when an incident happens.
-Team members: Who will coordinate, who will document.
-Communication lines: Who to notify, when to notify. When and who makes the decision to send a corporate communication.

You do not want to be doing these types of procedures, or diverting your resources, on-the-fly in the event of a real incident, as was done with this incident.

With this exploit, staying up to date on current bug listings from the software vendor would have alerted administrators to the potential dangers inherent on using the software. Because of this incident each application the corporation had approved for business use was assigned an Application Lead. One of the Application Leads primary duties was to be alert for any potential exploits made public with their assigned application(s). They were also responsible to keep the application up to date with any vendor improvements and patch releases. When any changes, patches, fixes were released by the vendor the Application Lead would notify the Change Control Committee and the newly formed Security Group. The responsibility for these groups, system administrators and application leads, are to evaluate security risks and test any new updates prior to implementing them in the production environment.

Identification: The network monitoring systems could not detect any changes on the exploited laptop but was used to detect some unusual network activity caused by the exploited laptop. Before this incident, normal practice was to periodically run various tools throughout the work week and "monitor" network traffic. In this test environment I also simulated this practice. Once such tool used is IPtraf. This tool collects TCP/UDP packets seen, on the monitored interface, and can display them in a chart format. Starting IPtraf is simply done by typing in IPtraf at the Linux command line. From the IPtraf main menu select Configure, displayed are various settings used to alter how IPtraf gets and displays information. Some helpful configuration parameters are setting, TCP/UDP service names, to, On, and Force promiscuous mode, to, On.

Once the configuration is set, from the main menu, select Statistical Breakdowns, then select, By TCP/UDP port. At the end of a long simulated work day the network administrator began his semi-normal checking and logging out for the day. When he checked the IPtraf tool he noticed this and made a screen capture.

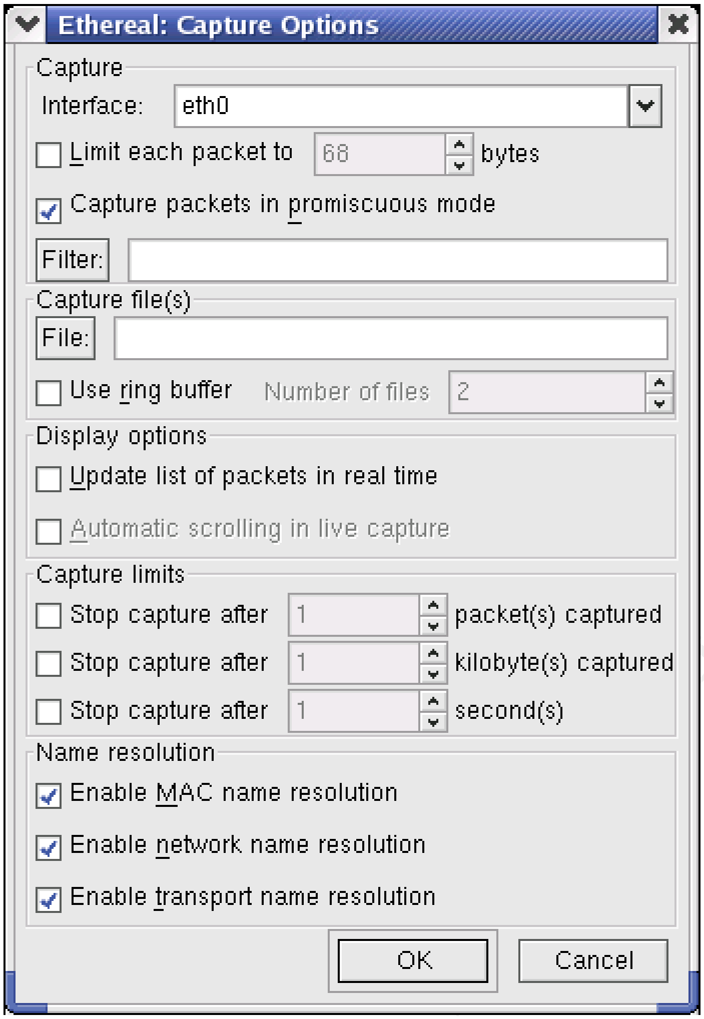


```
IPTraf
┌ Proto/Port ─────── Pkts ── Bytes ── PktsTo ─ BytesTo  PktsFrom BytesFrom ─
│ UDP/651                1       28        1        28         0         0
│ UDP/273                1       28        1        28         0         0
│ UDP/423                1       28        1        28         0         0
│ UDP/331                1       28        1        28         0         0
│ UDP/136                1       28        1        28         0         0
│ UDP/797                1       28        1        28         0         0
│ UDP/404                1       28        1        28         0         0
│ UDP/338                1       28        1        28         0         0
│ UDP/284                1       28        1        28         0         0
│ UDP/141                1       28        1        28         0         0
│ UDP/219                1       28        1        28         0         0
│ UDP/467                1       28        1        28         0         0
│ UDP/339                1       28        1        28         0         0
│ UDP/779                1       28        1        28         0         0
│ UDP/744                1       28        1        28         0         0
│ UDP/559                1       28        1        28         0         0
│ UDP/160                1       28        1        28         0         0
│ UDP/629                1       28        1        28         0         0
│ UDP/896                1       28        1        28         0         0
└ 739 entries ──── Elapsed time:   0:04 ─────────────────────────────────────
 Protocol data rates (kbits/s):      0.00 in        0.00 out        0.00 total
 Up/Down/PgUp/PgDn-scroll window  S-sort  X-exit
```

Image #18: IPtraf network tool.

What he saw was unusual, and he had not seen it before. He saw a high number of UDP packets, all with the same packet size, on a large number of ports. This is usually and indication of a network/port scan, but at first discovery, he was not sure if this was some kind of normal network activity or a sign of suspicious activity.

He continued to run IPtraf for another half-hour and saw nothing out of the ordinary. He left IPtraf running and finished logging out for the evening. Once home he logged back into the network, via VPN, and monitored for the next few hours. (Once connected to the network monitoring was done by using the VNC client, on his remotely connected laptop, to the VNC service running on the server dedicated to network monitoring.) He then would check the tool periodically throughout out the evening from home. At around 12:30am that night he had noticed no other suspicious activity and went to bed. The next morning he continued to watch IPtraf closely. The network administrator then saw a rapid increase in UPD/TCP port usage during the lunch hour. (He had stayed, to eat lunch, at his desk. His thinking/hunch was some network activity would maybe show up during the lunch hour.) He then launched another network tool called Ethereal, which is a network sniffer. It collects packets off of the monitored interface and displays source and destination IP addresses, among other things, along with what is in the captured packets, as long as they are not encrypted. Starting Ethereal is simply done by typing, Ethereal, at the Linux command line. After the application starts, select, Capture, from the menu. The below image (See Image #19, page 30) shows the various settings you can change before starting the capture. Select the interface you wish to capture traffic on and make sure you select the option, Capture packets in promiscuous mode. Otherwise Ethereal will only capture packets that are classified as broadcasts. Such as ARP (Address Resolution Protocol, DNS (Domain Name Service) and various network requests, EIGRP (a Cisco proprietary routing protocol) among others. Hit OK to begin the scan.



Ethereal: Capture Options

Capture

Interface: eth0

☐ Limit each packet to 68 bytes

☑ Capture packets in promiscuous mode

Filter:

Capture file(s)

File:

☐ Use ring buffer   Number of files 2

Display options

☐ Update list of packets in real time

☐ Automatic scrolling in live capture

Capture limits

☐ Stop capture after 1 packet(s) captured

☐ Stop capture after 1 kilobyte(s) captured

☐ Stop capture after 1 second(s)

Name resolution

☑ Enable MAC name resolution

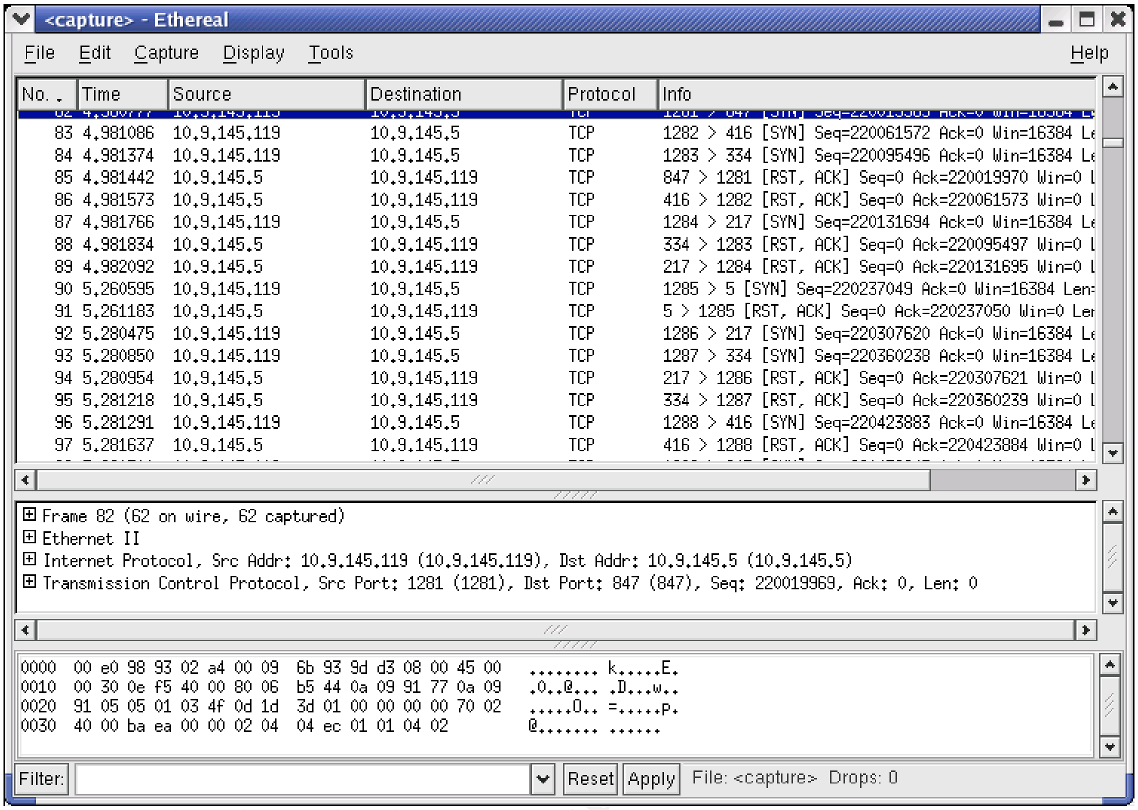
☑ Enable network name resolution

☑ Enable transport name resolution

Image #19: Ethereal Config dialog box.

Some helpful tips: To speed up the displaing of the capture process unselect the check boxes under Name resoultion. To view a capture in real time, (as it happens), make sure you select the option, Update list of packets in real time.

This screen capture gave the source IP address of the UDP/TCP traffic. (See Image #20, page 31.)



```
No. . Time      Source          Destination     Protocol  Info
 83 4.981086  10.9.145.119    10.9.145.5      TCP       1282 > 416 [SYN] Seq=220061572 Ack=0 Win=16384 Le
 84 4.981374  10.9.145.119    10.9.145.5      TCP       1283 > 334 [SYN] Seq=220095496 Ack=0 Win=16384 Le
 85 4.981442  10.9.145.5      10.9.145.119    TCP       847 > 1281 [RST, ACK] Seq=0 Ack=220019970 Win=0 L
 86 4.981573  10.9.145.5      10.9.145.119    TCP       416 > 1282 [RST, ACK] Seq=0 Ack=220061573 Win=0 L
 87 4.981766  10.9.145.119    10.9.145.5      TCP       1284 > 217 [SYN] Seq=220131694 Ack=0 Win=16384 Le
 88 4.981834  10.9.145.5      10.9.145.119    TCP       334 > 1283 [RST, ACK] Seq=0 Ack=220095497 Win=0 L
 89 4.982092  10.9.145.5      10.9.145.119    TCP       217 > 1284 [RST, ACK] Seq=0 Ack=220131695 Win=0 L
 90 5.260595  10.9.145.119    10.9.145.5      TCP       1285 > 5 [SYN] Seq=220237049 Ack=0 Win=16384 Len=
 91 5.261183  10.9.145.5      10.9.145.119    TCP       5 > 1285 [RST, ACK] Seq=0 Ack=220237050 Win=0 Len
 92 5.280475  10.9.145.119    10.9.145.5      TCP       1286 > 217 [SYN] Seq=220307620 Ack=0 Win=16384 Le
 93 5.280850  10.9.145.119    10.9.145.5      TCP       1287 > 334 [SYN] Seq=220360238 Ack=0 Win=16384 Le
 94 5.280954  10.9.145.5      10.9.145.119    TCP       217 > 1286 [RST, ACK] Seq=0 Ack=220307621 Win=0 L
 95 5.281218  10.9.145.5      10.9.145.119    TCP       334 > 1287 [RST, ACK] Seq=0 Ack=220360239 Win=0 L
 96 5.281291  10.9.145.119    10.9.145.5      TCP       1288 > 416 [SYN] Seq=220423883 Ack=0 Win=16384 Le
 97 5.281637  10.9.145.5      10.9.145.119    TCP       416 > 1288 [RST, ACK] Seq=0 Ack=220423884 Win=0 L

⊞ Frame 82 (62 on wire, 62 captured)
⊞ Ethernet II
⊞ Internet Protocol, Src Addr: 10.9.145.119 (10.9.145.119), Dst Addr: 10.9.145.5 (10.9.145.5)
⊞ Transmission Control Protocol, Src Port: 1281 (1281), Dst Port: 847 (847), Seq: 220019969, Ack: 0, Len: 0

0000  00 e0 98 93 02 a4 00 09  6b 93 9d d3 08 00 45 00   ........ k.....E.
0010  00 30 0e f5 40 00 80 06  b5 44 0a 09 91 77 0a 09   .0..@... .D...w..
0020  91 05 05 01 03 4f 0d 1d  3d 01 00 00 00 00 70 02   .....O.. =.....p.
0030  40 00 ba ea 00 00 02 04  04 ec 01 01 04 02         @....... ......
```

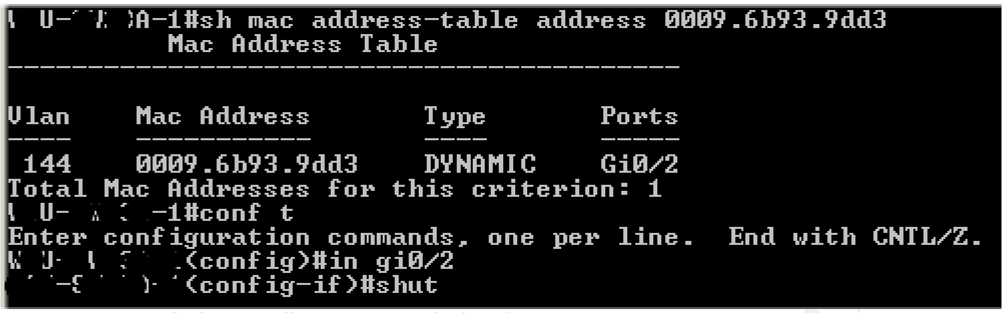
Image #20: Ethereal network tool.

Buy using nslookup, and an internal database used to track PC's to their assigned users, he was able to trace the traffic back to a PC and the registered user of that PC.
Here is an example of the nslookup command. Bring up a command prompt on a Windows 2000 machine and type the following,
nslookup 10.9.145.119 and hit enter

```
C:\nslookup 10.9.145.119      (the target system you wish to get info on)
Server:  name.domain.com      (the name and address of the name server
Address: 10.9.144.1            the command automatically displays)

Name: pc123.domain.com       (the name and address of the PC found)
Address: 10.9.145.119
```

With this information the identity of the system and user was established. After verifying where the identified individual was located, the administrator made a casual, albeit hurried, stroll past the user to see if indeed it was that person at the attacking computer system. Visual conformation was done and management was notified immediately. Back at my desk I examined Ethereal's output. One piece of information captured by the sniffer is the attacking machines MAC address, the physical hardware identification number of the PC's ethernet card. With our network consisting of Cisco switches, I was able to trace the actual port the particular machine was using to connect into the network. With the port identified

I was able to disable the network connection, thus disabling the PC's access onto the network and preventing any further damage by the attack. The below screen capture, sanitized, shows that process of finding and disabling the port.



```
[redacted]A-1#sh mac address-table address 0009.6b93.9dd3
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
 144    0009.6b93.9dd3    DYNAMIC     Gi0/2
Total Mac Addresses for this criterion: 1
[redacted]-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
[redacted](config)#in gi0/2
[redacted](config-if)#shut
```

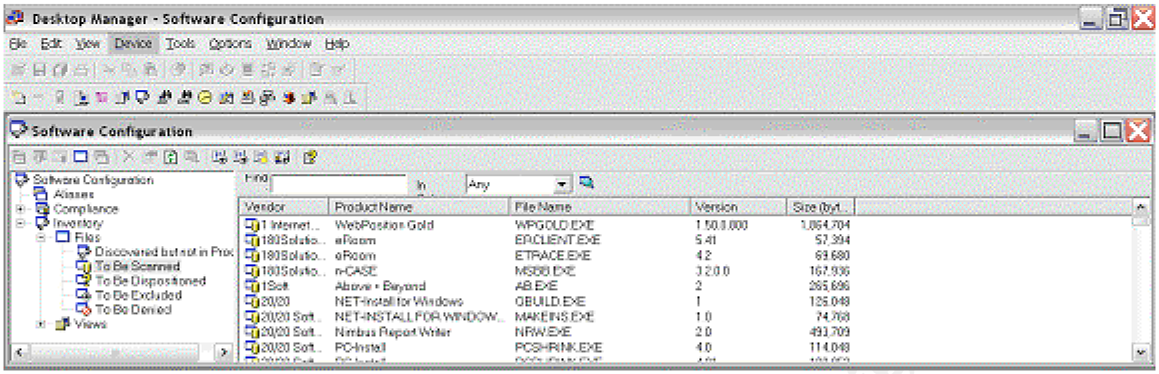
Image #21 Switch port discovery and shutdown.

The person was then very shortly pulled into a meeting with the network administrator, desktop administrator, and the person's supervisor and presented with what was discovered, and asked to explain.

Timeline of events:

- Laptop exploited: Unknown. The exploit could of happened any time prior to discovery.
- Exploited laptop conducts a network scan: Thursday, between the monitoring systems being started, ~7:30am and ~5:00pm when monitoring tools were checked
- Network Administrator discovers unusual UDP traffic: ~5:00pm Thursday
- Network Administrator monitors the situation: Thursday ~5:00pm – 12:30am.
- Network Administrator monitors traffic: Friday ~6:00am –12:15pm.
- Exploited laptop conducts a network scan/Network administrator sees scan: Friday 12:15pm
- Network Administrator runs Ethereal sniffer: 12:16pm
- Attacking/scanning PC identified: 12:22pm
- Visual confirmation of PC and person: 12:30pm
- Notification of Management of incident: 12:35pm
- Attacking/scanning PC network port identified and shut down: 12:49pm
- Identified person confronted and offending PC confiscated: 1:05pm

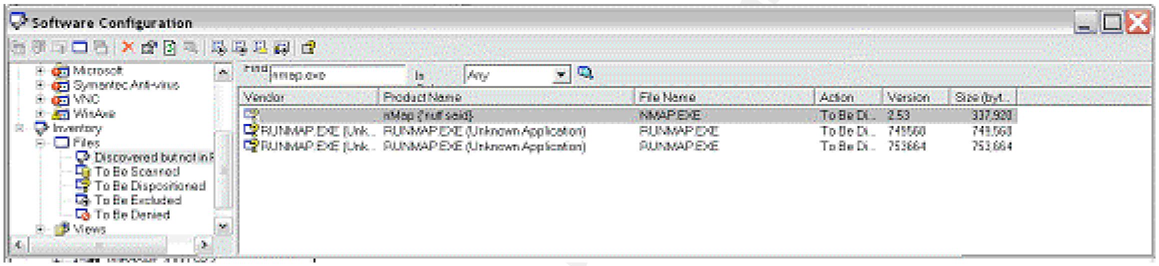
Another method of identification, but not being utilized at the time of the incident, would to use the use of some type of enterprise monitoring solution. One product of this type is the software package called LANDesk. The desktop department had this tool for deploying software and updates, however one capability that the software could do was not being utilized. The software had the capability to scan computer systems attached to the network that had the LANDesk client installed. One feature, of the software, is the ability to alert administrators when a scan discovers a match against a pre-defined list of files to search for.



Vendor	Product Name	File Name	Version	Size (byt...
1 Internet...	WebPosition Gold	WPGOLD.EXE	1.50.0.000	1,064,704
180Solutio...	eRoom	ERCLIENT.EXE	5.41	57,394
180Solutio...	eRoom	ETRACE.EXE	4.2	69,680
180Solutio...	n-CASE	MSBB.EXE	3.2.0.0	167,936
1Soft	Above + Beyond	AB.EXE	2	265,696
20/20	NET-Install for Windows	QBUILD.EXE	1	126,048
20/20 Soft...	NET-INSTALL FOR WINDOW...	MAKEINS.EXE	1.0	74,768
20/20 Soft...	Nimbus Report Writer	NRW.EXE	2.0	493,709
20/20 Soft...	PC-Install	PCSHRINK.EXE	4.0	114,048

Image #22: Landesk tool, defined listing.

In this listing administrators could put known common files of hacker tools and be alerted to the presence of them on computer systems.



Vendor	Product Name	File Name	Action	Version	Size (byt...
	nMap (nuff said)	NMAP.EXE	To Be Di...	2.53	337,920
RUNMAP.EXE (Unk...	RUNMAP.EXE (Unknown Application)	RUNMAP.EXE	To Be Di...	745560	745,560
RUNMAP.EXE (Unk...	RUNMAP.EXE (Unknown Application)	RUNMAP.EXE	To Be Di...	753664	753,664

Image #23: Landesk tool, nmap discovery.

The above screen capture shows the identification of Nmap installed on a monitored PC. One draw back to this is that a pre-defined list of files, has to be created, that has the “right” files to look for. If a hacking tool is new or unknown this type of monitoring would not be sufficient. However having multiple levels, and types, of monitoring tools increases your chances of catching deficiencies in one tool by another.

Containment: The exploited laptop was confiscated and physically removed from the network. (It already had been disconnected at the network port switch level) and examined. On the laptop it was discovered that the Windows version of Nmap was loaded on the system along with other non-approved corporate software, mostly demos of games. Initial conversation with the individual said that they saw the VPN vulnerability posted on some web site, which they could not remember exactly. After seeing the post they followed the instructions and bypassed their logon restrictions. This gave the individual the ability to load any software onto the laptop. The person primarily wanted to install and run games on his corporate laptop. After that, the person confessed, that they delved a little deeper into discovering what else they could find, which is the reason Nmap was installed. “With no intention of breaking into anything, just poking around”, was also said by the individual.

Eradication: After searching the VPN vendors web site and various vulnerability notification sites we discovered the vulnerability and proceeded to apply one of the recommended fixes; Either disabling the option, Enable Start Before Logon in the VPN client and/or upgrading the VPN client to version 4.0(1)A or greater. After an assessment was done a recommendation was given to upgrade all VPN software clients to a non-exploitable version. Management concurred with our upgrade recommendation. A part of the assessment was to verify that the new VPN client was compatible, and did not “break”, any existing corporate approved software on our respective desktop images. A roll out plan was established to upgrade all remaining vulnerable VPN clients.

A thorough examination of the PC was conducted. The system was checked for unauthorized software and system and group accounts. In this case the eradication of the vulnerable VPN version was an upgrade to the VPN application. An alternate option, recommended by Cisco, but not implemented, was to remove the end user access to the VPN files that enabled launching of other applications before logon.

The steps used to verify that the system and group accounts were not modified or changed, on the exploited Windows 2000 Professional PC, are: Right click in the desktop icon, My Computer, and select Manage.

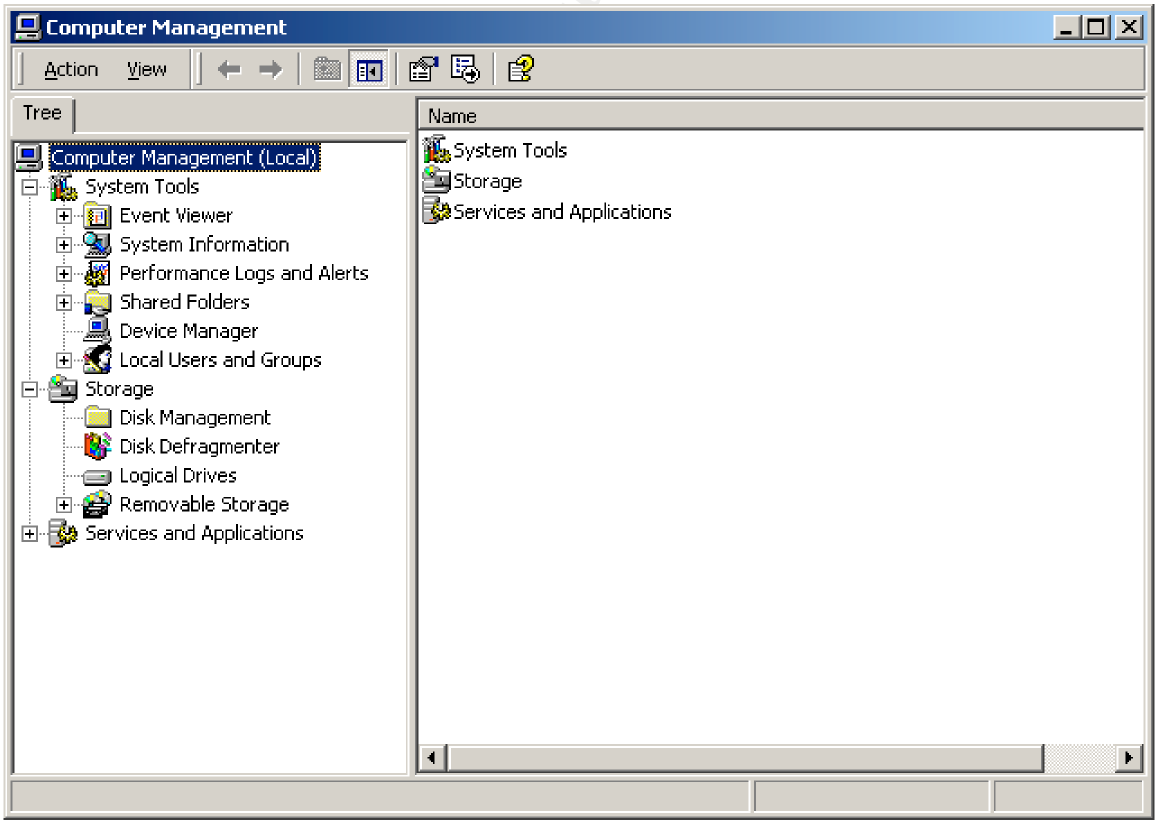
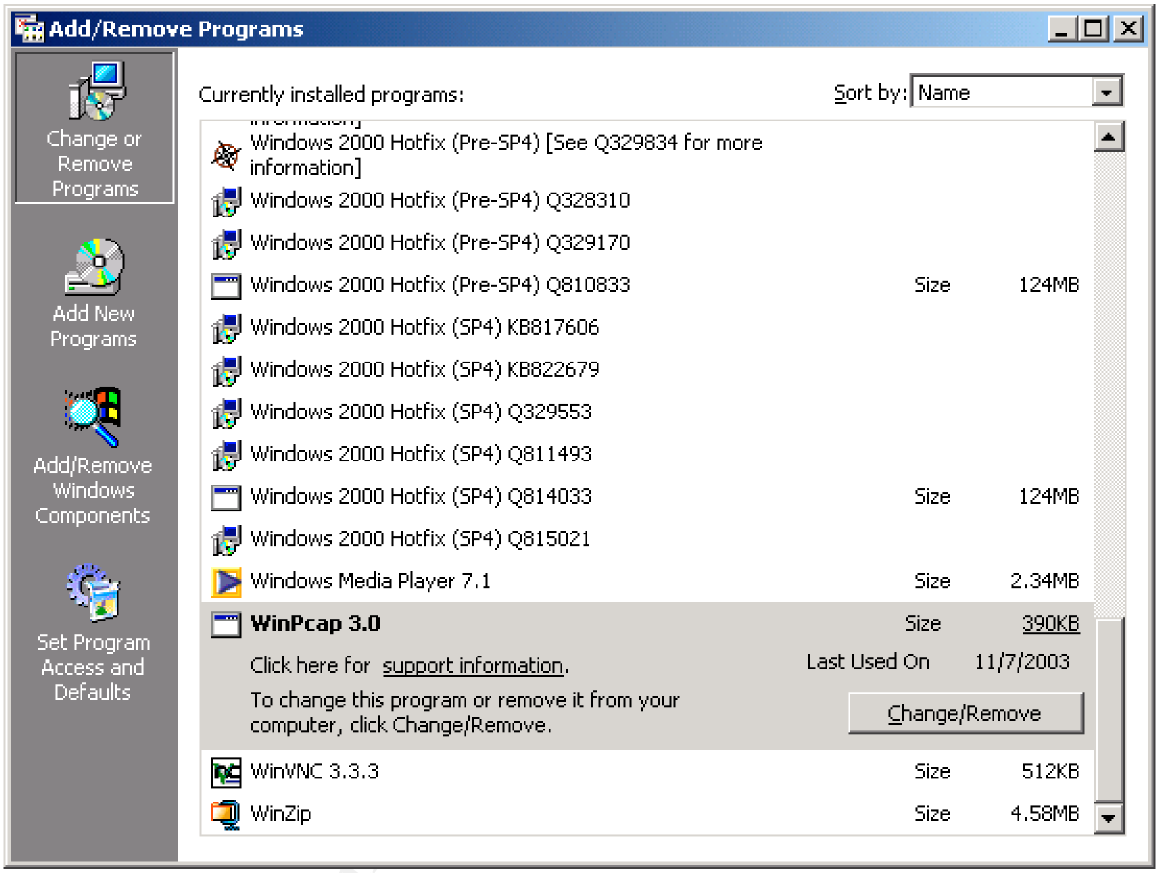


Image #24: Computer Management.

From here select, Local users and Groups. Under the users folder we verified that no additional accounts were added or that the existing accounts were not modified. These account privileges were examined and compared to what the user would have been assigned originally. The same was checked for the security groups, any deletions, additions or modifications. Also all non-approved software was uninstalled via the control panel Add/Remove Programs.



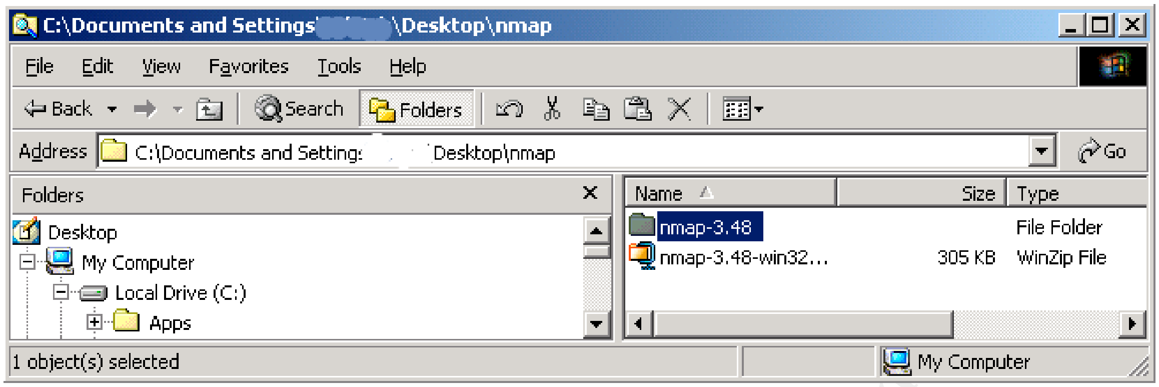
Add/Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Sort by: Name
Change/Remove

Currently installed programs:

Windows 2000 Hotfix (Pre-SP4) [See Q329834 for more information]
Windows 2000 Hotfix (Pre-SP4) Q328310
Windows 2000 Hotfix (Pre-SP4) Q329170
Windows 2000 Hotfix (Pre-SP4) Q810833 Size 124MB
Windows 2000 Hotfix (SP4) KB817606
Windows 2000 Hotfix (SP4) KB822679
Windows 2000 Hotfix (SP4) Q329553
Windows 2000 Hotfix (SP4) Q811493
Windows 2000 Hotfix (SP4) Q814033 Size 124MB
Windows 2000 Hotfix (SP4) Q815021
Windows Media Player 7.1 Size 2.34MB
WinPcap 3.0 Size 390KB
Click here for support information. Last Used On 11/7/2003
To change this program or remove it from your computer, click Change/Remove.
WinVNC 3.3.3 Size 512KB
WinZip Size 4.58MB

Image #25: Add/Remove deletion on non-approved software.

After that a manual sweep of the file system was done to remove any other software that could not be remove by the operating system.



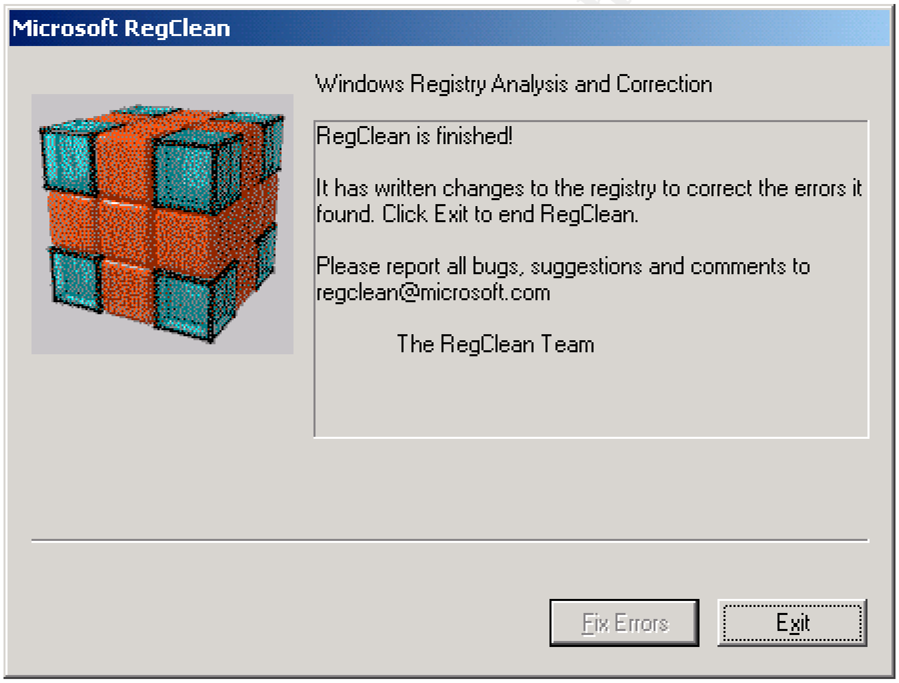
C:\Documents and Settings\[redacted]\Desktop\nmap

Name	Size	Type
nmap-3.48		File Folder
nmap-3.48-win32...	305 KB	WinZip File

1 object(s) selected

Image #26: Manual deletions of non-approved software.

After the uninstall was run, a manual verification of the files system was also conducted. Anything the Windows uninstall didn't remove was deleted by selecting the files and folders left behind by the software through the Windows Explorer. We also checked the registry by running the Microsoft utility called Regclean. This tool removes all unused registry settings that can be left behind when uninstalling applications. Regclean is started by running the executable called regclean.exe..



Windows Registry Analysis and Correction

RegClean is finished!

It has written changes to the registry to correct the errors it found. Click Exit to end RegClean.

Please report all bugs, suggestions and comments to regclean@microsoft.com

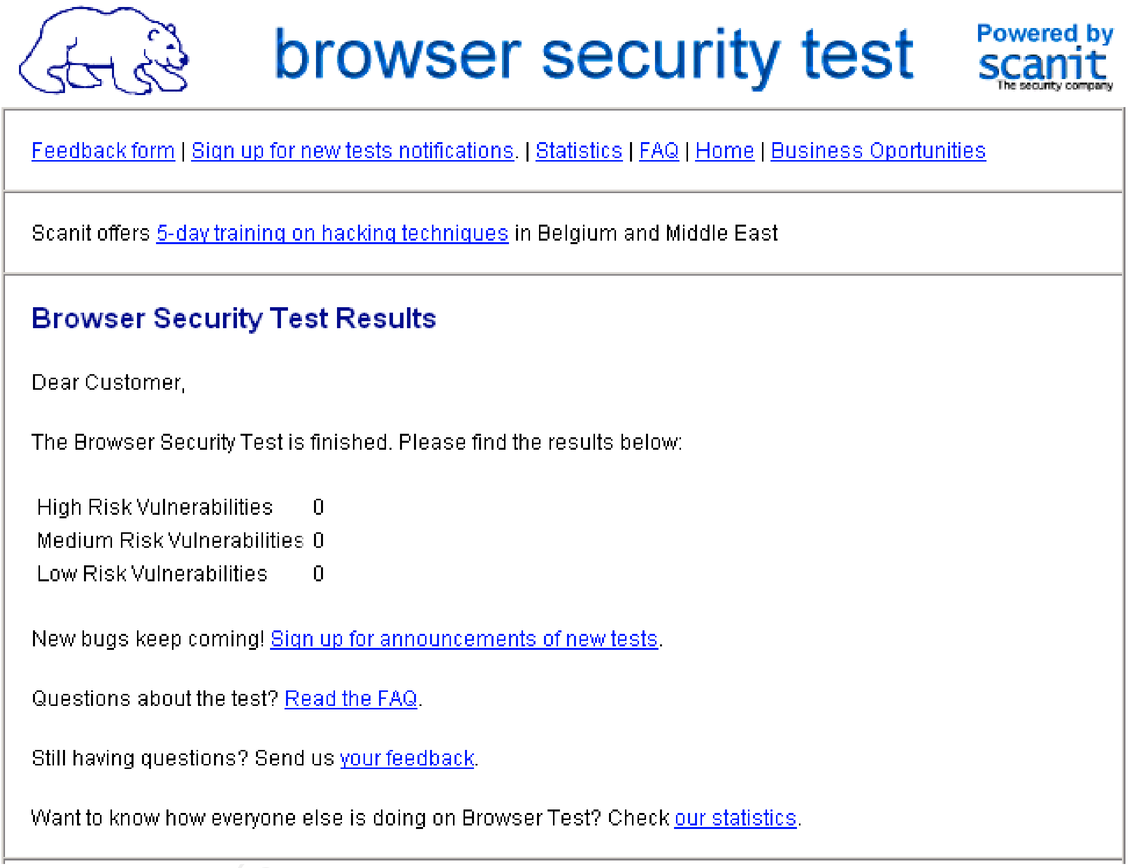
The RegClean Team

Image #27: Regclean application.

One additional final step was the PC was reconnected to the network and used to connect to two Internet scanning sights to verify no other malicious software was installed. (Note Norton anti virus software was running and up-to-date on the exploited PC. Norton anti-virus did not alert or discovery any type of virus on the exploited PC. We thought, in our best interest, after the user downloaded non-approved software onto the PC it would be viable to use other sources in checking for malicious code.)

Neither scan produced or discovered anything unusual.

http://bcheck.scanit.be/bcheck



browser security test
Powered by scanit
The security company
Feedback form | Sign up for new tests notifications. | Statistics | FAQ | Home | Business Oportunities

Scanit offers 5-day training on hacking techniques in Belgium and Middle East

Browser Security Test Results

Dear Customer,

The Browser Security Test is finished. Please find the results below:

High Risk Vulnerabilities	0
Medium Risk Vulnerabilities	0
Low Risk Vulnerabilities	0

New bugs keep coming! Sign up for announcements of new tests.

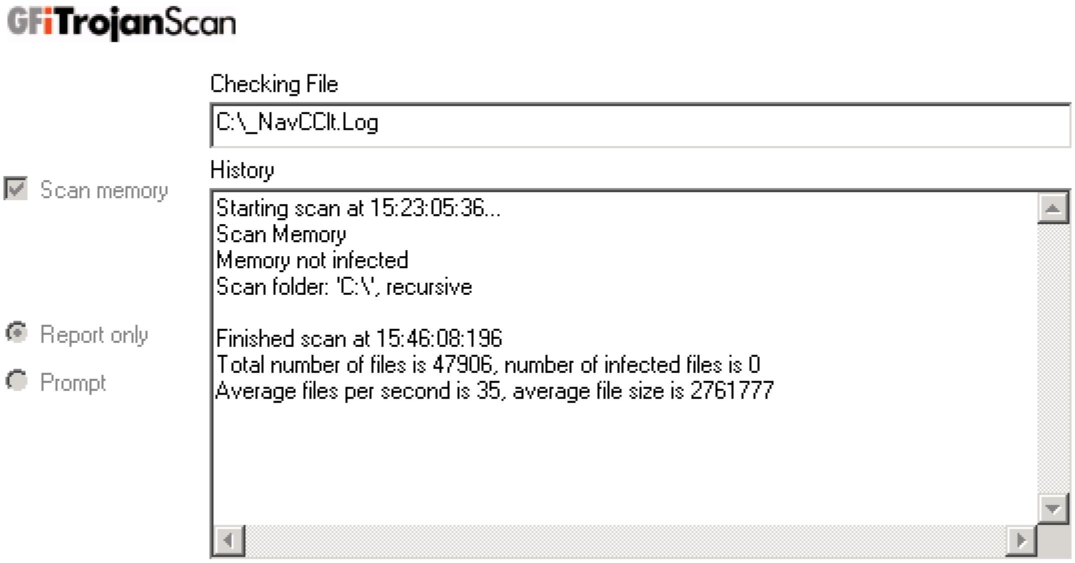
Questions about the test? Read the FAQ.

Still having questions? Send us your feedback.

Want to know how everyone else is doing on Browser Test? Check our statistics.

Image #28: bcheck, Internet scan #1.

http://www.trojanscan.com



Checking File

C:_NavCClt.Log

History

```
Starting scan at 15:23:05:36...
Scan Memory
Memory not infected
Scan folder: 'C:\', recursive

Finished scan at 15:46:08:196
Total number of files is 47906, number of infected files is 0
Average files per second is 35, average file size is 2761777
```

Image #29: TrojanScan, Internet scan #2.

Recovery: The exploited laptop was cleaned, as described in the eradication steps, and returned to service. It was determined after the above examination a full system wipe and restore would not be necessary. The following incident report was created.

Incident Summary Report

Identification:
Incident number: 001-10-1-2003
Cause of Incident(s): Malicious program, Nmap scanning.
Host Name: AAQ43
Hardware: IBM Laptop
IP Address: 10.9.145.5
Operating System Name: Windows 2000
Patch Level: SP4 – latest hotfixes and patches to date.
Log files reviewed (filenames and locations): Symantec Virus History log.
Evidence cited and Intruder Activity (files added/changed/removed): nmap and winpcap files installed on the laptop.
Location (where incident took place):Main corporate office.
Security Policy Breached: Unauthorized use of corporate equipment.
Stakeholders (owner/department): XXXX / IT Department, XXXX / Design Department
Detection Method: IPtraf network monitoring tool.

Containment:
Method: Offending laptop was disconnected from network by shutting down network port at the switch level. Laptop then was confiscated for examination.

Eradication:

Method: 1.) Deleted non-approved programs via operating system Add/Remove and verified through a manual detection of the file system. Microsoft RegClean utility was run. Verification of system configs, accounts, groups, and settings were compared to what they were originally set to. Internet scanning conducted from two sites.

Recovery:

Damages: None.

Testing: Run various tools against laptop. http://bcheck.scanit.be/bcheck/, http://www.trojanscan.com/, Run windows update.

Monitoring: Monitor activity on PC. For 1 week.

Summary:

Timeline of events:

- Laptop exploited: Unknown. The exploit could of happened any time prior to discovery.
- Exploited laptop conducts a network scan: Thursday, between the monitoring systems being started, ~7:30am and ~5:00pm when monitoring tools were checked
- Network Administrator discovers unusual UDP traffic: ~5:00pm Thursday
- Network Administrator monitors the situation: Thursday ~5:00pm – 12:30am.
- Network Administrator monitors traffic: Friday ~6:00am –12:15pm.
- Exploited laptop conducts a network scan/Network administrator sees scan: Friday 12:15pm
- Network Administrator runs Ethereal sniffer: 12:16pm
- Attacking/scanning PC identified: 12:22pm
- Visual confirmation of PC and person: 12:30pm
- Notification of Management of incident: 12:35pm
- Attacking/scanning PC network port identified and shut down: 12:49pm
- Identified person confronted and offending PC confiscated: 1:05pm

HR, Human Resources, the person's manager and the head of IT resolved the issue with the user and an unknown discipline was handed out.

Our newly formed internal handling procedures helped define different recovery procedures, depending on type of system, desktop or server that in the future, be unfortunately involved in an incident.

How to Protect against: Cisco recommends two methods for fixing this vulnerability. The first involves giving only read access to the files and directory where the VPN client is installed. This prevents the modification of required operation files the VPN client reads upon execution. The second option, and most preferred, is to upgrade the VPN client to a repaired version, in this case 4.0(1)A. Administrators must take care to test and verify that either protection method they choose actually stops the exploit from happening.

Some default conclusions were made as to what to do with systems. Albeit these baselines procedures were designed to be flexible enough to change with each incident, but also to give a baseline to start with. Desktop systems, after any removal of any critical data, the hard disk should be wiped clean and re-imaged with a new corporate desktop image. The same should be said for any server. Careful inspection of any needed data must be conducted. If you can pinpoint the time of the exploit, you can go back to system backups, prior to that time, and get the system back to a known pristine state. Knowing what the exploit is will help an administrator install the proper patches, hotfixes and upgrades as necessary for the operating system and installed software.

Once the patches or updates are completed, test weather the exploit is still possible. Do not take the word of the software manufacturer! Verify for yourself. In this exploit we tried to alter the files directly, after removing access to them. (One fix/cure method recommended by the vendor that we did not employ.) We also tried to launch a renamed executable. (ipsecdialer.exe variant exploit for client version 4.0(1)). We tested these options before putting the system back into production.
One point to note is after recovering the system and applying the necessary upgrades/patches to fix the exploit, make sure the business reason, why you have the software, still works as it was intended. Also ask yourself, do you have sufficient monitoring, testing and validation in place? After this incident the creation of the Application Lead role should hopefully prevent incident similar to this from happening again.

We checked the rest of our deployment and verified all systems with the affected VPN client were upgraded. (There is/was no released Cisco patch for fixing this issues, just a required application upgrade. Patching in this case would require altering the access rights to the files and directory where the VPN client installs. In this case the vpnclient.ini and the appropriate Profile text files.)

Lessons Learned:
An administrator must be up to date and aware of what software is used in their corporate environment and what possible exploits are made public. A continuing effort has to be made from multiple sources to discover what potential threats are possible. Once this process is created and followed future incidents will be minimized. In this exploit, the VPN client was used as the manufacture designed it, however the end user constructed an attack that took advantage of these default settings along with the lack of security checking within the VPN application.

Our process was lacking for this piece of software and others. This lesson, and our own realization, help us define and created the role, Application Lead. We also documented that anyone noticing any kind of suspicious activity, known, or unknown, should report it immediately to the now defined security team, regardless of time or location. Although the network administrator acted in good faith, by continually monitoring the situation, he should have made some attempt to notify other individuals. Although in this incident, it would have not made any difference, we determined that we could not rely on this type of operations in the future.

We also noted, that although we believe we have sufficient monitoring tools in place, they were not being watched, in a timely or structured manner. An example of this was that we had an application that could scan the network and compare it's scan, of PC's and servers, to a defined database and alert of any discrepancies found. This application was primary used by Desktop to deploy software and patches to remote desktops.
This also pointed out the lack of communications between departments. Rules and responsibilities were assigned to each tool and report mechanisms were put into place for each department. We also established a weekly security meeting and scheduled to have selected Application Leads report any discoveries learned since the last time they attended a meeting. In these meetings, as a group, we also established a process to review the gathered reports and increase our knowledge and boost our network and system security.
Periodic sweeps of the network searching for non approved software would be a good preventive procedure. With sweeps of this nature discovery of vulnerable software, i.e. out of date, would help distinguish differences between software levels of the same type of applications. In this case after it is known particular version levels are vulnerable a sweep would identify weather or not a particular application is at the current approved levels.

A listing of security initiatives implemented.

Security Initiatives:

- Creation of the role Application Lead: Primary duties are to keep track of available upgrades/patches/hotfixes on their assigned applications.
- Structured monitoring methods established for tools: A documented method for monitoring systems established for each tool. Including timelines, schedules, training, and reporting mechanisms.
- Communications between departments for security: Each department to have a security lead for communicating security related items.
- Weekly Security Meetings: An established forum for the discussion of security related items.
- Incident handling team: Assigned responsibilities for conducting and incident.
- Incident handling "Jump Kit": A collection of tools already gathered for incident handling. Our newly formed jump-kit consisted of the install disks of our major corporation operating systems and major software applications. CD's with various security tools installed on them. And a dedicated laptop for mobile incident handling; which already has a predefined list of applications installed for security incidents. Documentation was also included in the jump-kit, phone lists, communication guidelines, processes, procedures and incident forms.

Conclusion / Summary

Here is a high level summary for the Cisco VPN Client Privilege Escalation exploit.

Issues:

1. The exploit is a local system exploit. – It can be conducted off the network and the affected system can be quietly reestablished to the network. The discovery of the exploit can in turn be very difficult to discover.
2. Not every system has a Host IDS, or other monitoring process to alert administrators. Again leading to the difficult nature of seeing this exploit. Active scanning would have to be done.
3. VPN software is a common corporate approved application. It does not standout as much as some other “black hat” applications would.
4. With this exploit if a user were only used to install local programs, an example would be games, the incident would have not been discovered. It was the addition of other “black hat” activities that alerted us to the fact there was some problem.

Solutions:

1. Be aware of what is running on your systems and networks. Know what is happening on them. Do not focus on just the operating system keep in mind what is installed on that operating system.
2. Have monitoring systems that overlap. It would most likely be a financial, as well as a management, nightmare to have a host IDS on every system. Have other tools in place to sweep the network and attached systems for up to date, patched/upgraded software.
3. Keep up to date on all your applications flaws. Keep an eye on CERT and CVE lists along with any software manufactures bug/exploit listings. (New responsibility for the newly created Application Lead.)
4. Review, Patch/upgrade when fixes, or exploits, become available! (New responsibility for the newly created Security Team.)
5. There are tools available that can scan network attached PCs and servers and search for unauthorized software. If this type of monitoring tool were employed, local exploits of this type could be discovered. In the example, if the user would only use their escalated privileges to download and install games on the PC, a scan by this type of application could discover unauthorized software installs. A part of this process would be the creation of a list/database of popular game titles and known hacker tools, which the application could to alert administrators of any hits while scanning.

The above reasons emphasize the necessary due-diligence required by a System Administrators, and Application Leads, to keep ahead of known exploits, buffer overflows, flaws, design flaws, etc., and also how an attacker could utilize, to their ends, common features of installed applications.

The most important lesson for an administrator, or Application Lead, to know is to understand what applications are installed and running on your systems and network. This coupled with knowing and keeping up to date with patches, vulnerabilities, and exploits, that are publicly available for those applications, will go a long way in preventing incidents like this, and others, from happening.

Extras:

Preparation Extras:
Preparation helps answer these questions.

- Do you *have* adequate policies, processes, procedures and documentation?
- Do you have checklists?
- Are the right resources, primary, secondary, tertiary and help desks properly identified?
- Has data, software and hardware been classified?
- Do you know who, how and when to contact someone?
- Are you aware of any possible delays?

Some good preparation ideas are doing what-if types of scenarios. What-if this happened, or what-if that happened, or both! A part of being prepared is to know when things happen. Does the corporation have the correct and/or sufficient types of monitoring devices in play? Does the corporation have adequate baselines of network traffic? These baselines help administrators recognize when any abnormal behavior happens? (So long as they are adequately reviewed.) Most importantly are your administrators keeping up to date on patches, upgrades and public exploits that are available to them.

If you do not have an Incident policy some tried and true emergency techniques are as follows:
Keep calm: There are most likely others, management and end users, being excited enough. Take your time. Things will be missed, evidence lost or corrupted. Mistakes can and will happen if you yourself are not in control.

Establish a chain of command: Communication is essential when the incident fires are burning.

Document everything: Including each and every step you or your team does. If you can't do both, fight the fire and document; assign someone else to write the documentation.

Attack the problem: Do the necessary steps to stop, collect information/evidence, eradicate and restore.

Review, Lessons learned: After all is said an done bring your group together and openly discuss what happened and what can be done in the future to make sure it doesn't happen again.

Identification Extras:

The actual verification of the exploit took very little time, what was disturbing was that the exploit was made public for several months before we even knew about it. That identified a process of not keeping up to date on various patches and updates for our corporate approved software. Most of our attention was directed on the operating system and not what was running on it! A good lesson to remember. Identification helps answer questions like these.

- Are you aware of the situation?
- Do you know the interactivity / relationships between systems?
- Is it a small, medium or large incident?
- When did it happen?

Is there a risk of continuing operations?

Also included for reference are definitions that can help classify an incident/event.

To help classify an incident or event an administrator should develop a High, Medium and Low classification chart based on the CIA characteristics; Confidentiality, Integrity and Availability.

Confidentiality: Consequences of unauthorized disclosure or compromise of information in the system.

Integrity: Consequences of unauthorized modification or destruction of information in the system.

Availability: Consequences of delay in processing, transmission or storage of information in the system or the disruption or denial of the service provided by the system.

In this case, Cisco VPN Client Privilege Escalation Vulnerability, the raising of access rights was classified as a High Confidentiality, High Integrity and High Availability incident. The high classification was given because access to files, that were not normally available to the end user were now readable, writeable and executable. Because of possible changes to these said files, their Integrity becomes questionable.

Another way, or used in conjunction with the CIA classification method, is to classify based on the targeted host PC. Some categories are based off of access method(s), interconnections with other systems and number of potential affected users.

Access Methods:
Low: Access to the system is via protected communications channels, (e.g. dedicated connections).
Medium: Access to the system is via relatively constrained communications channels, (e.g. Intranet connection).
High: Access to the system is via. Freely accessible communications channels, (e.g. Internet or unrestricted wireless networks).

Interconnections:
Low: No backend connections to any systems exist.
Medium: A backend connection to the system exists, which itself has relatively constrained connections to other systems.
High: A backend connection to the system exists, which itself has freely accessible connections to other systems.

End users:
Low: An extremely limited number of authorized individuals have access to the system.
Medium: A limited number of authorized individuals have access to the system.
High: An unlimited number of authorized individuals have access to the system. (e.g. walkup workstation)

Included below is a sample template for what types of question can and should be asked when an incident is being reported or discovered. This template covers the 5 basic W questions; Who, What, Where, When. Asking these types of questions will lead you to the Why.

Guideline – Incident Response
Guidelines for reporting an Incident Response event or suspicious activity. The preferred method for reporting an incident is by calling the help desk at extension XXXX, option X. Other less preferred methods are through existing central reporting mechanisms or by email at *security@yourdomain.com* An individual reporting the incident will be asked to provide the following information:

- Who: Name and phone number of person reporting the incident

- What: The types of information that will be needed if known:
  - Affected system(s) or site(s)
  - Hardware and operating system (If known)
  - Symptoms
  - Connections with other system that were active

- What: The types of information that will be needed if known: (continued)
  - Actions taken (if any)
  - Damage(s)

  - What the user(s) were doing when the incident happened.
  - Other application being run at the time
  - Number of people affected
  - Any other information the users deems relevant

- Where: Location of problem: building, remote office, home

- When: Date, time and duration (if not on going)

Once the above information is collected the user will be instructed to be available, if necessary, for further questioning, information gathering and testing.

Recovery Extras:
Depending on what type of system it was, desktop or server, different recovery procedures may be done. With a desktop system, after any removal of any critical data, the hard disk should be wiped clean and re-imaged with a new corporate desktop image. The same should be said for any server. Careful inspection of any needed data must be conducted. If you can pinpoint the time of the exploit, you can go back to system backups, prior to that time, and get the system back to a known pristine state. Knowing what the exploit is will help an administrator install the proper patches, hotfixes and upgrades as necessary for the operating system and installed software. Once the patches or updates are completed test weather the exploit is still possible. Do not take the word of the software manufacturer! Verify for yourself. In this exploit see if you can alter the files directly, provided you removed restrictions to them. See if you can launch a renamed executable. (ipsecdialer.exe variant exploit for client version 4.0(1)). Test before putting the system back into production. One point to note is after recovering the system and applying the necessary upgrades/patches to fix the exploit, make sure the business reason, why you have the software, still works as it was intended. Also ask yourself, do you have sufficient monitoring, testing and validation in place?

Be sure an check the rest of your deployment and verify all systems with the affected VPN client are patched. (There is no released Cisco patch for fixing this issues, just a required application upgrade. Patching in this case would require altering the access rights to the files and directory where the VPN client installs. In this case the vpnclient.ini and the appropriate Profile text files.)

Lessons learned Extras:
Make sure to document and report all incidents. This type of documentation may help you, or someone else in the corporation, fight the next fire.
Simply keeping up to date on software vulnerabilities would have alerted a diligent systems administrator to potential problems. Once alerted the administrator can take actions against reported security risks.

<u>Risk Analysis:</u>

Another proven way to keep abreast of you corporate systems and networks is to conduit a risk analysis against what your security policies state. The below diagram helps define a guideline for a step-by-step process for conducting risk analysis. The whole point, of a risk assessment, is to verify if you are actually doing what is defined in the corporate security policies, processes and procedures. A risk analysis will also help define security gaps. You will then be able to prioritize these "gaps" and further protect the corporate infrastructure. If for some reason a process is not being followed a risk analysis will bring that to light. It will also help clarify and point to needed modifications that otherwise may be missed.

Security policies define controls, which are used by Risk Assessments to help define and mitigate exposures and risks.

A Risk Assessment can begin on the "outside" with your Extended Perimeter. Business partners, Customers, Remote Users, Telecommuters, Branch Offices and Service Access. Work your way "inside" to the Perimeter. Wireless Access Points, Firewalls, Managed Security Services, VPN's, Intrusion Detection Systems, Circuits and Virus/Email Scanning. Further "inside" would be your Controls. Single Sign-On Authentication, RADIUS/TACACS (Terminal Access Controller Access Control System) Authentication, Policy Management & Enforcement, Access Control Lists, Network VLANS (virtual LANs) and Identity Management. The last point of verification would be your Resources. Devices, Hardware End Points, Applications, Voice Infrastructure, Data Infrastructure, Personal and Operating Systems.

Risk Assessment Direction:
Extended Perimeter → Perimeter → Controls → Resources

Your control goes from unknown environments to, hopefully, a controlled and documented environment, which you administer. There are may types of Risk Assessments, from Failure Mode and Effects Analysis, HAZOP (Hazard and Operability), Historical Analysis, Human-Error Analysis, Probabilistic Risk Assessment and Tree Analysis. You will have to determine which is best for you and you corporation.

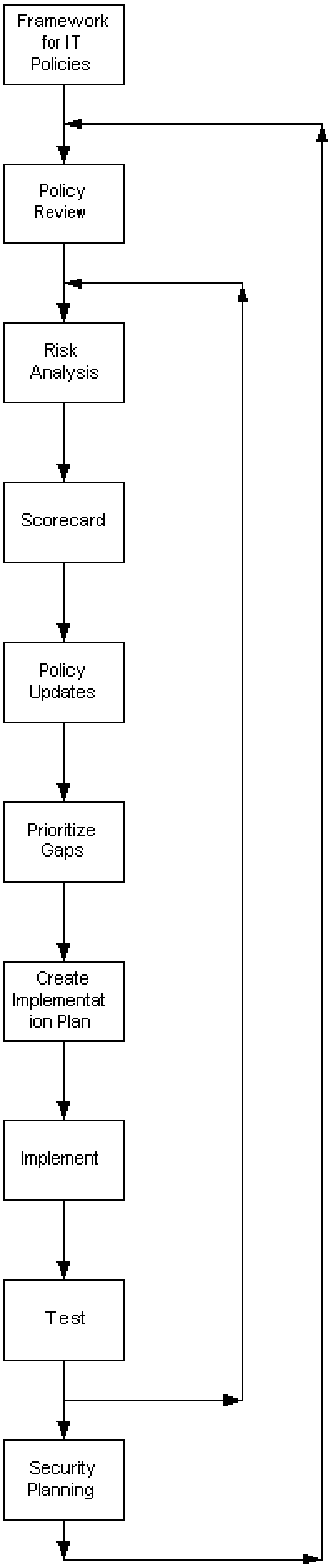

Framework for IT Policies
Policy Review
Risk Analysis
Scorecard
Policy Updates
Prioritize Gaps
Create Implementat ion Plan
Implement
Test
Security Planning

Image #30, Page 48, Risk Analysis flow chart

References:

1. Securityfocus.com, Vulnerabilities: "Cisco VPN Client Privilege Escalation Vulnerability", URL: http://www.securityfocus.com/bid/7599/info/ , (17, June 2003).

2. Securityfocus.com, Vulnerabilities: "Cisco VPN Client Privilege Escalation Variant Vulnerability", URL: http://www.securityfocus.com/bin/7665/info/ , (17, June, 2003)

3. Staff, Nick, "Cisco Systems VPN Client allows local logon with Elevated Privileges". 14, May 2003, URL:http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0305&L=ntbugtraq&F=P&S=&P=4117 , (15, August 2003)

4. Staff, Nick, "Re:Cisco Systems VPN Client allows local logon with Elevated Privileges". 14, May 2003, http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind0305&L=ntbugtraq&D=0&F=P&P=4605 , (15, August 2003)

5. Ludens, Douglas, "The Windows 2000 Boot Process", URL: http://windows.about.com/library/weekly/aa000716a.htm , (3, Sept. 2003)

6. Alternate Reference: Cisco.com, (Cisco login required) "Troubleshooting and Programming Notes", URL: http://www.cisco.com/en/US/customer/products/sw/secursw/ps2308/products_administration_guide09186a00800bd991.html , (17, June 2003)

7. Alternate Reference: Cisco.com, (Cisco login required) "CSCeb12179 Bug Details", URL: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb12179 , (17, June 2003)

Image Reference:

Image #1, Page 9: Diagram of Windows boot in relation to the Cisco VPN Client Winlogon feature.
Image #2, Page 10: Winlogon registry setting showing the GinaDLL modification.
Image #3, Page 14: Network Diagram
Image #4, Page 16: Demonstration of users desktop privileges before exploit
Image #5, Page 17: Insufficent install privileges
Image #6, Page 17: Disabled registy editing